

Hardening email security with threat prevention platforms

Anders Skogster

Master's Thesis
December 2017
School of Technology
Master's Degree Programme in Information Technology
Cyber Security

Author(s) Skogster, Anders	Type of publication Master's thesis	Date December 2017 Language of publication: English
	Number of pages 100	Permission for web publication: x
Title of publication Hardening email security with threat prevention platforms		
Degree Programme Master's Degree Programme in Information Technology, Cyber Security		
Supervisor(s) Karo Saharinen and Mika Rantonen		
Assigned by Antti Lehtonen, Cygate Oyj		
Abstract <p>Most of today's email traffic consists of spam, malicious emails and other unwanted emails. These emails will fill up the user's mailbox, infect your computer and possible the whole network you are using. Cygate offers its customers in their product portfolio a wide range of different security platforms that can be used for identifying and mitigating threats on different parts of the network.</p> <p>Some of Cygate's offered on-premises platforms for protection against the email attack vector were compared, a comparison of the threat identification, mitigation and important parts like, setting up the device, administration, logging, polling and cost and benefit ratio.</p> <p>The research was based qualitative research method, in more specific a collective case study. Key parts of the platforms were compared to each other and rated, from setup to cost/benefit ratio. The most valuable part of the study was the comparison of threat mitigation between the platforms, as Cygate can use the results in future projects.</p> <p>An understanding between the differences of the threat prevention platforms was obtained with the comparison. The capabilities of the platforms are also better known after analyzing the data and results. The results shows how the platforms positions to each other, in sense of what platform would suit which customer and environment. This is helpful and beneficial knowledge that can be used in future installations and even more helpful in coming assessments and discussions with customers on which platform to use.</p> <p>Similar projects could be done for other threat prevention platforms protecting against other attack vectors. The collection of the raw data and comparison process need to be refined in future projects.</p>		
Keywords/tags (Cyber-Security , threat prevention , email security)		
Miscellaneous		

Tekijä(t) Skogster, Anders	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Joulukuu 2017
		Julkaisun kieli Englanti
	Sivumäärä 100	Verkojulkaisulupa myönnetty: x
Työn nim Hardening email security with threat prevention platforms		
Tutkinto-ohjelma Master´s Degree Programme in Information Technology, Cyber Security		
Työn ohjaaja(t) Karo Saharinen ja Mika Rantonen		
Toimeksiantaja(t) Antti Lehtonen, Cygate Oyj		
Tiivistelmä <p>Päivittäisestä sähköpostista suuri osa koostuu roskapostista ja haittaohjelmia sisältävistä postista. Nämä sähköpostit täyttävät käyttäjän sähköpostilaatikon, tartuttavat tietokoneen ja mahdollisesta paikallisen verkon haittaohjelmilla. Cygate tarjoaa tuoteportfoliossaan asiakkaalleen valikoima tietoturvalaitteita, joilla voidaan tunnistaa ja estää tietoturvauhkia tietoverkon eri osa-alueilla.</p> <p>Cygaten tarjoamasta tuoteportfoliosta verrattiin kolme paikallisesti asennettavaan ja sähköposti-hyökkäysvektorin torjuntaan tarkoitettu tietoturvalaite kyky tunnistaa ja estää tietoturva-uhkia. Myös muut tärkeät osa-alueet kuten laitteen asennus, hallinta, lokien tuottaminen ja laitteen hinta-hyötysuhde verrattiin keskenään.</p> <p>Tutkimus perustui laadulliseen tutkimukseen, tarkemmin kollektiiviseen tapaus-tutkimukseen. Tärkein vertailu tutkimuksessa oli tietoturvalaitteiden kyky tunnistaa ja estää tietoturvauhkia. Tutkimuksesta saatiin ymmärrys laitteiden välisistä eroavaisuuksista. Dataa ja tuloksia analysoimalla saatiin myös selville laitteiden rajoitteet ja toiminnallisuus. Tulokset näyttävät, miten laitteet sijoittuvat toisiinsa nähden, eli mikä laite sopii millekin asiakkaalle ja ympäristöön. Tätä kattavaa tietoa voidaan käyttää hyväksi tulevissa asennuksissa ja vielä sitäkin hyödyllisempää, käyttää tieto tulevissa arvioinneissa ja keskusteluissa asiakkaiden kanssa, mitä laitetta käyttää.</p> <p>Vastaavia arviointeja voidaan myös suorittaa muille tietoturvalaitteille eri hyökkäys-vektoreilla. Raakadatan keräys- ja vertailuprosessit pitää jalostaa tulevia projekteja varten.</p>		
Avainsanat (Cyber-Security , threat prevention , email security)		
Muut tiedot		

Acronyms

ARPANET	Advanced Research Projects Agency Network
ASCII	American Standard Code for Information Interchange
CEO	Chief Executive Officer
CPU	Central Processing Unit
DDOS	Distributed Denial-of-Service
DEC	Digital Equipment Corporation
DLP	Data Loss Prevention
DOS	Denial-of-Service
EEST	Eastern European Summer
EEST	Eastern European Summer Time
FTP	File Transport Protocol
GB	Gigabyte
HTML	HyperText Markup Language
IETF	Internet Engineer Task Force
IMF	Internet Message Format
IOC	Indicators of Compromise
IP	Internet Protocol
ITOC	Information Technology Operations Center
KB	Kilo Byte
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MTA	Message Transfer Agent
PB	Petabyte
RADIUS	Remote Authentication Dial-in User Service
RFC	Request for Comments
SCP	Secure Copy Protocol
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
TB	Terabyte
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator

Contents

1	Introduction	6
1.1	Objective of the research	9
1.2	Research method	10
1.3	Research questions	10
1.3.1	Threat prevention capabilities	10
1.3.2	Work needed for setting up the system.....	11
1.3.3	Administration of the device	11
1.3.4	Reports, logging and device polling	11
1.3.5	Local vendor support	12
1.3.6	Cost of device compared to benefit.....	13
1.4	Structure of thesis.....	13
2	Theory background	14
2.1	SMTP protocol	14
2.2	Message format	17
2.3	Types of attacks used with emails	18
2.3.1	Spam	18
2.3.2	DDoS Attack (email bomb).....	19
2.3.3	Malware	20
2.3.4	Phishing.....	22
2.3.5	Spoofing	23
2.4	Email security in the future	23
3	Research	25
3.1	Environment	25
3.1.1	Platform type, virtual vs. physical	26
3.1.2	Mail flow	26

3.2	Types of threat prevention on platforms.....	27
3.3	Focus on advanced threats	28
4	Research results.....	29
4.1	Vendor results	29
4.2	Types of threats in the email attack vector	31
4.3	Vendor 1	35
4.3.1	Summary.....	35
4.3.2	Installation	35
4.3.3	Administration, logging, reporting and polling.....	36
4.3.4	Malware prevention	37
4.3.5	Malicious URLs	38
4.4	Vendor 2.....	40
4.4.1	Summary.....	40
4.4.2	Installation	41
4.4.3	Administration, logging, reporting and polling.....	41
4.4.4	Malware prevention	41
4.4.5	Malicious URLs	43
4.5	Vendor 3.....	44
4.5.1	Summary.....	44
4.5.2	Installation	45
4.5.3	Administration, logging, reporting and polling.....	45
4.5.4	Malware prevention	46
4.5.5	Malicious URLs	48
4.6	TOP Malware discovered during research	49
4.6.1	JS.Downloader.D	49
4.6.2	Ransom.Locky	50
4.6.3	Trojan.Pidief.X.....	50

4.6.4	W2KM_DLOADR.LRN	51
4.6.5	Trojan.Gen.7	51
4.6.6	Trojan-Downloader:JS/Locky	51
4.6.7	W97M.Downloader.M.....	52
4.7	Other findings	52
5	Evaluation of results	54
5.1	Summarization of threat results.....	55
5.2	Threat prevention capabilities.....	56
5.3	Work needed for setting up system	57
5.4	Administration of device	57
5.5	Reports, logging and device polling	58
5.6	Vendor support.....	58
5.7	Cost of the device compared to benefit	59
6	Conclusions and discussion.....	60
6.1	General.....	60
6.2	Challenges	61
	References.....	62
	Appendices.....	65

Figures

Figure 1.	Emails per day (B) (The Radicati Group, 2017)	7
Figure 2.	Email users growth (M) (The Radicati Group, 2017)	8
Figure 3.	SMTP communication	16
Figure 4.	SMTP communication result	16
Figure 5.	Outlook Body Format.....	18
Figure 6.	Basic principal of SMTP flow to threat prevention platforms	25
Figure 7.	Attachment disguised with dots – Outlook	33

Figure 8. Attachment disguised with dots using iPhone client	34
Figure 9. Attachment disguised with dots using Webmail.....	34
Figure 10. Threat distribution – TOP10 - Vendor 1.....	38
Figure 11. Threat distribution – TOP10 - Vendor 2.....	42
Figure 12. Threat distribution – TOP10 - Vendor 3.....	47
Figure 13. Virustotal result for hash	53
Figure 14. Summary of Malicious URLs per day	55
Figure 15. Summary of Malware per day	56

Tables

Table 1. Daily Email Traffic (The Radicati Group, 2017).....	7
Table 2. Worldwide email users growth (The Radicati Group, 2017).....	8
Table 3. Threat summary.....	29
Table 4. Threat attachments by extension.....	32
Table 5. Vendor 1 email summary	35
Table 6. TOP 10 Malware - Vendor 1	37
Table 7. TOP 10 Malicious domains - Vendor 1.....	39
Table 8. TOP 5 Top level domains - Vendor 1.....	40
Table 9. Vendor 2 email summary	40
Table 10. TOP 10 Malware - Vendor 2	42
Table 11. TOP 10 Malicious domains - Vendor 2.....	43
Table 12. TOP 5 Top level domains - Vendor 2.....	44
Table 13. Vendor 3 email summary	45
Table 14. TOP 10 Malware - Vendor 3	46
Table 15. TOP 10 Malicious domains - Vendor 3.....	48
Table 16. TOP 5 Top level domains - Vendor 3.....	49
Table 17. Thesis research questions	54

1 Introduction

With the wide variety means of communicating over Internet, email is still the most used tool for communication, almost half of the world population sends/receives emails on a daily basis (The Radicati Group, 2017). However, email being the most popular tool for communication it has its downsides. Looking at the statistics of Statista, their chart showed that of all world email traffic in December 2016 61.33% is spam (Statista, 2016).

Email security has always been an issue with the attackers designing and creating malware, constantly finding new ways to defeat the identification of the malware on threat prevention platforms. This has led to a cat and mouse game between the malware and threat prevention developers. Unfortunately, the malware developers seems to be winning the game. One reason is for sure, that development and results concerning malware is more open. Vulnerability findings and malware development is shared in the malware community and anyone interested in the subject can contribute (Trend Micro, 2016). Where again on the threat prevention side the vendors that develop new technologies are companies and their tools the company's intellectual property that they do not want to share, because sharing would mean losing business and money.

Most the emails arriving the email gateway of a company is spam or otherwise undesired. There is a need for a reliable device that can be trusted to filter undesired and malicious emails before they end up in the user's mailbox. Even then, the users should have been educated on email security and how to recognize suspicious emails and not to open attachments or click on URLs of those that are suspicious. Also education how to react and do if you click on these malicious emails to avoid causing more damage. How can incoming email be trusted and not be of malicious type; the answer is, it cannot be. There will always be fraudulent and malicious emails passing through any number of security controls. It helps if the prevention platforms identifies and mitigates 99.99% of the malicious emails and the last 0.01% is prevented from being executed. This can achieved by educating the personnel in email security.

There are numbers of companies that does research on the total number of emails and forecasts for the coming years. Just to give an idea how much traffic email generates, table 1 presents a report by Radicati Group Inc. that does quantitative and qualitative reports on different Internet based activity for example security, email, instant messaging (The Radicati Group, 2017) .

The Radicati Group Inc. does statistical analysis, and once per year publishes a new report on email statistics. This year it is named “Email Statics Report, 2017-2021”. In that report, they estimate that the daily emails will grow accordingly to the table and chart below (see Table 1 and Figure 1).

Table 1. Daily Email Traffic (The Radicati Group, 2017)

Daily Email Traffic	2017	2018	2019	2020	2021
Total Worldwide Emails Sent/Received Per Day (Billions)	269	281.1	293.6	306.4	319.6
% Growth		4.5 %	4.4 %	4.4 %	4.3 %

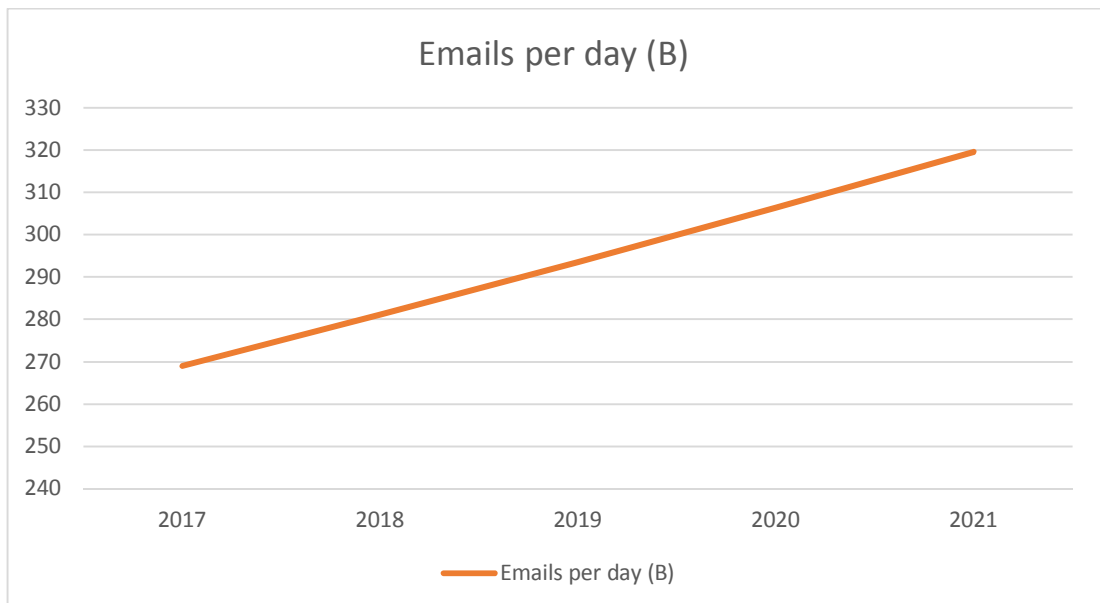


Figure 1. Emails per day (B) (The Radicati Group, 2017)

The same report estimates total of 3.7 Billions email users, meaning half of the world population. The chart shows how the estimated grow for 2017-2021 (see Table 2 and Figure 2) (The Radicati Group, 2017).

Table 2. Worldwide email users growth (The Radicati Group, 2017)

	2017	2018	2019	2020	2021
Worldwide email users (both business and personal) (Millions)	3718	3823	3930	4037	4147
% Growth		3 %	3 %	3 %	3 %

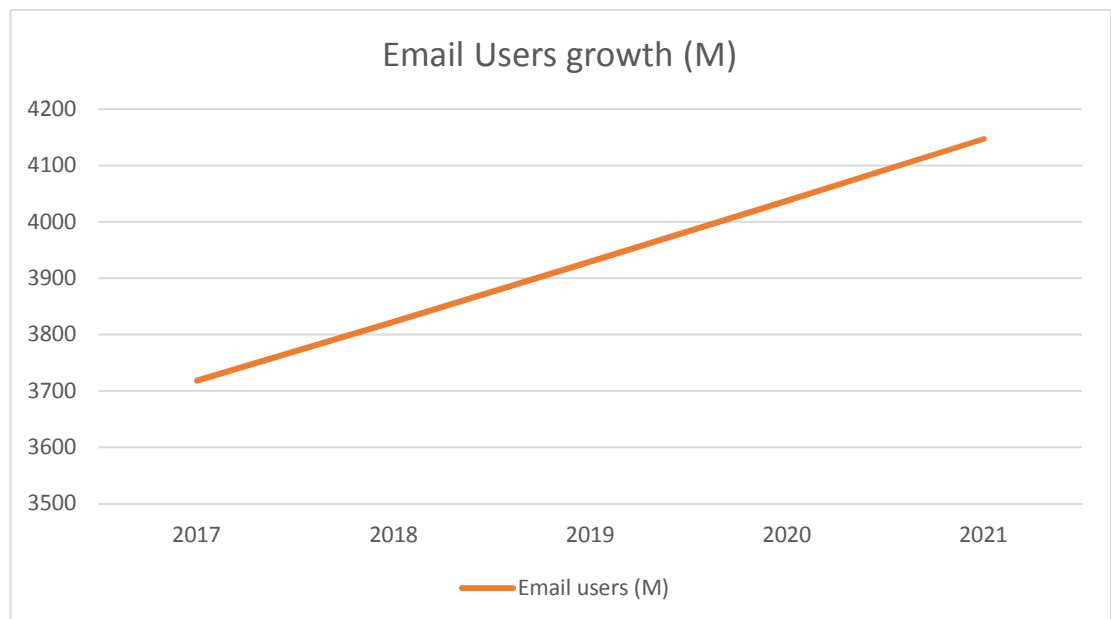


Figure 2. Email users growth (M) (The Radicati Group, 2017)

The report discusses email threats and reports that attacks are still growing although threat prevention is more effective than before. The most used attack is blended attack, where there can be multiple methods of delivering the malware. Blended attacks usually start with an email and then with user (victim) interaction for example clicking a link triggers the malware (The Radicati Group, 2017).

1.1 Objective of the research

The objective of the thesis is to create a more secure environment for handling incoming and outgoing email traffic. This will be achieved by implementing new threat prevention platform(s) in the existing or new email environment.

Threat prevention capability is the primary objective of the thesis research, however, there are other factors as well; also, the cost and labor are to be considered. Is the most expensive platform the best? Alternatively, are similar results achieved with a cheaper one? Are the platforms easy to set up and administer for the device life cycle? In addition, other considerations will be in more detail in chapter 1.3 Research questions.

In the thesis, three different vendor's threat prevention platforms will be compared on threat blocking performance as well a comparison on the other research questions. The platform was chosen based on what platforms Cygate offers customer as an on-premises hardware/virtual email threat prevention platform. All platforms have MTA capability so they could also be set up in a new environment without an existing email gateway.

The author has been working with email gateways and security platforms for more than eleven years, and bringing an extra layer of security, be that physical or cloud based solution preventing threats in emails is the next step in stopping malware and cyber-crime on the email attack vector.

For a theoretical basis, the thesis uses vendor documentation, white papers as well as Internet based writing.

For the implementation part, the setup of the threat prevention platforms was placed and installed in Cygate's environment and live email traffic streamed to each of the solutions for comparison purpose. The concrete results of thesis research were to be the comparison of the different vendor platforms on how they identify, mitigate and report threats. The other research questions were also to be assessed and rated. Cygate can use the results when making security proposals and new email threat prevention platform installations for their customers.

1.2 Research method

The research was based qualitative research method, in more specific a collective case study. The question is what would be the suitable threat prevention platform would be when threat prevention capabilities, price, vendor support, logging, reporting, administration and work setting up the vendor device are to be considered. The implementation could be to an already existing environment with threat prevention capabilities such as a second line of defense or an environment with no existing threat prevention capabilities.

1.3 Research questions

To benefit from the study and to produce something Cygate Oy can use, the following research questions were identified. The device/vendor needs to answer these questions:

- how good is the device at mitigating advanced threats?
- how much work is needed to set up the device?
- how is the administration set up for day-to-day use?
- what are the capabilities of the logs, reports and polling the platform?
- what is the support level of the local vendor?
- does the cost of the device sum up to capabilities?

1.3.1 Threat prevention capabilities

The most important requirement in this thesis research is the capability to mitigate advanced threats. . As live email traffic is streamed through the thesis research environment, there is not a 100% assurance all threats are mitigated. There is always a chance that there is a new virus, Trojan or some other malicious code sent in the mail body, attachment or as an URL in the email. By comparing the results, this study can establish which of the platform identifies and mitigates the advanced threats most efficiently. The research data for the three-vendor platform comparison was to be gathered from the device logs and then harmonized. The threat prevention was to be rated using a five-level scale:

- poor

- fair
- good
- very good
- excellent

1.3.2 Work needed for setting up the system

How much work and configuration is needed to get the system from factory default to the state it is blocking threats efficiently? The time in hours or days will not be recorded for how much is used on getting the system running but rather just rate the work needed using a five-level general scale:

- very easy
- easy
- normal
- hard
- very hard

1.3.3 Administration of the device

The administration of the device is important for Cygate. Cygate offers threat prevention platforms as a service. In addition, Cygate ITOC or other specialists handle the change requests (Cygate, 2017). To minimize costs and work, the devices need to be easily administrated, and minimum effort should be needed to understand the functionalities. The rating was to be done using the author's personal view of setting up the device in the thesis environment. The author has a long history with installing and setting up threat prevention platforms. A five-level general scale also rates the administration of the device:

- very easy
- easy
- normal
- hard
- very hard

1.3.4 Reports, logging and device polling

To automatize alerts, ticketing, and only bringing up the vital information for Cygate ITOC 24/7 polling, the health of the platform is extremely important. The logging can

be an important key feature when determine root cause for issues. It can also be regulated by a law, or the customer's requirement that logs are stored for a certain period. The reports are a good tool to provide information about the platform and the environment to the customer. The reports can be used to determine if the system needs to be tuned in either direction, to tighten or loosen the security controls. The log, reporting and logging capability of the three-vendor platforms were compared with each other. Reports, logging and polling were rated using a five-level scale:

- poor
- fair
- good
- very good
- excellent

1.3.5 Local vendor support

As depicted from previous experience, good local vendor support is very important. The local team can help with issues and give good advice for setting up the system. The local team usually arrange workshops and give valuable training. The local team can also introduce new features and roadmaps. Local vendor support can also help and instruct in the local native language, which is a great advantage and helps with having less problems in miscommunication. Most of the vendor platforms that Cygate offers and supports have local vendor support; however, there are also vendors lacking this support. A key aspect of the professional services, ITOC and other specialist that work with the specific vendor and platforms when a problem arises, is how fast the problem can be solved. If the service providers cannot solve the problem, they rely on the vendor support. If the vendor support is lacking or insufficient due to slowness or incompetence of getting the problem solved, the customer relations could be damaged. This type of issues can also lead to a situation that company elements that set up the platforms will start avoiding the use of the specific platforms and vendor. This rating will be more of a personal view on the vendor's support capability as well as the author's own history operating with the vendors. The author has personal experience of the support they offer and produce with all three vendors in Finland. He has personally opened tickets with every vendor

regarding issues or asking for help with their products. The vendor support will be rated by a five-level scale:

- poor
- fair
- good
- very good
- excellent

1.3.6 Cost of device compared to benefit

The device price in the thesis analysis ranges from moderate to expensive. Can a device that is considerable more expensive make up for the price in performance and threat mitigation compared to the equivalent cheaper model? The rating here is not calculated with any formula but more using a personal view against the cost of the device and threat mitigation capability. The cost/benefit ratio will be rated using a five-level scale:

- poor
- fair
- good
- very good
- excellent

1.4 Structure of thesis

The thesis is divided into four parts. The first part, starting with Chapter 2 goes through the theory of email, email security and attacks used in emails. The second part starting with Chapter 3 contains the actual research, introducing threat prevention types and the thesis research environment. Part three, Chapter 4, presents the results of the vendor platforms. In the final part, Chapter 5, the conclusions of the thesis are presented and the research questions are answered.

2 Theory background

Electronic mail, better known as email, is built on two base pillars, RFC 5321 and RFC 5322. The first, RFC 5321 SMTP protocol, explains how the message is transported over the network, and RFC 5322 Internet Message Format explains how the actual email is built; e.g. text, sender, receiver, subject and email body. The purpose of SMTP is to transmit mail reliably and efficiently over networks (Klensin, 2008). The email message IMF constrained of standards of the message syntax, describes how the IMF is composed (Resnick, 2008). There are several other RFCs that are needed for today's email communications, such as RFC 5322 which takes no provision in sending other than plain text (ASCII), e.g. images, audio and other structured data are not covered in this RFC (Resnick, 2008). For other mentioned media in messages there are other RFCs, such as the MIME document series, RFC 2045, 2045 and 2049 that explain the syntax for building messages, including images and audio (Resnick, 2008).

2.1 SMTP protocol

SMTP protocol is based on the RFC 5321 and the RFC explains how to transmit mail reliably and efficiently over networks. One of SMTP's most important features is the capability to deliver emails over networks. This feature is called SMTP mail relaying, which means that emails can be sent through relays and not just point-to-point, making it possible to send an email from one end of the Internet to the other using intermediate networks and relays in between. The SMTP protocol uses TCP port 25 (Klensin, 2008).

SMTP can also be secured by TLS, known as SMTPS. SMTPS uses the same TCP port 25. TLS is used to protect the data flow of SMTP, meaning that the client and server can start their initial communication using TCP 25 on the application layer, initialize STARTTLS and after securing the communication channel they then start to transfer the data (Hoffman, 2002).

SMTP is a text-based, connection-oriented protocol where the client communicates with the server utilizing command strings and issuing necessary data over a reliable

data stream channel, usually TCP. The SMTP sessions are built up on three command/reply phases (Klensin, 2008):

- MAIL
- RCPT
- DATA

MAIL is where the return path is established, also known as the return-path, mfrom, envelope sender or bounce-address (Klensin, 2008).

RCPT is where the recipient of the message is established. This command can be used multiple times creating multiple recipients for the same email (Klensin, 2008).

The DATA part is where the actual content of the email is defined. The DATA part is divided into two parts, message header and message body. An empty line separates the header and body part. As from the example below can be seen, the subject is injected to the message header part followed by an empty line, and then the text is inserted to the message body. The DATA end is signaled by the '.' (dot). The message can either be accepted or rejected after the end signal, depending on the email server settings (Klensin, 2008).

Connecting to a mail server on port 25, the following commands to send an email can be issued. The same example is used as an example in 2.4.5 Spoofing. From the command/reply phase, all three parts are used to send a basic email. The communications starts with the command HELO. The HELO or EHLO is for the client and server to introduce themselves to each other. In this case the test communication introduces itself as "mailgw.test.fi".

HELO mailgw.test.fi

MAIL FROM: therealpresident@usa.com

RCPT TO: anders.skogster@cygate.fi

DATA

Subject: presidential information

This is a test mail for Anders

.

Here is when it is used against an email server (see Figure 3).

```

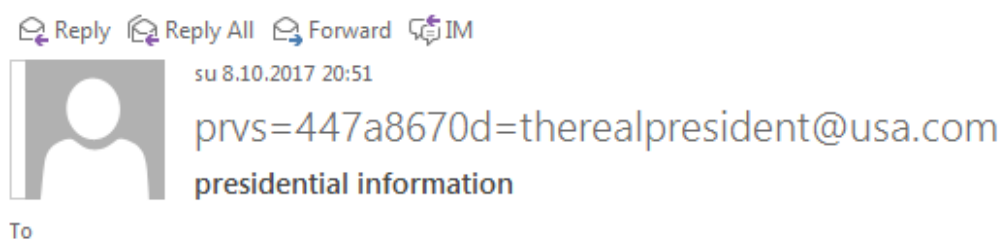
Connected to 81.20.229.20.
Escape character is '^]'.
220 smtpgw1.cygate.fi ESMTP
HELO mailgw.test.fi
250 smtpgw1.cygate.fi
MAIL FROM: therealpresident@usa.com
250 sender <therealpresident@usa.com> ok
RCPT TO: anders.skogster@cygate.fi
250 recipient <anders.skogster@cygate.fi> ok
DATA
354 go ahead
Subject: presidential information

This is a test mail for anders
.
250 ok: Message 79552 accepted

```

Figure 3. SMTP communication

As can be seen, the SMTP commands were accepted, and the email was sent and received (see Figure 4).



This is a test mail for anders

Figure 4. SMTP communication result

As can be seen from figure above the communication was successful and a “spoofed” email was delivered from ‘therealpresident@usa.com’. The email was

successfully received because of how the email gateway was configured and same result cannot be guaranteed if sending through another email relay. The extra “prvs-44a8670d=” in front of the sender is from a configuration called bounce verification option that is configured on the email gateway (Cisco, 2014).

2.2 Message format

The Email Message Format bases on RFC 5322 and describes all rules and regulations on how the message format should be composed, all from line length limits, header fields, body message syntax and much more (Resnick, 2008). The IMF consists of two major components, the message header and the message body. The header is built upon blocks as (Resnick, 2008):

- From
- Date
- To
- Subject
- CC

These are familiar to anyone who has composed an email. There are many more headers than these and one can create one’s own custom headers to store a value or trigger. These header blocks are used to get the email successfully delivered to the correct recipient, and to make sure that the recipient can respond to the email and that it finds its way back (Resnick, 2008).

The body part is where the actual email message resides. The body part also contains a signature part on the bottom. The body part was originally designed for 7-bit ASCII. Later, the MIME standard was introduced enabling non-ASCII use. Modern email client allows the user to choose between plain text or HTML format in body. The figure below shows Outlook options for the body format (see Figure 5).

- HTML
- plain text
- rich text

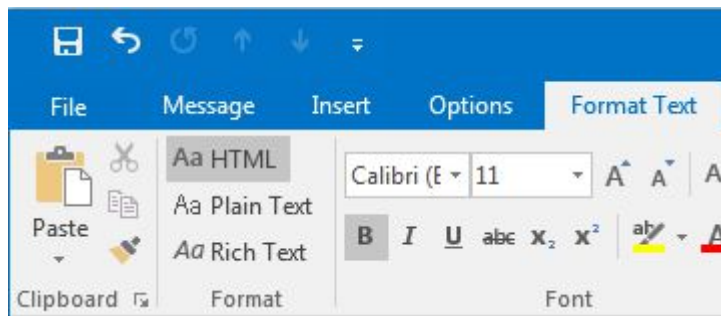


Figure 5. Outlook Body Format

There are advantages of using HTML format, as pictures, HTML content, URLs, font styles and much more. The disadvantage of course is that the email is easier to use for malicious purpose as sending malicious URLs, abuse of HTML code (Resnick, 2008).

2.3 Types of attacks used with emails

In the next part, attacks are introduced, that are encountered in the email attack vector. These type of attacks can be identified and mitigated with the email threat prevention platform. Attacks most likely to be encountered in the thesis research include (GetCyberSafe, 2017):

- spam
- DDOS-attack
- malware
- phishing
- spoofing

2.3.1 Spam

Spam is surely common to all email users. Spam is junk mail, i.e. emails sent in bulk to thousands of users promoting a site or advertising products. The email could be about “How to make money fast”, “Pills that will grow your..” and other great offers that are too good to be true. The reason why spamming still is an ongoing problem is that spamming is a way to make money. If same email to enough people, someone will visit the site, or buy the product (Hambridge & Lunde, 1999). Although most the spams are harmless and do not cause any problems other than filling the mailbox,

there are also ways of making spam nasty. Spam can be infected with malware or malicious URLs can be inserted to a site that infects users' computers, or so much spam can be sent that a volumetric attack is created. DEC (Digital Equipment Corporation) sales representative Gary Thuerk sent the first spam in ARPANET in 1978. This spam was sent to approximately 400 ARPANET users (Luther, 2010).

2.3.2 DDoS Attack (email bomb)

Performing a successful DDoS attack today using emails is not an easy task. The emails are relative small in size, and emails gateways specialized in recognizing and dropping unwanted emails. It is still a possible and widely used email attack format because of its simplicity. If an organization or a company is using old technology and hardware the likelihood of getting successfully attacked is more likely (CERT, 2017a). A DDoS using spam/emails is known as email bomb. There are three ways to deliver an email-bomb (TheWindowsClub, 2017):

- mass mailing
- list linking
- ZIP bombing

In mass mailing, the attacker usually targets a single or multiple email addresses to mass mail. For sending the emails, zombie botnets are used (TheWindowsClub, 2017).

In link listing, known as "email cluster bomb", the victim email address is signed to several email list subscriptions that the user then has to unsubscribe. The subscription process can be done manually or with scripts. Scripts, of course, are more effective. Most of the email subscription lists require the users to confirm the email, however, even these confirmation emails count as an attack (TheWindowsClub, 2017).

Zip bombing, also known as zip of death is not a big threat for today's threat prevention platforms due to their processing power and ability to recognize a zip bomb. The zip bombing bases on compressing a file containing millions and more characters of a specific letter or number. Any other compressed random data could

also be used. The compression makes the file really small; however, on decompression, the file size is huge and requires from the threat prevention platform a huge load of free memory and disc space to handle the file. The decompression usually leads to a system failure due to insufficient resources to handle the file. A known example of the zip bomb is the file 42.zip. This file is a compressed file and contains 42,374 bytes of compressed data, in five layers of compressed zip files in sets of 16 as illustrated below (CERT, 2017a):

$16 \times 4\,294\,967\,295 = 68\,719\,476\,720$ bytes (~68GB)

$16 \times 68\,719\,476\,720 = 1\,099\,511\,627\,520$ bytes (~1TB)

$16 \times 1\,099\,511\,627\,520 = 17\,592\,186\,040\,320$ bytes (~17TB)

$16 \times 17\,592\,186\,040\,320 = 281\,474\,976\,645\,120$ bytes (~281TB)

$16 \times 281\,474\,976\,645\,120 = 4\,503\,599\,626\,321\,920$ bytes (~4.5PB)

The bottom layer contains 4.3GB file and totals to 4.5 PB. The 42.zip can be downloaded at <http://www.unforgettable.dk>. There are even YouTube videos on uncompressing the 42.zip showing the Windows machine to crash. Just open YouTube and search for 42.zip (CERT, 2017b).

2.3.3 Malware

Malware can be broken down into multiple threats that can be delivered by emails trough (Phifer, 2010):

- virus
- Trojans
- worms
- malicious URLs

Computer viruses are very common and can be encountered on a daily basis in emails if not filtered. Now and then, a virus sneaks through the threat protection platform and causes trouble. The mission of a virus is to infect and replicate itself once executed. The infection usually means the virus inserting its own code in other programs. A successful virus is one that can infect the system, replicate itself and then infect other system without being detected. Usually viruses also have some kind

of an agenda: ransom, spying, sabotage, personal amusement, political agenda or other purpose. The virus business today is blooming and causes billions of dollars of damage annually. Constructing a virus today is very easy, no knowledge of coding is required. Tools can be used to modify existing viruses to a new variant and one's own agenda can be inserted in it (F-Secure, 2017a).

Trojan or Trojan horse are malware disguised to pose as valid software. In email-based attacks, Trojans are delivered as attachments and the malicious payload is executed as soon as it is opened. Trojans have a slightly different action or agenda compared to viruses. Trojans usually insert themselves to the system and work as backdoors to the infected system. Other actions can include (Kaspersky, 2017:

- removing data
- transferring data
- modifying data
- blocking data
- interfering with network communication or computer performance

Trojans cannot self-replicate as viruses and worms. There are many different types of Trojans and they have been categorized by the type of action they perform. These are some of the subtypes (Kaspersky, 2017):

- backdoor
- exploit
- rootkit
- Trojan-Banker
- Trojan-DDOS
- Trojan-Downloader
- Trojan-Dropper
- Trojan-FakeAV
- Trojan-Gamethief
- Trojan-IM
- Trojan-Ransom
- Trojan-SMS
- Trojan-Spy
- Trojan-Mailfinder

Worm is a malicious computer program, the only purpose of which is to replicate itself and spread to other networks and computers. With the replication and spreading, the worm always create problems for the victim and network by consuming network bandwidth and computer processing power. The worms spread by exploiting the operating system and program vulnerabilities. The worms can also

carry a payload for dropping onto the infected system. This payload can be a ransomware or some malware to create a backdoor to the system (F-Secure, 2017b).

Malicious URLs are URLs that when visiting drop malicious content through exploits and vulnerabilities in a browser or browser plug-in. Once the malicious site has been entered, the site will collect as much data as possible from the victim. Based on the information the site will try to push a malware to the victim. Even a short visit to the compromised site can infect the computer even if links are not pushed, or nothing is done on the site. The malware will use the exploits and self-execute as soon as it has infected the system (Symantec.com, 2017a).

2.3.4 Phishing

Phishing is a targeted attempt to collect information and infect a victim. A phishing attack is usually a targeted attack at a certain group, company or even individuals. This also means the malware used is especially picked and chosen for the group, company or individual making the attacks more precise, and the success rate in them is much higher than with other attacks. Phishing also contains social engineering elements making the attack more personal. In phishing, there are several different types of phishing (PhishingBox, 2013):

- spear phishing
- clone phishing
- whaling

Attacks on individuals and companies are referred by spear phishing. Gathering of personal information is a pre-part of the attack (PhishingBox, 2013).

In clone phishing the attacker clones a previously sent email and changes the URLs or/and attachments with malicious ones and sends the email again, claiming it as a resend because the previous email was missing some information (PhishingBox, 2013).

Whaling is where the attacker only targets users such as CEOs, executives in high posts or other high-profile users that can have valuable information to extract (Cain & Jevans 2010; PhishingBox, 2013).

2.3.5 Spoofing

In email spoofing an email is sent in someone else's name. Email protocol does not have any means for authentication, so sending an email in someone else's name is easy (Ferguson & Senie, 2000). Only access to an email server is needed and anyone's name can be entered as the sender, e.g. taking a 'telnet 25' connection to the email server. Below is demonstrated how it can be done:

```
HELO mailgw.test.fi
MAIL FROM: therealpresident@usa.com
RCPT TO: anders.skogster@cygate.fi
DATA
Subject: presidential information
```

This is a test mail for Anders

.

The SMTP communication was showcased in Chapter 2.1 SMTP Protocol.

To make it even easier, one just needs to have an email client available to use for entering the sender, recipient, body text and attachments.

Spoofing the client-IP is more tricky. The SMTP protocol is TCP-based, i.e. there is two-way communication, when setting up the connection. If the spoofed IP does not respond to the TCP session handshake, the connection is dropped (CERT, 2017c). By the use of software or services, you will be able to hide or change the IP. Some examples for hiding or changing IPs are the use of:

- proxy-servers
- VPN-tunneling programs e.g. NordVPN and F-Secure Freedome
- network address Translation (NAT)
- use of dark web, e.g. Tor and Freenet

2.4 Email security in the future

As already observed, more and more of the today's email security and threat prevention is moving towards the cloud. The need of an on-premises device is no

longer necessary; both email relay, and email security can be handled as a service from the cloud. All of the major vendors offer email MTA service as a cloud service, and the threat prevention can be handled in the cloud. One of the best-known cloud based email services is Office 365 email. Office 365 is Microsoft's email service, i.e. the Exchange server in the cloud acts as a shared service from Microsoft. Microsoft also offers its O365 users Office 365 Advanced Threat protection. This offered service mitigates basic and advanced threats that targets the email users (Microsoft, 2017).

The advantage of a cloud-based service is, of course, that there is no need to maintain any platforms or threat configurations. As a cloud resource and used as a service, the email service should always be available without interruptions. On the other hand, the responsibility of the threat identification and mitigation is given to an outside party. Of course, a hybrid solution can be run where email is handled in the cloud and all emails are relayed through the own threat prevention platform before the delivery to an end user (Coolhead Tech, 2014).

The time for on-premises email threat prevention platforms is not over yet, however, they will need to make room for the cloud-based solutions.

3 Research

The thesis research is conducted by building identical threat prevention setups. The easiest way to achieve this is by setting up all the threat prevention platforms in parallel and sending the same SMTP traffic flow through each one. With this setup, all platforms will be exposed to the same flow, and threats and results are comparable. Below is a simplified figure to visualize the thesis research setup (see Figure 6).

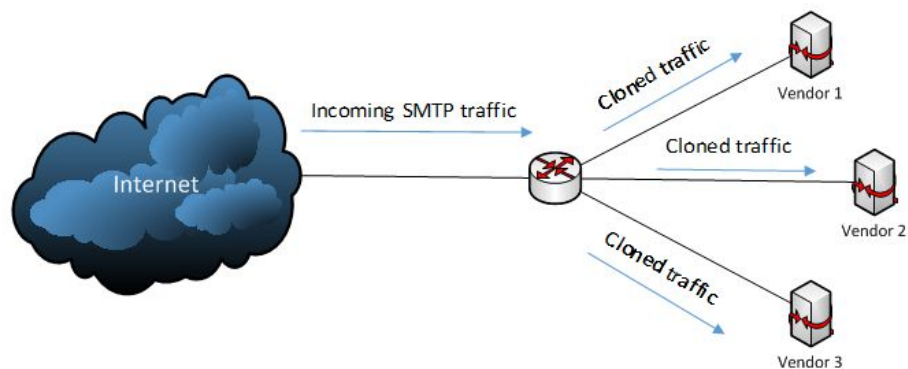


Figure 6. Basic principal of SMTP flow to threat prevention platforms

The platforms are exposed to the same SMTP traffic for the duration of ten days, after which the data is collected and analyzed. The data consists of the platforms logs and reports.

3.1 Environment

For implementing the thesis research, three different vendor platforms were chosen from Cygate's product portfolio. Due to non-disclosure agreements between Cygate and the company's vendors, the results of the platform with the vendor specific

threat name or the vendor or platform name cannot be used in the thesis. Instead of naming the vendors and proclaiming which of the brands is the best, the focus is on the way threats can be identified and mitigated, and which of the platforms uses its functionalities best. The results are to be published without the vendor or platform name.

3.1.1 Platform type, virtual vs. physical

The platforms used in the environment are both virtual and physical based servers. Both virtual and physical based platforms have the same functionalities if comparing the vendor's virtual version and physical version. For setting up the thesis environment, the virtual platform are much easier to set up. Below are some examples why (RoseHosting, 2016):

- no need for rack space, power or cabling
- no physical installation
- evaluation licenses easier to obtain
- backup snap shot easy to take and rollbacks are fast and easy
- faster to deploy and decommission afterwards

3.1.2 Mail flow

The mail traffic used for the thesis research was from Cygate, i.e. in other words, the emails that were analyzed in the thesis environment were emails that was received by Cygate's own email gateways. The emails were cloned on the incoming email gateway and sent to the three thesis platforms before any blocking decisions were made. The thesis environment platforms all received the raw flow of Cygate emails at the same time. The benefit of using real email flow instead of fabricated email flow in a lab environment is that the incoming types of malicious emails cannot be predicted, and they correspond to the current malicious emails used in today's attacks. The email flow to the three vendors was carried out for the period of 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST. The mail flow for the specified period included roughly 30,500 emails.

3.2 Types of threat prevention on platforms

An email threat prevention platform can identify and mitigate threats with numerous technologies. Below, the most common ways of identifying malicious emails are listed.

- antivirus scanning
 - one engine
 - multiple engines
- spam scanning
- IP-reputation
- file-reputation
- URL-reputation
- URL-categorization
- URL-databases
- URL-scanning
- sandboxing
 - on premise
 - cloud based
- content filters
 - message filters
 - custom written triggers and actions
- dictionaries and heuristics
- outbreak warning
- Data Loss Prevention (DLP)
- domain Keys and other signing keys
 - DMARC
 - sender ID
 - DKIM
 - SPF
 - certificates
 - personal signing keys
- encrypted connections
- bounce verification
- mail-account check
 - verify against local database
 - check against LDAP or Active Directory
 - check against outside 3rd party database

Most vendors use all the mentioned or a set of the mentioned technologies to identify and mitigate threats. For a vendor to stand out in the competition, they usually have a vendor-specific technology to make them “better” than the competition and use that as the selling argument when talking to customers.

3.3 Focus on advanced threats

As from the previous listing can be seen, there are many ways to identify and mitigate attacks. The three vendors chosen for the thesis research have their specific technology that makes them better than the others. The better part is biased, it is used by the vendors themselves and their own claims when comparing themselves to the competitors. With vendor-specific technology the study refers to the vendor that is superior in sandboxing as the other vendor is more focused on IP/File/URL reputation. This also meant that comparing the results could be difficult. To even the game field, the study focused more on the vendor's threat prevention ability to mitigate advanced attacks than mitigating spam. This means configuring all three vendors to focus on

- malware
- malicious URLs
- sandboxing

and to skip

- IP-reputation
- SPAM scanning
- dictionaries
- Domain Keys and other signing keys
- mail-account checks
- content filters
- outbreak warnings
- DLP
- URL Categorization (to some part)

The skipped protection types are common for a mail gateway serving as a front line MTA device. By skipping these types of protection, more hits on actual malware are gained, which makes the end-report more interesting. In addition, it helps with the comparison of the threat mitigation between the three vendors.

4 Research results

4.1 Vendor results

All three vendors were exposed to the same mail flow of 30,476 emails between 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST. Below is a summary table of the findings (see Table 3).

Table 3. Threat summary

Time period 6 June 2017 9 p.m. EEST – 14 June 2017 9 p.m. EEST
Total emails: 30,476

	Total Threats	Malware	Malicious URL
Vendor 1	2,199	1,033	1,166
Vendor 2	1991	816	1,175
Vendor 3	1,328	1,046	282

As displayed in Table 3, vendor 1 mitigates the most threats (in numbers), vendor 2 and vendor 3 are behind it, vendor 3 even more than vendor 2. Going into a more detailed analysis, it can be noticed that the numbers are not that important.

Different vendors mitigate threats in different ways, and the numbers cannot really be compared directly. A more detailed cross-reference between the three vendors can be examined in Appendix 1.

The attack timeline can be viewed in Appendix 1 and the verdict of the corresponding vendor of the event. If one of the vendor rows is empty for a certain event, this means the vendor did not identify and prevent the threat that was identified and prevented by another vendor. It can be seen from the summary report that vendor 1 mitigated most threats, i.e. the other vendors have more blank rows. Appendix 1 illustrates that although vendor 1 had the most threat prevention it also has blank lines, which means the other vendors identified threats that vendor 1 did not identify.

Appendix 1 is in a CSV format, and the data table consists of ten fields separated by a semicolon ‘;’ as listed below.

- Time
- Filehash
- Virustotal by Filehash or equivalent
- Vendor 1
- Vendor 2
- Vendor 3
- Attachment
- Malicious URL or domain
- SMTP-From
- Client-IP

“Time” field refers to the timeline for the collection of the data for the thesis from 6 June 2017 9 p.m. EEST to 14 June 2017 9 p.m. EEST. For every threat that was recognized there is an event available.

“Filehash” field, the logs provided a SHA or MD5 filehash for the file if the verdict was threat. The filehash was used to provide a virus name (which is used in the “Virustotal or equivalent verdict” field) for the threat so the original, vendor-specific name could be hidden. Virustotal is a site owned by Google, and it can be accessed at www.virustotal.com. The site offers free online service to analyze files and URLs. After analyzing, the site will indicate what malicious content was identified and offers details about it. Filehash can also be used and that is the function used in the thesis to find an equivalent second-vendor threat name to mask the name of the original threat (Virustotal, 2017a).

“Vendor 1”, “Vendor 2” and “Vendor 3” fields contains the vendor verdict of the threat.

The “Attachment” field, if there was an attachment in the malicious email the filename or filenames will be listed in the field.

The malicious URL or domain that was discovered in the threat will be inserted in the “Malicious URL” or domain” field. The “SMTP-From” field contains the information from who the malicious mail came from? This entry is easily spoofed but still interesting.

“Client-IP” field contains the IP from which the malicious email was sent.

4.2 Types of threats in the email attack vector

In the 30,476 emails analyzed, there were several different viruses, Trojans and other malicious executables. Based on the results, most of the malware is Trojan. The attack pattern for the email attack vector is usually implemented in two ways: emails with malicious attachment or emails with malicious URLs.

- emails with malicious attachment
 - o PDFs
 - o executables

- emails with malicious URLs
 - o full URLs
 - o tiny URLs
 - o spoofed URLs

Besides these attack methods there could also be attacks using social engineering without any actual malware used.

Looking into what kind of attachments are used for delivering malicious content, 1,000 unique files were identified. Despite that, these files all had unique names, many of the files had content, and the malicious payload was the same.

Below is a table of extension used in the files (see Table 4).

Table 4. Threat attachments by extension

Time period 6 June 2017 9 p.m. EEST - 14 June
2017 9 p.m. EEST

Total unique files: 1,000

	Amount	Percentage
ZIP	767	76.70 %
WSF	99	9.90 %
PDF	49	4.90 %
DOC	44	4.40 %
DOCM	21	2.10 %
JS	7	0.70 %
EXE	4	0.40 %
<none>	2	0.20 %
JAR	3	0.30 %
GZ	1	0.10 %
DOCX	1	0.10 %
RAR	1	0.10 %
ARJ	1	0.10 %
TOTAL:	1,000	100.00 %

The most popular file extension as attachment is .zip as Table 4 displays. The other extensions are far behind in numbers. The explanation, why .zip was the most used extension or some other compressed file extension is quite easy. By compressing the file, the attacker tries to prevent any scanner from detecting the malicious payload. Then, when the user opens the compressed file, the malicious content is released and executed resulting in the user's computer being infected and compromised.

A content filter could be created, which would automatically block emails containing attachments with a risky file extension. By doing this, valid attachments that are sent could also be blocked. For example, Symantec has a list of risky extensions that could possible deliver malicious content (Symantec, 2017a).

From all 1,000 unique files that were identified some the files used the actual naming of the file trying to hide its true purpose.

The files:

IMG20170606_004356.jpg.....
.....gz

IMG20170606_004356.jpg.....exe

The files were disguised to look as normal .jpg pictures but used an excess amount of dots after the .jpg..... , and one ending as executable and the other a compressed .gz. By using the extra dots and depending on the client program for viewing and opening the actual email the real extension could be hidden because of the long name, or if the user just quickly looks at the file extension and only notices .jpg he/she might think it is harmless and therefore opens the attachment releasing the malicious content.

To demonstrate this, a non-harmful .jpg with extra dots was sent to the author's email accounts to demonstrate how the attachment looks like.

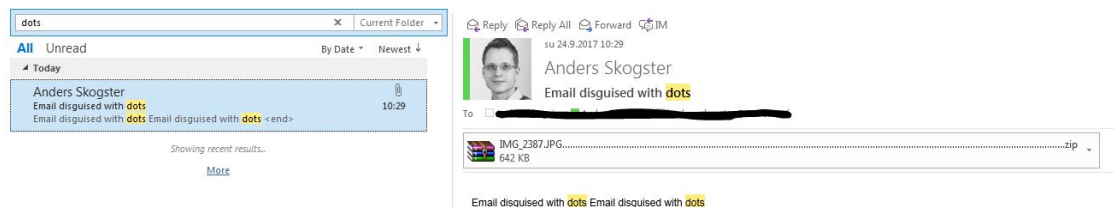


Figure 7. Attachment disguised with dots – Outlook

Outlook client does not really fool anyone. It can be clearly seen that the extra dots end in a .zip (see Figure 7); the same thing with viewing the email on the author's iPhone using the native email client (see Figure 8), and again, the .zip extension is clearly visible.



Figure 8. Attachment disguised with dots using iPhone client

When sent to a web-based client the .zip extension is not seen, not even when the mouse pointer is on the attachment (see Figure 9).

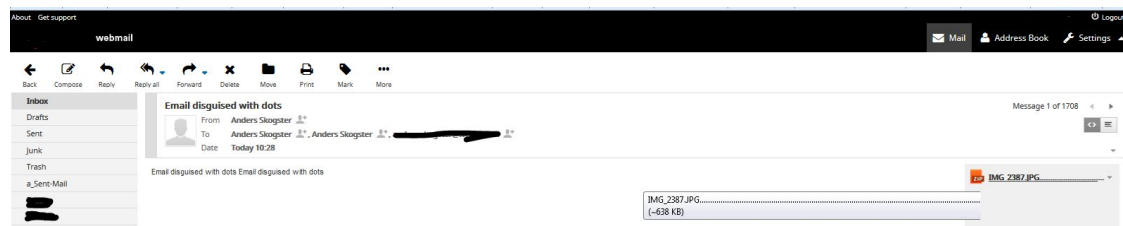


Figure 9. Attachment disguised with dots using Webmail

The email was also sent to Google mail, however, Google blocked the email:

Remote Server returned '<[173.194.222.27] #5.0.0 smtp; 5.3.0 - Other mail system problem 552-'5.7.0 This message **was blocked because its content presents a**

potential\n5.7.0 security issue. Please visit\n5.7.0

<https://support.google.com/mail/?p=BlockedMessage> to review our\n5.7.0 message content and attachment content guidelines. c23si1135925lfh.577 - gsmtp' (delivery attempts: 0)>'

Google blocked the email based on the compressed format (Google, 2017). the extension is renamed toaaa, the attachment is delivered; however, then again, the file is not “executable” anymore and will not automatically open in any program making the file quite harmless, and the recipient will notice the spoof.

4.3 Vendor 1

4.3.1 Summary

Vendor 1's device performed really well. The device identified overall the most threats, summing up malware and malicious URLs. Table 5 illustrates the Vendor 1 email summary.

Table 5. Vendor 1 email summary

Time period 6.6.2017 9pm EEST - 14.6.2017 9pm EEST
Total emails: 30,476

	Total Threats	Malware	Malicious URL
Vendor 1	2,199	1,033	1,166

The findings between threats based on virus, malware signatures and sandboxing compared to malicious URLs were quite close. The sandboxing functionality on the device found 26 medium rated threats in processed emails. Vendor 1 used a pre-defined URL database with URLs and domains to cross-reference to the ones found in emails. The result was good.

The use of a URL database of course relies completely on the integrity and trust of the database publisher.

4.3.2 Installation

The device was easy to set up and the initial installation consisted of the following:

- IP / mask / gateway
- hostname
- DNS / NTP
- license

The actual MTA and mail flow configuration was straightforward. There is comprehensive installation documentation available on the vendor website. The configuration options are good for modifying the mail flow and pre-defined or

custom profiles based on multiple factors (sender, receiver and domain) can easily be assigned to do the desired scans.

The device needs to be configured; it is not a plug and play device. After the set up and configuration it needs to be tested that it works in the desired way. There was a great deal of testing of the malware and malicious URL scanning settings to get to the best results when setting up the thesis environment for the actual analysis.

Plenty of time was used to get the output in a good format and the logs and reports in such syntax that the three-vendor results could easily be compared to each other

4.3.3 Administration, logging, reporting and polling

Once all the initial setup and the actual MTA and mail flow setup was done, the device is easy to maintain. As long as there is no need to change the scanning behavior or new email domains needs to be added, the day-to-day administration stays minimal.

Role-based administrators can be created for specific users on the device.

Scheduled reports can be created and sent to different members of the organization. Moreover, all reports are customizable for creating multi-purpose report content.

The device also supports SNMP queries and traps as well as sending the wanted log with syslog to a server for just log-purpose or a further analysis.

4.3.4 Malware prevention

The threat findings were the results that were most valuable in this research. The presented malware findings are harmonized, and the malware name is presented in other vendor names such as Symantec, TrendMicro, Sophos and more. This will protect the identity of the vendor. If results were presented with the original vendor threat name, it would be easy to figure out the results of which vendors are introduced.

Table 6. TOP 10 Malware - Vendor 1

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST
Total threats: 1033

Malware	Amount	Percentage
JS.Downloader.D	467	45.21 %
W2KM_DLOADR.LRN	98	9.49 %
JS_NEMUCOD.SMK17	79	7.65 %
Trojan.Gen.7	69	6.68 %
W97M.Downloader	41	3.97 %
Trojan.Mdropper	35	3.39 %
JS_NEMU.B2B35B1C	33	3.19 %
TROJ_GENZM.F299E00FB17	30	2.90 %
TROJ_IN.5BD4624C	29	2.81 %
Trojan.Pidief.X	33	3.19 %
Other	119	11.52 %
Total	1,033	100.00 %

Most of the malware identified for vendor 1 is within the list of top 10 threats. Only 11.52% are not among the top 10. (Figure 10)

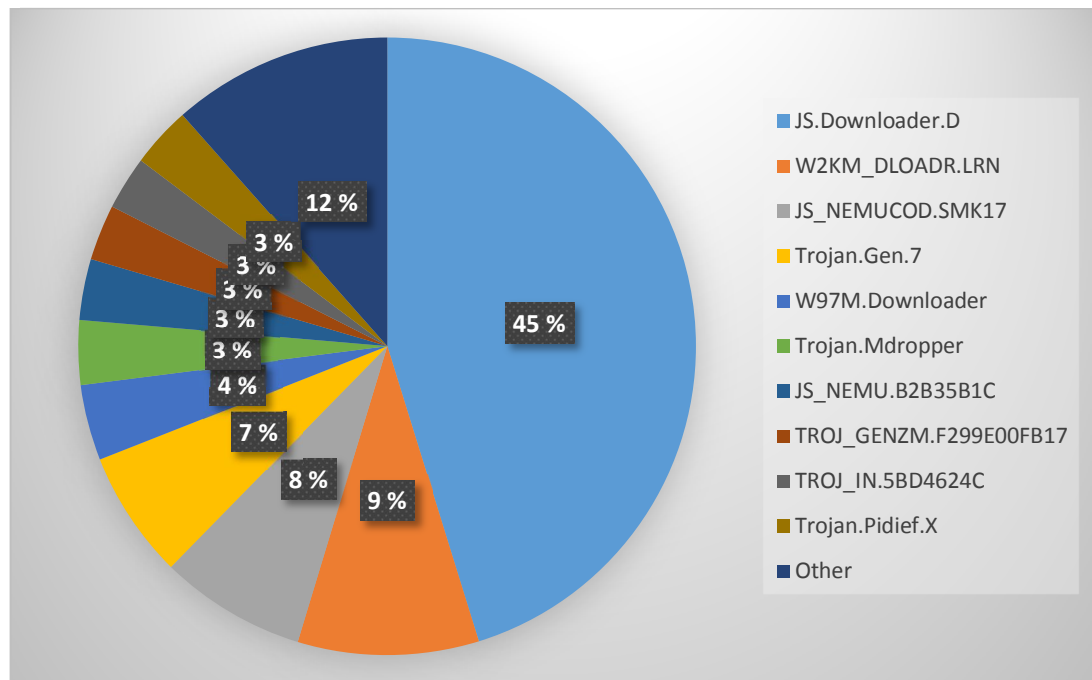


Figure 10. Threat distribution – TOP10 - Vendor 1

Some of the top malware is introduced in Chapter 4.6 'Top Malware discovered during research'. The full list of malware found by vendor 1 is presented in Appendix 1.

4.3.5 Malicious URLs

Vendor 1 was good at identifying malicious URLs. The vendor identified 1,166 threats based on the malicious URL identification. In the conclusion part, the figures will be analyzed in more detail. The data for malicious URLs for vendor 1 is of basic content, the device only logged that the email contained a malicious URL and the URL domain. For deeper analysis of the malicious content, the log and quarantine configuration on the device should have been set up differently. This is discussed later in Chapter 6.1 'Challenges'. All the identified malicious URLs are listed in Appendix 1.

Vendor 1 logged the domain for the malicious URLs, however, if several vendors identified the same malicious URL, Appendix 1 will contain the most detailed URLs available. From the 1,166 malicious URLs, there are only 189 unique domains. Below Table seven presents a breakdown of the domains discovered during the research.

Table 7. TOP 10 Malicious domains - Vendor 1

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST
Total malicious URLs: 1166

Domain	Amount
macartu.cn	159
amino-disqus.club	110
organictabletinc.ru	68
ynlanta.cn	66
medicalrxquality.su	59
medicalrxreward.ru	58
express-catalogs.com	40
marrytags.de	34
sexy-dates.ru	32
smartrxshop.su	26

An interesting detail is that most of the domains end in .com, .ru or .cn, which means that the most of the malicious emails domains are registered as commercial, Russian or Chinese. (Table 8)

Table 8. TOP 5 Top level domains - Vendor 1

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST
Total malicious URLs: 1166

Top level Domain	Explanation	Amount
com	Commercial	337
ru	Russia	255
cn	China	230
club	Brands, clubs, celebrities	110
su	Soviet Union	88

For the full list of malicious emails, please look at Appendix 1.

4.4 Vendor 2

4.4.1 Summary

Vendor 2 performance in overall was also very good. Vendor 2 identified threat emails the other vendors did not. Vendor 2 used virus engines, sandboxing and file reputation to identify threats in the email body, attachments and URLs.

Table 9. Vendor 2 email summary

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST
Total emails: 30,476

	Total Threats	Malware	Malicious URL
Vendor 2	1,991	816	1,175

4.4.2 Installation

The installation of vendor 2 threat prevention platform was easy. The installation guides from the vendor are well written and informative. By following the guides and documentation, the setup can be performed by a user not familiar with the product, however, familiar with similar technology. The basic setup can be done via a wizard, so getting the device installed in the network with basic configuration is really quick. Licenses were easy to obtain and install. Based on the purchased licenses, different threat prevention methods are “unlocked”. After setting up the basic network configuration, the configuration of the handling of the actual mail flow is started. The options for doing some nice tweaks and actions on the mail flow are really good. The downside is that a complex configuration can be created, and it could be hard to read and troubleshoot by another administrator. Vendor 2 configuration needed to be tested and modified several times, for an output that would be comparable by all three vendors.

4.4.3 Administration, logging, reporting and polling

The daily administration tasks on device are done to be easy, and the data is simple to read. There are pre-made administrator roles, read (no editing rights), write (can edit and save configuration) and views for different parts of the configuration, including mail tracking and the results for mail handling. The vendor has configuration tools and actions to satisfy even the most complex configuration setups. The vendor supports basic polling via ping or SNMP traps and/or queries. The vendor creates logs that can be forwarded with syslog or transferred via FTP/SCP for storing or deeper analysis. Automated reports with configured schedule can also be created and developed for different levels of administration.

4.4.4 Malware prevention

As with the previous vendor, the presented malware findings are harmonized and the malware name is presented in other vendor name such as Symantec, TrendMicro, Sophos and more. This will protect the identity of vendor. Vendor 2 had a good identification rate in the malware detection/prevention.

Table 10. TOP 10 Malware - Vendor 2

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST

Total threats: 816

Malware	Amount	Percentage
JS.Downloader.D	297	36.40 %
W2KM_DLOADR.LRN	98	12.01 %
Trojan.Gen.7	69	8.46 %
W97M.Downloader	54	6.62 %
JS_NEMUCOD.SMK17	46	5.64 %
Trojan.Mdropper	35	4.29 %
TROJ_GENZM.F299E00FB17	30	3.68 %
TROJ_IN.5BD4624C	28	3.43 %
Trojan.Pidief.X	33	4.04 %
TROJ_GENZM.F299E00FI17	26	3.19 %
Other	100	12.25 %
Total	816	100.00 %

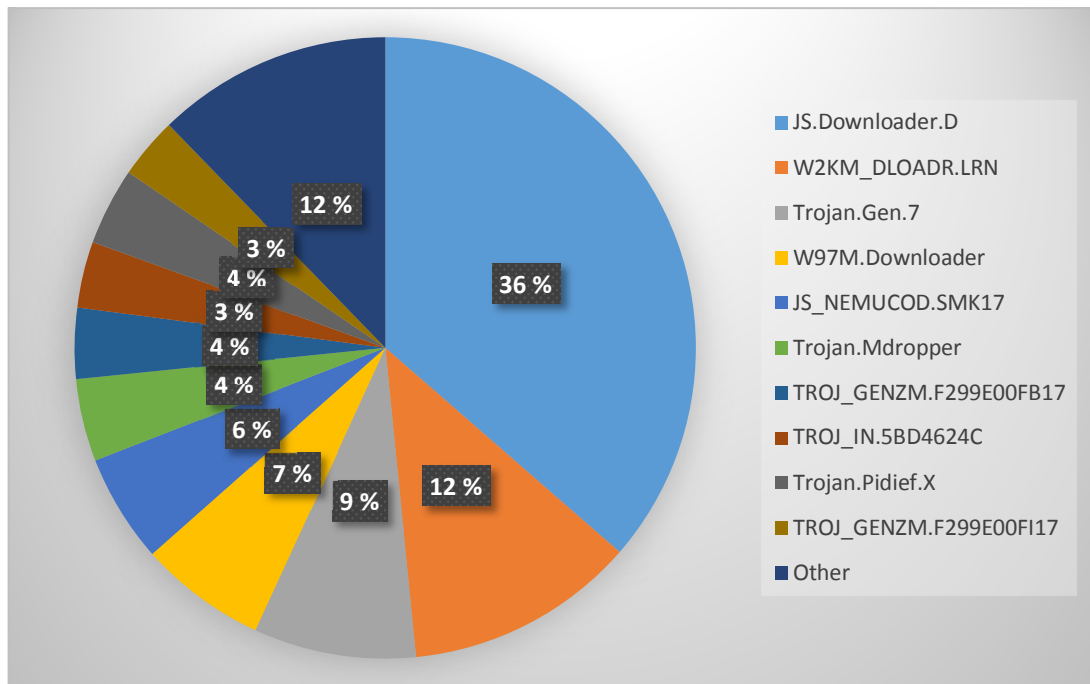


Figure 11. Threat distribution – TOP10 - Vendor 2

As can be seen from the table and chart (see Table 10 and Figure 11), most of the malware items identified are Trojans and recognizable by the malware name. Some

of the malware is introduced in Chapter 4.6 Top Malware discovered during research, for the full list of malware found by vendor 2, refer to Appendix 1.

4.4.5 Malicious URLs

Vendor 2 had a good record on identifying malicious URLs. The vendor identified 1,175 threats based on malicious URL identification. Vendor 2 identified the most threat URLs compared to the other vendors. In the conclusion part, a comparison with other vendor results is presented. All the identified malicious URLs are listed in Appendix 1. Some of the malicious URL addresses are missing from the vendor in Appendix 1. This is due to some of the identification having logging configured differently than other threat identification. What can be extruded from the log is that the URL was malicious; however, no deeper analyze can be concluded. Same as for vendor 1 and vendor 3 if several vendors identified the same malicious URL, the most detailed one is listed. From the 1,175 identified malicious URLs, the URL or domain details are listed for 983. From the 983 URLs or domains, there are only 106 unique domains. Below (Table 11) is a breakdown of the domains encountered.

Table 11. TOP 10 Malicious domains - Vendor 2

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m.
EEST
Total malicious URLs: 1,175

Domain	Amount
macartu.cn	159
amino-disqus.club	110
organictabletinc.ru	68
ynlanta.cn	66
medicalrxquality.su	59
medicalrxreward.ru	58
express-catalogs.com	40
marrytags.de	34
sexy-dates.ru	32
hotcuringbargain.ru	25

Some of the same domains were encountered multiple times, as the table above displays. The reason why the same domain comes up multiple times also depends on how malicious URLs are sent. If a malicious email, for example 100 users are hit at the same time or in the timeline within which the data is collected with the same malicious content, the counter for that domain will go up with 100 since all the malicious emails are counted separately and handled in this thesis as a separate incident. (Table 12)

Table 12. TOP 5 Top level domains - Vendor 2

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m.
EEST
Total malicious URLs: 1,159

Top level Domain	Explanation	Amount
ru	Russia	250
com	Commercial	196
club	Brands, clubs, celebrities	110
su	Soviet Union	88
cn	China	69

In the top level domain breakdown, similar values are seen as in the earlier results. Vendor 2 identified the most malicious URLs with .ru and .com extensions.

4.5 Vendor 3

4.5.1 Summary

Vendor 3 had the least hits on identifying malicious URLs but had the highest rate on malware identification. This is easy to explain because vendor 3 does not use the same tools to identify malicious URLs than the other vendors but rather relies on URL scanning, i.e. it scans what really is behind the URL rather than relying on URL reputation or pre-made URL databases on what is a good or bad URL. This can be seen in the low numbers of malicious URLs identified; however, it also means the URLs that have been identified as malicious really had something bad “waiting”

behind the URL. In just labeling URLs malicious on reputation or pre-made URL databases has a bigger chance of resulting in false positives. The malware identification on the device was really good. (Table 13)

Table 13. Vendor 3 email summary

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST
Total emails: 30,476

	Total Threats	Malware	Malicious URL
Vendor 3	1,328	1,046	282

4.5.2 Installation

Of all the vendors, vendor 3 had the most straightforward approach on the installation. After the basic network setup, the actual mail flow rules on scanning and actions were easy to set up. On the downside, the flexibility and use of complex rules were not possible to achieve. This could lead to that the device is not suitable for all environments. There should be no problems to install the device in simple environments built with good practices. As in the other vendor devices, also vendor 3 has good documentation on installation and administration of the device, the only problem is to find them. To obtain the documentation a registration with the vendor is needed, and even then, their portal is quite a maze.

4.5.3 Administration, logging, reporting and polling

The device administration is made simple, since there are not that many configuration options. Role-based administrators can be created so not every administrator has the same view and privileges. Also, polling and sending logs outside the box is possible; Syslog, SMTP and SNMP both traps and/or queries can be enabled. Events can be sent via http/https if needed, making the event handling better on this device than the others. The reports are visually really good and customizable making the reporting to the different levels of organization very easy.

4.5.4 Malware prevention

Vendor 3 had the best malware identification of all the vendors. Looking at the TOP 10 Malware table and figure (Table 14 and Figure 12) below, same Trojans malware is seen as before in the vendor findings. All the vendors had the same number one malware, JS.Downloader.D –trojan. It needs to be kept in mind that all vendors had the same identical mail flow so the lists should be quite similar.

Table 14. TOP 10 Malware - Vendor 3

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST
Total threats: 1,046

Malware	Amount	Percentage
JS.Downloader.D	467	44.65 %
W2KM_DLOADR.LRN	98	9.37 %
JS_NEMUCOD.SMK17	78	7.46 %
Ransom_.165681C8	66	6.31 %
W97M.Downloader	41	3.92 %
JS_NEMU.B2B35B1C	33	3.15 %
Trojan.Mdropper	31	2.96 %
TROJ_GENZM.F299E00FB17	30	2.87 %
TROJ_IN.5BD4624C	29	2.77 %
Trojan.Pidief.X	33	3.15 %
Other	140	13.38 %
Total	1,046	100.00 %

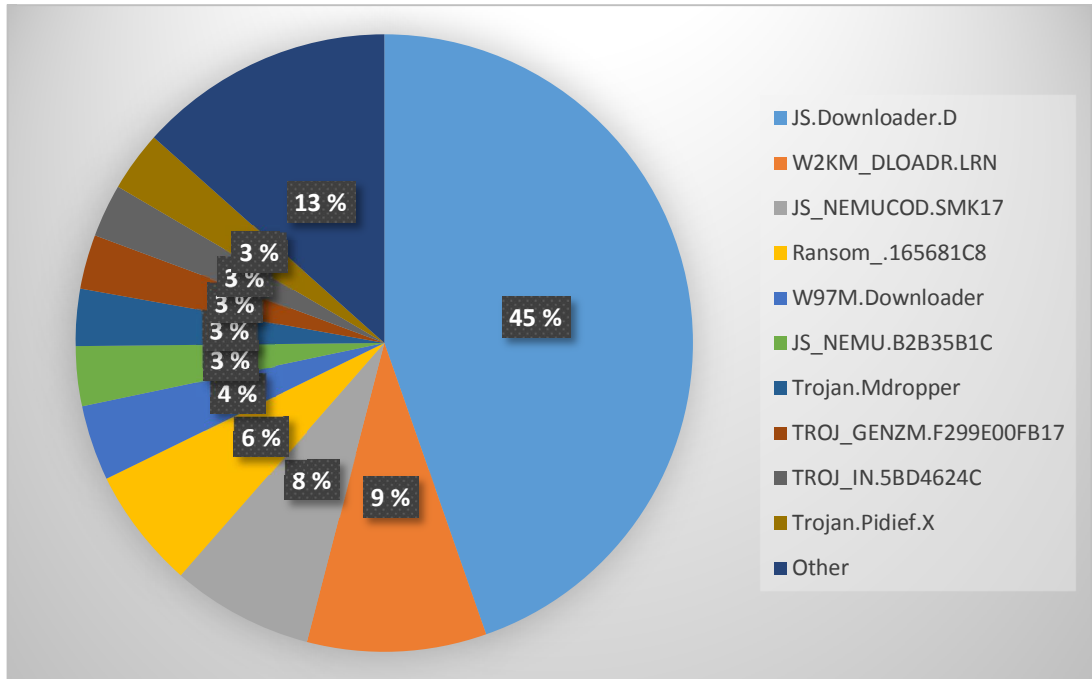


Figure 12. Threat distribution – TOP10 - Vendor 3

Some of the malware is introduced in Chapter 4.6 'Top Malware discovered during research'; for the full list of malware found by vendor 3, please refer to Appendix 1.

4.5.5 Malicious URLs

The TOP list of malicious URLs for vendor 3 (see Table 15) is completely different from the ones displayed earlier with vendor 1 and vendor 2. The vendor still performs quite good on identifying the malicious URLs. One of the strengths of vendor 3 is that it easily logged the complete malicious URL instead of just the domain and there is no need to pick the malicious URL data from several places. Another advantage of vendor 3 is that it analyzes the URL to the full, not only compares the URL to a known list of malicious URLs or the reputation of the URL but really scans the site behind the URL.

Table 15. TOP 10 Malicious domains - Vendor 3

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m.
EEST
Total malicious URLs: 282

Domain	Amount
amino-disqus.club	110
bucksinvestmentgroup.com	13
fitnesssuperstore-bestbuy.com	9
app.emailbackend.com	7
BINFORDTOOL.COM	7
digitalactionist.com	6
MYSAFERRETIREMENT.COM	6
CRAFTSDUJOUR.COM	5
scottshelp.com	5
UN-TIREMENT.COM	5

Below is the breakdown in top domain level (Table 16). Most of the malicious URLs are registered as commercial or .club, i.e. brands, celebrity sites and different clubs.

Table 16. TOP 5 Top level domains - Vendor 3

Time period 6 June 2017 9 p.m. EEST - 14 June 2017 9 p.m. EEST
Total malicious URLs: 282

Top level Domain	Explanation	Amount
com	Commercial	133
club	Brands, clubs, celebrities	112
net	generic, alternative to .com	9
org	organizations (non-commercial)	5
in	India	5

Some new top domains entering the list with vendor 3 are .in, .org and .net.

4.6 TOP Malware discovered during research

In this chapter, TOP malware discovered in the research is introduced beginning with the malware that was number one for all vendors, JS.Downloader.D , what it is and what it does. Ransom.Locky is also discussed because it is linked to the JS.Downloader.D. The other malware is in no specific order.

4.6.1 JS.Downloader.D

JS.Downloader.D is a Trojan, first discovered in November 2016. The variation of this Trojan that was discovered by vendor 1 on June 12, 2017, which is in the same time frame as the data collected for this thesis. The creation of a new variable of an old virus is not trivial. There are pre-made tools for doing this. With a small variation in the malware and there is a brand new malware that could potentially be undetectable. In this case, the variant of the malware is not that hard to detect.

The Trojan affects Windows operating system, and soon infects the system it downloads with executable malicious files and tries to execute them. Ransom.Locky is one of the malware it tries to execute (Symantec.com, 2016a).

4.6.2 Ransom.Locky

Ransom.Locky is not in the top 10: however, it was mentioned in the JS.Downloader.D as one of the malware it tries to execute. Ransom.Locky was discovered in February 2016, and it infects Windows system. It is a Trojan that encrypts files in the infected system. It also places itself in the Windows registry so it runs every time the operating system is started. The Trojan does not encrypt the whole computer but targets files with a specific extension, the full list can be found on Symantec's web page (Symantec, 2016a). Once the encryption is finished, it contacts a remote server and displays a ransom note for the user as the operating system wallpaper. The note consists of text like "all your files have been encrypted", "decrypting of your files is only possible with private key" and of the instructions where and how to obtain this private key, i.e., purchasing the private key for decryption with bitcoins or other virtual currency. There is no guarantee that the private key works even if the ransom is paid. The encryption is done by RSA-2048 and AES-128 thus, trying to decrypt the files with computer power would take a long time. According to DigiCert.com, breaking a RSA-2048 with normal desktop computer would take about 6.4 quadrillion years (DigiCert, 2017). The only real option is that the user has backups of the files that can be restored, and in the future the user should have a threat prevention system in place to block future attacks. Ransom.Troldesh that is in the top 10 works as is Ransom.Locky. There is some variation in the ransom note; however, on the basic level it does the same: encrypts files, communicates with remote server and displays ransom note and awaits for payment.

4.6.3 Trojan.Pidief.X

Trojan.Pidief.X is a PDF-based Trojan that allows on execution just to open the PDF document, download the PDF macro and execute a malicious malware. The Trojan was discovered in April 2017 and it affects Windows system (Symantec, 2017b).

4.6.4 W2KM_DLOADR.LRN

W2KM_DLOADR.LRN is like the most of the malware on the top 10 list, a Trojan. More specifically a Trojan-downloader. Discovered on 13 June 2017, so again within the same time frame as the collected data. The Trojan affects Windows systems and it usually arrives as an attachment, usually a .doc file and on execution it will download files. If the download of the files is successful, the next step is the execution of these files. (Trend Micro, 2017). This Trojan is also known as W97M.Downloader by Symantec and is part of the Dridex campaign. This is a financial attack campaign in which the Trojan was spread by millions of emails on daily basis in its peak in 2015. The Trojan's target is banking credentials, and especially it targets users in the English speaking countries in financial institutions. The Trojan is very much alive and still active as can be seen from the data collected between 6 June and 14 June 2017 (Symantec, 2016b).

4.6.5 Trojan.Gen.7

Trojan.Gen.7 is another Trojan. The GEN part in the definition means that that the Trojan is a generic variant and no specific definition for the Trojan has been created. This type of generic variant was discovered in the October 2017 and affects Windows system (Symantec, 2016d).

4.6.6 Trojan-Downloader:JS/Locky

Trojan-Downloader:JS/Locky is a Trojan-downloader that affects Windows system, i.e. it is a ransomware that encrypts the victim's system and demands ransom for the decryption key. Depending of the variant of the Trojan, it encrypts the system files using AES-128 or RSA 2048-bit encryption algorithm. After encrypting the system the malware saves the text file demanding ransom or displays it as the background on the operating system. The ransom note contains the details for obtaining the decryption-key (F-Secure, 2017c).

4.6.7 W97M.Downloader.M

W97M.Downloader.M is a Trojan-downloader found in December 2016. Its threat rate is very low. The Trojan uses a macro in Windows document to infect. After it executes, it will download a malware and execute it. When Symantec analyzed the downloaded file it contained Ransom.Locky (Symantec, 2016c).

4.7 Other findings

From all the 2,494 entries in Appendix 1, only two false positives could be identified. A false positive in this case is a result where the device analyzes the email, attachment or URL, and the verdict is that the email is malicious. If the results are analyzed by a second or third party, and the verdict is clean, a or manual investigation on the email verdict states that it contains no threat, it is then a false positive. False positives are rare; however, they can impose a problem as they can stop legitimate emails from being delivered. Checking the false positives for malicious URLs would not have been a feasible task, as we do not have data on all malicious URLs attacks. In some cases the data field is empty or only domain data is available.

The false positives found are:

8.6.2017 16:41 1982b37775f50e653308808e0f80d037 Couliaaren..docx
missarenbaly@gmail.com 208.70.128.176


(Time, FileHash, Attachment, SMTP-From and Client-IP)

and

7.6.2017 20:07 7d5855214b4b68b21d03ef57cc8d6182 PO34216.jar
mail@sawawada.com 84.38.129.169

The false positive results were identified when searching VirusTotal with the attachment filehash. It showed the results as clean for the vendors listed in Virustotal.

Virustotal shows the hash 7d5855214b4b68b21d03ef57cc8d6182 that one of the vendors would rate as bad, however, when all the other report it as clean, it will be treated like a false positive. The result can be seen from the figure below (Figure 13), only Ikarus verdict is 'Win32.Outbreak', where all the others' verdict of the hash is 'Clean'. In addition, in the figure below (Figure 13) there are plenty of vendors that verdict the hash as 'Clean' (see Figure 13) (Virustotal, 2017b).



One engine detected this file

SHA-256 4a227b06c2877c4bc315dafa9dc4029d0b28882dd2108ecbd9e150ea5265cf92

File name PO34216.jar

File size 355.94 KB

Last analysis 2017-06-07 19:06:28 UTC

1 / 59

Detection	Details	Relations	Community
Ikarus		⚠ Win32.Outbreak	Ad-Aware ✔ Clean
AegisLab		✔ Clean	AhnLab-V3 ✔ Clean
Alibaba		✔ Clean	ALYac ✔ Clean
Antiy-AVL		✔ Clean	Arcabit ✔ Clean
Avast		✔ Clean	AVG ✔ Clean
Avira		✔ Clean	AVware ✔ Clean
Baidu		✔ Clean	BitDefender ✔ Clean
Bkav		✔ Clean	CAT-QuickHeal ✔ Clean
ClamAV		✔ Clean	CMC ✔ Clean

Figure 13. Virustotal result for hash

5 Evaluation of results

In this chapter, the research results are summarized and also determine the results of the three vendors. The results of the research questions can be found in the table below. More detailed information on why the specific results were concluded will be discussed in chapter 6 – Conclusions and discussion.

The results in Table 17 present the author's personal views of the vendors after analyzing and reviewing the data of the thesis research.

Table 17. Thesis research questions

Vendor	Vendor 1	Vendor 2	Vendor 3
Scale: poor - fair - good - very good – excellent			
How good is the device at mitigating advanced threats?	Very good	Good	Very good
What are the capabilities of the logs, reports and polling the platform?	Good	Good	Excellent
What is the support level of the local vendor?	Excellent	Good	Poor
Does the cost of the device sum up to capabilities?	Excellent	Very Good	Fair
Scale: very easy - easy - normal - hard - very hard			
How much work is needed to set up the device?	Normal	Normal	Easy
How is the administration set up for day-to-day use?	Normal	Normal	Easy

5.1 Summarization of threat results

This chapter presents a summary of the malware and malicious emails by the vendors.

Below is a chart for the identified malicious URLs per day (Figure 14).

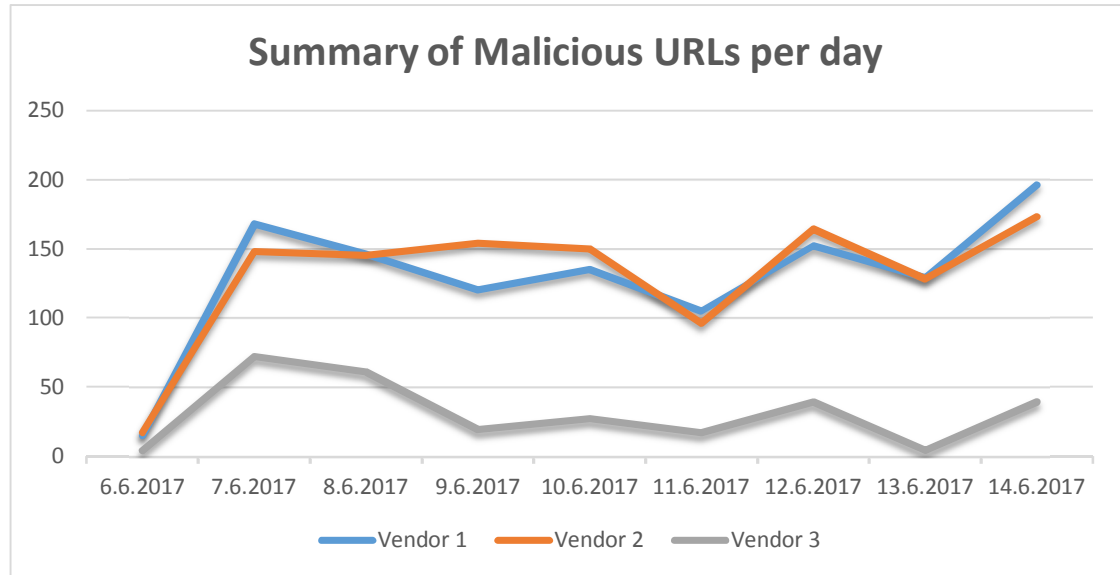


Figure 14. Summary of Malicious URLs per day

Vendor 1 and vendor 2 follow each other quite closely through all the days when the data for the research was collected.

A similar chart for the malware per day (Figure 15) was created. In the malware graph, the vendors all have a very similar curve.

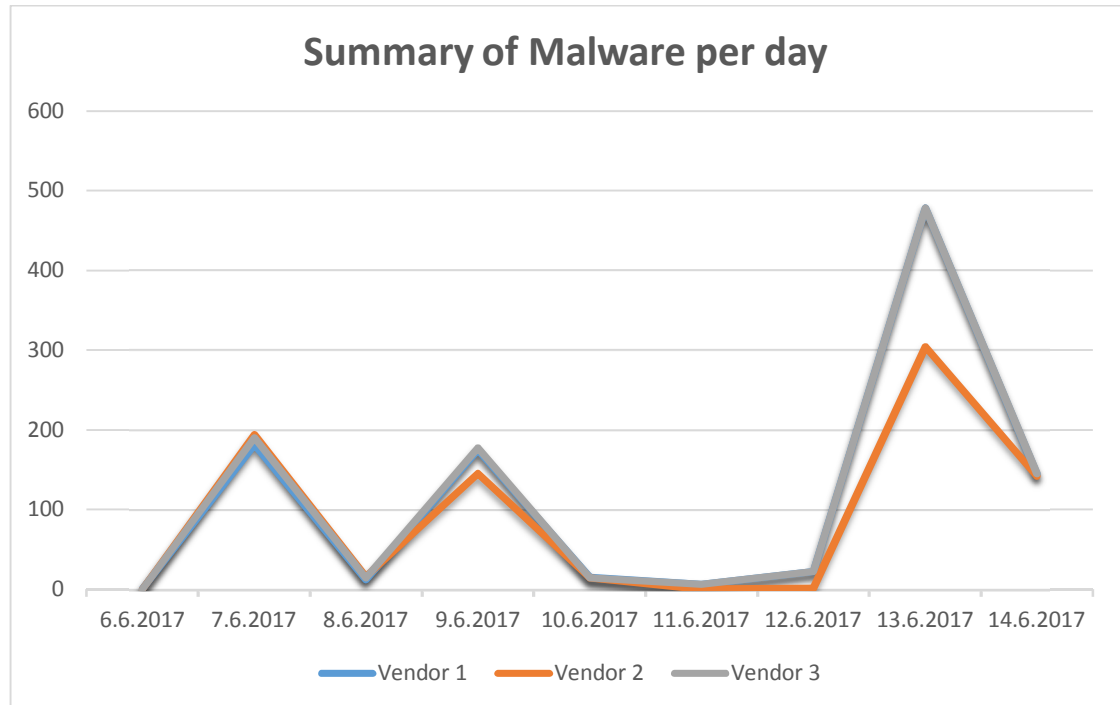


Figure 15. Summary of Malware per day

Having the summarized numbers as a graph helps to see that the vendors' results in identifying malware compared to each other were quite close. The peaks are at somewhat same level for all.

5.2 Threat prevention capabilities

Comparing the three vendors, vendor1 and vendor 3 were rated as the vendors with the best threat prevention capability. The results of vendor 2 are not that far behind; however, looking at the results from the vendor's own reports and then comparing them in Appendix 1 vendor 2 is still behind the other two in numbers. In many cases, vendor 3 identified malicious email whereas vendor 1 and vendor 2 did not identify it as malicious. Vendor 3 used similar threat identification tools as vendor 1 and vendor 2 when identifying malware in attachments, virus engine, sandboxing and own

vendor specific malware recognition engines. Still, the difference comes from the vendor specific capability to identify and mitigate threats. Also, bearing the threat prevention capability in mind, vendor 1 and vendor 2 can be configured and installed in the most complex network, and they carry out a good threat mitigation job, whereas vendor 3 could face problems having the role as first line of defense. The optimal setup would have vendor 1 or vendor 2 as the first line defense and vendor 3 as the second line analyzing the flow that comes through the first line. How the vendor 3 identifies malicious URLs, it is better suited as the second line defense.

5.3 Work needed for setting up system

Vendor 3 was the easiest device to set up and install since it has less configuration options than vendor 1 and vendor 2, and also the device is designed to be easy to set up in the existing environment. If the environment is complex and requires more from the configuration, vendor 1 and especially vendor 2 are better suited for the job. Still in all vendors, with the setup and configuration of the devices for the thesis environment all had some setup or configuration issues that were struggled with. There is still a huge difference between setting up real hardware compared setting up a virtual device. Setting up the device with real hardware is so much more time consuming. One has to take into consideration e.g. racking space, cabling, power and switch configuration. Setting up a virtual device is much more straightforward. Instead of taking into account racking, power, cabling one needs to be sure that the virtual device gets enough resources e.g. CPU cores, disk space and virtual switch ports.

5.4 Administration of device

Comparing the administration gives the same answer as the installation part. Vendor 3 has less configurable options, and the configuration will more likely stay more static, whereas more complex setups can be made with vendor 1 and vendor 2; i.e. more configuring is required making the administration part more heavy. All the

vendors supported role based administration so the task and privileges can be divided between administrators. All vendors also supported outside authorization, so Radius or LDAP authentication could be used against a back-end server that offers centralized authentication to the devices. All the devices also have the opportunity to use their vendor-specific centralized management platform that will help a great deal if there are many threat prevention platforms. The same profiles and objects can then be used on multiple objects, which helps with generating a common threat rule base and profiles when the same objects can be utilized on all devices.

5.5 Reports, logging and device polling

All vendors provide pre-made reports and support scheduled delivery. Vendor 3 has more options to device polling and logging than the other two vendors. The reports generated on vendor 3 device are clear and easy to read. If the centralized management offered by the three vendors were to be used, data could be summarized from all devices or summarized reports created. It would also be easier to find specific emails or specific attacks when one can search all devices at the same time. The centralized management platform can work as a log-collector for log analysis, or one can use the device as a node to relay the logs further.

5.6 Vendor support

The vendor support is a critical aspect for getting help and problems solved. Vendor support is needed when the devices are ordered, licensed, device support contracts drafted, and when the actual support of the devices is needed. The setup and installation of the thesis research environment communication with all the vendors took place with getting the actual device (hardware or virtual) and licenses so they would operate. Some small issues were encountered and they showed that communication is needed with the vendor representative to help solve the issues.

The skill levels of the support provided by all vendors are really good but the lacking of local support on vendor 3 makes vendor 1 and vendor 2 better in the comparison. Communication with vendor 3 took longer, as one needed to talk outside Finland in another time zone and not in Finnish. Vendor 1 was rated the best of all three

vendors. The major reason was the local support; vendor 1 was the most active, easily reached and approachable. It offered more than was asked for and was very helpful in the installation and setup part. Vendor 2's global support must also be mentioned; after opening a ticket one gets help quickly and very professionally. This lead to the end result that the issues were quickly and efficiently resolved.

5.7 Cost of the device compared to benefit

All devices have costs, and comparing the hardware or virtual version and licenses, support contracts costs to the malware mitigation performance, vendor 1 has a really good cost/benefit ratio. Not far behind is vendor 2. With vendor 3, the costs are quite high compared to the benefits, however, vendor 3 is still a good investment.

6 Conclusions and discussion

6.1 General

Comparing the three vendors with the same live email flow is something that has not been done in Cygate before. The comparison and use of the same flow indicates how well the different vendor platforms identified malware and malicious URLs. In addition, other useful knowledge was obtained from the thesis research, comparing the installation, administration and configuration of the three vendors.

With the data and results from the thesis research, more details about the capabilities of the three vendors are identified and how they are positioned to each other in the sense of which vendor would suit to which customer and environment. This will be helpful knowledge in forthcoming installations and even more helpful when assessing on and discussing with customers which platform to use.

The comparison between logging, polling and reporting capabilities of the devices can lead to new projects at Cygate internally and for customers, ways on how to get more out of the device management and monitoring. The use of sending events as http/https that vendor 3 supported could be interesting to work on more. The thesis could be used, for example, when making automatic tickets via a ticketing system or pushing values like IPs to a dynamic object and utilizing that object in the firewall policy for blacklist/whitelist purposes. The scheduled reports are a feature that has been in minimal use; however, it should also be a feature that needs more consideration on ways to get more out of it.

The thesis research changed my understanding and pre-assumptions of the vendors. Much was learned in all the stages of the thesis research, all through installation, configuration, data collection, data comparison, and lastly, with the technical review and comparison of the results. The most interesting part of the stages is the actual installation of the devices and finding out about new features and tools as well as figuring out how they can be used in future projects. The most time consuming part was working on Appendix 1 and getting all results in the same Excel spreadsheet and making them somehow comparable to each other. It was also the most frustrating part, documenting the results and noticing that two malware that are with different

names from two vendors are the same, and combining them changes a great deal of the results and tables. That topic is discussed more in detail in Chapter 6.2 'Challenges'.

6.2 Challenges

On the biggest challenges in the thesis research was getting comparable results of the threat prevention from all vendors. All the vendors create a great number of logs, and comparing and cross-checking results manually is time consuming. If a new comparison on threat prevention platforms is done in the future, the recommendation is to use even more time on testing the output of the devices to make the comparison easier. Alternatively, to use a log collector to send all device logs via syslog and use the log collector's tools to make comparison of the data collected. Also SNMP traps could be used for collecting the threat events and an SNMP tool for editing and comparing the data. I cannot say without testing if the log collector or SNMP collector would be less time consuming compared to manual comparison work. Installing and setting up the log collector or the SMNP analyzer should bring future use for the platforms so the installation and setup would not just be for the comparison project.

References

- Klensin, J. 2008. IETF RFC5321, Simple Mail Transport Protocol. Accessed 30.4.2017. Retrieved from <https://tools.ietf.org/html/rfc5321>
- Trend Micro. 2016. The problem with open source malware. Accessed 15.10.2017. Retrieved from <http://blog.trendmicro.com/the-problem-with-open-source-malware/>
- Cygate. 2017. Cygate Oy. Accessed 29.10.2017. Retrieved from <http://www.cygate.fi/en/welcome>
- Cisco. 2014. ESA FAQ: How do I configure bounce verification on the ESA? Accessed 29.10.2017. Retrieved from <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117918-technote-esa-00.html>
- Resnick, P. 2008. IETF RFC5322, Internet Message Format. Accessed 30.4.2017. Retrieved from <https://tools.ietf.org/html/rfc5322>
- GetCyberSafe. 2017. Common threats to be aware of. Accessed 29.10.2017. Retrieved from <https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx>
- TheWindowsClub. 2017. Email Bombing and ways to protect yourself. Accessed 29.10.2017. Retrieved from <http://www.thewindowsclub.com/email-bombing>
- Coolhead Tech. 2014. 4 Benefits of Cloud Email. Accessed 29.10.2017. Retrieved from <http://www.coolheadtech.com/blog/4-benefits-of-cloud-email>
- RoseHosting. 2016. Physical server vs Virtual server: All you need to know. Accessed 29.10.2017. Retrieved from <https://www.rosehosting.com/blog/physical-server-vs-virtual-server-all-you-need-to-know/>
- Phifer, L. 2010. Top 10 Email Malware Threats. Accessed 29.10.2017. Retrieved from <https://www.esecurityplanet.com/views/article.php/3903881/Top-10-Email-Malware-Threats.htm>
- PhishingBox. 2013. Types Of Phishing Defined. Accessed 29.10.2017. Retrieved from <https://www.phishingbox.com/news/phishing-news/types-of-phishing-defined>
- The Radicati Group. 2017. Email Statistics Report, 2017-2021. Accessed 30.4.2017. Retrieved from <http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf>
- Statista. 2016. Global spam volume as percentage of total e-mail traffic from January 2014 to March 2017, by month. Accessed 30.4.2017. Retrieved from <https://www.statista.com/statistics/420391/spam-email-traffic-share/>
- Symantec. 2017a. File extensions and types that are common threat vectors for email. Accessed 23.9.2017. Retrieved from https://support.symantec.com/en_US/article.INFO3768.html

Google, 2017. Some file types are blocked. Accessed 24.9.2017. Retrieved from https://support.google.com/mail/answer/6590?p=BlockedMessage&visit_id=1-636418363953476576-1867596567&rd=1

Symantec.com. 2016a. JS.Downloader.D. Accessed 30.9.2017. Retrieved from https://www.symantec.com/security_response/writeup.jsp?docid=2016-110312-1900-99&tabid=2

Symantec. 2016a. Ransom.Locky. Accessed 30.9.2017. Retrieved from https://www.symantec.com/security_response/writeup.jsp?docid=2016-021706-1402-99

Symantec. 2017b. Trojan.Pidief.X. Accessed 30.9.2017. Retrieved from https://www.symantec.com/security_response/writeup.jsp?docid=2017-042613-5240-99

Virustotal. 2017a. About VirusTotal. Accessed 1.10.2017. Retrieved from <https://www.virustotal.com/en/about/>

Luther, M. 2010. Voltage.com, The very first spam? Accessed 3.10.2017. Retrieved from <https://www.voltage.com/email/the-very-first-spam/>

Hambridge, S. & Lunde, A. 1999. IETF RFC2635, DON'T SPEW - A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*). Accessed 15.10.2017. Retrieved from <https://tools.ietf.org/html/rfc2635>

CERT. 2017a. Email Bombing and Spamming. Accessed 15.10.2017. Retrieved from https://www.cert.org/historical/tech_tips/email_bombing_spamming.cfm

CERT. 2017b. IDS04-J. Safely extract files from ZipInputStream. Accessed 15.10.2017. Retrieved from <https://www.securecoding.cert.org/confluence/display/java/IDS04-J.+Safely+extract+files+from+ZipInputStream>

Ferguson, P. & Senie, D. 2000. IETF RFC2827, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Accessed 15.10.2017. Retrieved from <https://www.ietf.org/rfc/rfc2827.txt>

F-Secure. 2017a. Viruses. Accessed 15.10.2017. Retrieved from https://www.f-secure.com/en/web/labs_global/viruses

Kaspersky. 2017. What is a Trojan Virus? – Definition. Accessed 6.10.2017. Retrieved from <https://usa.kaspersky.com/resource-center/threats/Trojans>

Trend Micro, 2017. Accessed 7.10.2017. Retrieved from https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/w2km_dloadr.lrn

Symantec. 2016b. W2KM_DLOADR.LRN. Accessed 7.10.2017. Retrieved from <https://www.symantec.com/connect/blogs/dridex-financial-Trojan-aggressively-spread-millions-spam-emails-each-day>

Symantec. 2016d. Trojan.Gen.7. Accessed 7.10.2017. Retrieved from https://www.symantec.com/security_response/writeup.jsp?docid=2016-122103-5010-99

F-Secure. 2017c. Trojan-Downloader:JS/Locky .Accessed 7.10.2017. Retrieved from https://www.f-secure.com/v-descs/Trojan-downloader_js_locky.shtml

Symantec. 2016c. W97M.Downloader.M. Accessed 7.10.2017. Retrieved from https://www.symantec.com/security_response/writeup.jsp?docid=2016-120111-2355-99&tabid=2

Virustotal. 2017b. Accessed 8.10.2017. Retrieved from <https://www.virustotal.com/#/file/4a227b06c2877c4bc315dafa9dc4029d0b28882dd2108ecbd9e150ea5265cf92/detection>

F-Secure. 2017b. Worms. Accessed 15.10.2017. Retrieved from https://www.f-secure.com/en/web/labs_global/worms

Symantec.com. 2017a. What are malicious websites and drive by downloads? Accessed 15.10.2017. Retrieved from <https://us.norton.com/internetsecurity-malware-what-are-malicious-websites.html>

Cain, P. & Jevans, D. 2010. IETF RFC5901, Extensions to the IODEF-Documents Class for Reporting Phishing. Accessed 15.10.2017. Retrieved <https://www.ietf.org/rfc/rfc5901.txt>

CERT. 2017c. Spoofed/Forged Email. Accessed 8.10.2017. Retrieved from https://www.cert.org/historical/tech_tips/email_spoofing.cfm

Hoffman,P. 2002. IETF RFC3207, SMTP Service Extension for Secure SMTP over Transport Layer Security. Accessed 15.10.2017. Retrieved <https://www.ietf.org/rfc/rfc3207.txt>

Microsoft. 2017. Office 365 - Stay in sync with business-class email .Accessed 8.10.2017. Retrieved from <https://products.office.com/en/business/office-365-business-email-and-shared-calendar-services>

Digicert. 2017. Check our Numbers. Accessed 19.10.2017. Retrieved from <https://www.digicert.com/TimeTravel/math.htm>

Appendices

Appendix 1. Theat prevention summary – all vendors.

TIME;FileHash;VirusTotal by hash or equivalent;Vendor 1;Vendor 2;Vendor 3;Attachment;Malicious URL or domain;SMTP-From;Client-IP;;

6.6.2017 21:04;;Malicious-URL;Malicious-URL;;organictabletinc.ru;kferguson@msh.org;209.54.52.85;;

6.6.2017 21:04;;Malicious-URL;Malicious-URL;;organictabletinc.ru;support+sagaymymjq3bc@msh.org;209.54.52.85;;

6.6.2017 21:27;;Malicious-URL;;031530.com;;;

6.6.2017 21:41;;Malicious-URL;;mejohn@rea-alp.com;190.180.47.244;;

6.6.2017 21:42;;Malicious-URL;;qcksih@vtl-automotive.com;27.7.194.130;;

6.6.2017 21:42;;Malicious-URL;;sdygto@static.vnpt.vn;14.186.62.138;;

6.6.2017 21:45;;Malicious-URL;;hxxp://www.travel.multi-service.ma/0858cae9bec.html;tenho.moilanen@netti.fi;123.120.121.170;;

6.6.2017 21:46;;Malicious-URL;Malicious-URL;amino-disqus.club;alvarezc.alvarez54@etrade.com.au;139.228.90.53;;

6.6.2017 21:55;;Malicious-URL;Malicious-URL;;hxxp://www.ggmp4.com/plus/hftgmt/martin.huber@iiad.net;125.212.220.155;;

6.6.2017 21:55;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;notification+7py2q4zq33nv@iiad.net;125.212.220.155;;

6.6.2017 22:03;;Malicious-URL;Malicious-URL;;hxxp://new.macartu.cn;uyprnj@hmsinet.ca;83.239.58.162;;

6.6.2017 22:03;;Malicious-URL;Malicious-URL;;macartu.cn;uyprnj@hmsinet.ca;83.239.58.162;;

6.6.2017 22:09;;Malicious-URL;Malicious-URL;;amfikenya.com;jucaribou@beersandcutler.com;187.141.38.2;;

6.6.2017 22:16;;Malicious-URL;;aritory.ru;;;

6.6.2017 22:22;;Malicious-URL;Malicious-URL;;macartu.cn;wyncriez@hmsinet.com.au;59.72.109.47;;

6.6.2017 22:24;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;update+hyd9erivrry@mds.nordion.com;82.165.157.158;;

6.6.2017 22:29;;Malicious-URL;Malicious-URL;;macartu.cn;shijotz@hmsinet.com.au;115.231.16.138;;

6.6.2017 22:43;;Malicious-URL;Malicious-URL;;medicalrxquality.su;support+e2ewe88drtaq@prudentialgeorgia.com;93.115.248.32;;

6.6.2017 22:54;;Malicious-URL;;xujing@16ds.com;117.79.81.101;;

6.6.2017 22:56;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;siuming8149@yahoo.com.hk;62.48.155.53;;

6.6.2017 23:19;;Malicious-URL;;lining@dlbc.org.cn;218.25.172.138;;

6.6.2017 23:19;;Malicious-URL;;lining@dlbc.org.cn;218.25.172.138;;

7.6.2017 0:02;;Malicious-URL;Malicious-URL;;macartu.cn;asgluwiouvozf@vdtvtech.us;123.59.100.243;;

7.6.2017 0:05;;Malicious-URL;Malicious-URL;;macartu.cn;info@WHICH.com;189.84.86.245;;

7.6.2017 0:07;;Malicious-URL;Malicious-URL;;macartu.cn;subcsagabyp@hmsinet.com.au;213.32.67.185;;

7.6.2017 0:15;;Malicious-URL;Malicious-URL;;medicalrxquality.su;update+77ugxx973m@netscape.net;121.254.170.245;;

7.6.2017 0:20;;Malicious-URL;Malicious-URL;;medicalrxquality.su;k.ing@live.de;200.219.244.56;;

7.6.2017 0:34;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 0:56;;Malicious-URL;Malicious-URL;;organictabletinc.ru;notification+dy9gaajdeq1y@yahoo.com.tw;193.227.248.241;;

7.6.2017 1:02;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 1:42;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;nfox@jenkinsinsgroup.com;192.145.239.35;;

7.6.2017 1:49;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 1:54;;Malicious-URL;Malicious-URL;;medicalrxquality.su;michael7190@netscape.net;62.152.59.102;;

7.6.2017 2:27;;Malicious-URL;;rboca.com;;;

7.6.2017 2:27;;Malicious-URL;;rboca.com;;;

7.6.2017 2:27;;Malicious-URL;;rboca.com;;;

7.6.2017 2:29;;Malicious-URL;Malicious-URL;;macartu.cn;520726620715803.BU72864@are.hmsinet.com.au;180.210.205.107;;

7.6.2017 2:35;;Malicious-URL;Malicious-URL;;medicalrxquality.su;stevensean@lives.fr;88.87.139.81;;

7.6.2017 2:39;;Malicious-URL;Malicious-URL;;organictabletinc.ru;support+mhqkqyghggo@google.com;61.19.97.200;;

7.6.2017 2:40;;Malicious-URL;Malicious-URL;;macartu.cn;wwjfuevarur@hmx.de;178.33.161.254;;

7.6.2017 2:44;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 2:45;;Malicious-URL;Malicious-URL;;medicalrxquality.su;lay@peoplepc.com;216.55.187.54;;

7.6.2017 2:48;;Malicious-URL;Malicious-URL;;medicalrxquality.su;motherpam@juno.com;110.45.144.153;;

7.6.2017 2:50;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;Mailer-Daemon@cp3.awsia.com;54.253.250.62;;

7.6.2017 2:51;;Malicious-URL;Malicious-URL;;medicalrxquality.su;;;

7.6.2017 2:53;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 3:03;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;update+zu47k6qy6p3t@theatre.sk;111.67.21.148;;

7.6.2017 3:09;;Malicious-URL;Malicious-URL;;dingzhijiu8.com;yangjie@beifabook.com;123.103.6.17;;

7.6.2017 3:31;;Malicious-URL;Malicious-URL;;macartu.cn;muoam@growthstrategies.us;117.239.212.50;;

7.6.2017 3:31;;Malicious-URL;Malicious-URL;;macartu.cn;hwpfqtjw@billings.k12.mt.us;117.239.212.50;;

7.6.2017 3:38;5530b442f6206d1087979330f9ea0ef;Trojan.GenericKD.5277956;;Malware;Malware;RFQ#KTC-06072017.pdf.exe;hxxp://clck.ru/BDUF5;mustafar.vadie@ktcco.net;198.57.206.195;;

7.6.2017 3:41;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 4:00;;Malicious-URL;Malicious-URL;;macartu.cn;nfskj@hmsinet.com;115.231.16.175;;

7.6.2017 4:05;;Malicious-URL;Malicious-URL;;dingzhijiu8.com;lizheng@handdb.com;121.12.119.42;;

7.6.2017 4:17;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 4:18;;Malicious-URL;Malicious-URL;;macartu.cn;dslifzseg@hmsinet.com.co.uk;186.27.126.130;;

7.6.2017 4:26;;Malicious-URL;Malicious-URL;;macartu.cn;862636520520434.MI55148@keta.hmt.hitachi-metals.com;59.72.109.47;;

7.6.2017 4:33;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 4:59;;Malicious-URL;Malicious-URL;;tbwjlx.com;lijing@dgpp.com;61.189.63.122;;

7.6.2017 5:12;;Malicious-URL;Malicious-URL;;macartu.cn;626207175826047.FM82572@jlm.hmsinet.harvard.edu;59.37.22.82;;

7.6.2017 5:16;;Malicious-URL;;dealydid.com;;;

7.6.2017 5:36;;Malicious-URL;Malicious-URL;;onlinesmartsale.com;;;

7.6.2017 5:39;;Malicious-URL;;ssqelhxq@iphonia.com;113.163.94.163;;

7.6.2017

5:42;347972a2d6e5bfd8d0665218729472db;SecurityRisk.gen1;Malware;Malware;Malware;IMG20170606_004356.jpg.....
.....g.z;neal.belmont@gmail.com;184.179.10.71;;

7.6.2017

5:42;fe330cf1b96152162516cd092f2f9fa2;Trojan.Gen.2;Malware;Malware;Malware;IMG20170606_004356.jpg.....
.....exe;neal.belmont@gmail.com;184.179.10.71;;

7.6.2017

5:49;a3fd7e6f938a78b9e04914caa0229a9f;Trojan.Gen.2;Malware;Malware;Malware;PURCHASEORDER777373383_pdf.exe;;mail@sawawada.com;84.38.129.169;;

7.6.2017 5:49;f93c7598cc76f6a6fe947aaf2199522;Malware;Malware;Malware;Malware;PURCHASEORDER777373383_pdf.rar;;mail@sawawada.com;84.38.129.169;;

7.6.2017 5:51;;Malicious-URL;;acuadugah@iphonia.com;87.107.209.66;;

7.6.2017 6:14;;Malicious-URL;Malicious-URL;;dingzhijiu8.com;liuhua@hysj.cn;219.148.58.78;;

7.6.2017 6:17;;Malicious-URL;Malicious-URL;;macartu.cn;bnizubvgl@hmt.hitachi-metals.com;212.52.44.51;;

7.6.2017 6:20;;Malicious-URL;Malicious-URL;;dingzhijiu8.com;ligang@xinfagroup.com.cn;221.2.221.146;;

7.6.2017 6:20;;Malicious-URL;Malicious-URL;;macartu.cn;nzkoth@hmsinet.org.uk;94.20.21.38;;

7.6.2017 6:37;;Malicious-URL;Malicious-URL;;onlinesmartsale.com;;;

7.6.2017 7:00;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 7:30;;Malicious-URL;;aritory.ru;;;

7.6.2017 7:38;;Malicious-URL;Malicious-URL;;macartu.cn;shocxjcy@awr.us;212.52.44.51;;

7.6.2017 7:50;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 8:07;;Malicious-URL;Malicious-URL;;hxxp://miltonbellphotography.com/Benjamin/login.htm;marco@policiaivil.pa.gov.br;177.74.63.169;;

7.6.2017 8:13;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;www.run@srv-web.site;90.182.157.205;;

7.6.2017 8:14;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;hyu1201880001@hyu-120188.hichina.com;121.40.181.129;;

7.6.2017 8:22;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;philip@supernova.webgravity.org;192.169.58.104;;

7.6.2017 8:35;;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;

7.6.2017 8:40;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;byu1191480001@byu-119148.hichina.com;123.56.106.140;;;

7.6.2017 8:40;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;webmaster@xn----7sba7aaopjrlade0k.xn--c1avg;185.125.218.137;;;

7.6.2017 8:41;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;apache@proteusdynamic.com;81.142.110.244;;;

7.6.2017 8:41;;;Malicious-URL;Malicious-URL;;macartu.cn;qaaiosjsqu@hmsheridan.co.uk;49.140.65.25;;;

7.6.2017 8:50;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;qyu1251330001@qyu-125133.hichina.com;118.190.173.87;;;

7.6.2017 8:54;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;www-data@neutrino.intrex.hu;87.229.112.69;;;

7.6.2017 8:56;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;sol@svm46108.vps.tagadab.com;80.241.49.114;;;

7.6.2017 9:02;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;chinnu@rh05.chinmayi.com;108.165.21.81;;;

7.6.2017 9:05;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;hyu1201880001@hyu-120188.hichina.com;121.40.181.129;;;

7.6.2017 9:13;;;Malicious-URL;;;niktusia@buziaczek.pl;123.24.193.49;;;

7.6.2017 9:18;;;Malicious-URL;;hxxp://app.emailbackend.com/unsubscribe.php?M=102188509&C=adab40e87aba66c4ea1a5ed53cdbc74&L=12720&N=16303;bounce@emailbackend.com;185.13.3.137.19;;;

7.6.2017 9:18;;;Malicious-URL;;hxxp://app.emailbackend.com/unsubscribe.php?M=102191285&C=65a65d85cb4e2bfb926e614bd024d784&L=12720&N=16303;bounce@emailbackend.com;185.13.3.137.19;;;

7.6.2017 9:34;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;webmaster@rdc-karelia.ru;178.19.248.59;;;

7.6.2017 9:38;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;sales@customercare.sap;207.246.241.250;;;

7.6.2017 9:49;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;platform@bueregexperten.de;91.250.99.64;;;

7.6.2017 9:49;;;Malicious-URL;Malicious-URL;;macartu.cn;125876274538516.PA07108@ujg.hmshost.com.au;179.111.242.56;;;

7.6.2017 9:51;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;webmaster@oilclub.kz;185.100.64.74;;;

7.6.2017 9:51;;;Malicious-URL;Malicious-URL;;macartu.cn;437031834538466.QL73627@tmi.hmsoldies.org.uk;49.140.162.133;;;

7.6.2017 9:54;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;chinnu@rh05.chinmayi.com;108.165.21.81;;;

7.6.2017 9:54;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;senateng@qua.quantisedsolutions.com;142.4.13.75;;;

7.6.2017 10:04;;;Malicious-URL;Malicious-URL;;scandigogo.com;jacquiline@readbs.com;212.16.98.57;;;

7.6.2017 10:06;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;anonymous@plesk2.rttcomm-sibir.ru;95.172.146.253;;;

7.6.2017 10:07;;;Malicious-URL;Malicious-URL;;macartu.cn;dcifyzme@hn-f.com;177.220.252.30;;;

7.6.2017 10:07;;;Malicious-URL;Malicious-URL;;macartu.cn;hwbalu@hn-health.com;177.220.252.30;;;

7.6.2017 10:11;;;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

7.6.2017 10:24;;;Malicious-URL;Malicious-URL;;scandigogo.com;;;

7.6.2017 10:34;;;Malicious-URL;Malicious-URL;;dingzhijiu8.com;wangying@baw.com.cn;221.195.40.89;;;

7.6.2017 10:34;;;Malicious-URL;Malicious-URL;;doneforyoub2bleads.us;System@doneforyoub2bleads.us;185.141.206.19;;;

7.6.2017 10:35;;;Malicious-URL;;forums@developer.bmc.com;204.93.64.116;;;

7.6.2017 10:37;;;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

7.6.2017 10:50;;;Malicious-URL;Malicious-URL;;familierabatnordic.dk;;;

7.6.2017 10:52;27849ada53e43e958792af3072a09de8;NO HIT;;Malware;Malware;4543.js;info@85-218-118-212.dclient.lisne.ch;41.87.9.66;;;

7.6.2017 10:52;3be9436fc665b20107cf8c962977c946;NO HIT;;Malware;Malware;6645465648653.zip;info@85-218-118-212.dclient.lisne.ch;41.87.9.66;;;

7.6.2017 10:52;af658e226597e7e0ca7e046b83290cc;NO HIT;;Malware;Malware;4543.zip;info@85-218-118-212.dclient.lisne.ch;41.87.9.66;;;

7.6.2017 10:56;;;Malicious-URL;;forums@developer.bmc.com;204.93.64.116;;;

7.6.2017 10:59;;;Malicious-URL;Malicious-URL;;macartu.cn;ggpjyacqke@hn-health.com;115.49.52.26;;;

7.6.2017 11:07;;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

7.6.2017 11:14;;;Malicious-URL;Malicious-URL;;medicemail.com;;;

7.6.2017 11:21;;;Malicious-URL;;nordiskhandelsplads.dk;;;

7.6.2017 11:32;be0e2c6016fb3c543b3c5159e4fc3c0d;Trojan.Mdropper;Malware;Malware;Malware;4G7U6MIK.doc;;anonymous@plesk2.rttcomm-sibir.ru;95.172.146.253;;;

7.6.2017 11:42;;;Malicious-URL;;forums@developer.bmc.com;204.93.64.117;;;

7.6.2017 11:45;;;Malicious-URL;;reply@gedonte.com;212.16.98.57;;;

7.6.2017 11:52;c173cd02f9e0960e6ca85b77a2152507;Trojan.Pidief.X;Malware;Malware;Malware;001_3097.pdf;jackiegardener@edendeal.co.uk;122.160.33.40;;;

7.6.2017 11:52;c7c42d9c37e52180a82547da55a745c1;W97M.Downloader;Malware;Malware;Malware;690UICEBVOFF735.docm;jackiegardener@edendeal.co.uk;122.160.33.40;;;

7.6.2017 11:58;2ed0ee58bf131bfa1b0c348ebd61c0f0;Trojan.Pidief.X;Malware;Malware;Malware;001_1608.pdf;briannavilliers@arcabreukelen.nl;185.108.124.26;;;

7.6.2017 11:58;2ed0ee58bf131bfa1b0c348ebd61c0f0;Trojan.Pidief.X;Malware;Malware;Malware;001_0362.pdf;emiliokingston@thenotarysolution.co.uk;45.121.190.238;;;

7.6.2017 11:58;42526e7598e3a9967bd031f3c0dff8bd;Trojan.Pidief.X;Malware;Malware;Malware;001_7721.pdf;carlobull@amsterdamtour.co.uk;197.232.26.137;;;

7.6.2017 11:58;42526e7598e3a9967bd031f3c0dff8bd;Trojan.Pidief.X;Malware;Malware;Malware;001_0977.pdf;dwrightfitpatrick@the-beacon-bod.cornwall.sch.uk;122.167.236.45;;;

7.6.2017 11:58;42526e7598e3a9967bd031f3c0dff8bd;Trojan.Pidief.X;Malware;Malware;Malware;001_9281.pdf;jedmundodickey@kukaz.com;103.83.128.82;;;

7.6.2017 11:58;58b3ea52c75a1c067407e6c3d9649608;W97M.Downloader;Malware;Malware;Malware;259R93GIDHL309.docm;carlobull@amsterdamtour.co.uk;197.232.26.137;;;

7.6.2017 11:58;f71c23d3f7f85bc2140faf6e2f6ece37;NO HIT;Malware;Malware;Malware;187NNEPNGSLC134.docm;emiliokingston@thenotarysolution.co.uk;45.121.190.238;;;

7.6.2017 11:59;42526e7598e3a9967bd031f3c0dff8bd;Trojan.Pidief.X;Malware;Malware;Malware;001_1496.pdf;antwancolquitt@mintpm.co.uk;39.36.177.201;;;

7.6.2017 11:59;42526e7598e3a9967bd031f3c0dff8bd;Trojan.Pidief.X;Malware;Malware;Malware;001_6335.pdf;dixiekedslie@milosuk.co.uk;203.76.149.66;;;

7.6.2017 12:05;;;Malicious-URL;Malicious-URL;;macartu.cn;uubqfkyh@hmv-ahien.de;60.10.163.122;;;

7.6.2017 12:08;12793149daa5e9bf0d29657ad9934b4f;Trojan.Pidief.X;Malware;Malware;Malware;132NNKY1O5162.docm;joycebuston@pcmi.co.uk;103.194.28.33;;;

7.6.2017 12:08;3372348d84c01a8441bf5a06b11205d5;Trojan.Pidief.X;Malware;Malware;Malware;001_5514.pdf;jewellbotham@mainpay.co.uk;185.135.96.43;;;

7.6.2017 12:08;3372348d84c01a8441bf5a06b11205d5;Trojan.Pidief.X;Malware;Malware;Malware;001_9127.pdf;jewellnoland@zukanavi.com;43.252.141.88;;;

7.6.2017 12:08;39f1452727108a0adcd2e656f5580b9;Trojan.Pidief.X;Malware;Malware;Malware;902ASSQOXE5458.docm;jewellnoland@zukanavi.com;43.252.141.88;;;

7.6.2017 12:08;fde3e5118602f7800dc55a0a6b9ffcc0;Trojan.Pidief.X;Malware;Malware;Malware;001_2298.pdf;dianafindley@grahamsweetsstudios.co.uk;103.43.80.42;;;

7.6.2017 12:08;fde3e5118602f7800dc55a0a6b9ffcc0;Trojan.Pidief.X;Malware;Malware;Malware;001_1837.pdf;joycebuston@pcmi.co.uk;103.194.28.33;;;

7.6.2017 12:09;3372348d84c01a8441bf5a06b11205d5;Trojan.Pidief.X;Malware;Malware;Malware;001_0075.pdf;broderickkirwan@hovershut.co.uk;116.193.161.82;;;

7.6.2017 12:09;3372348d84c01a8441bf5a06b11205d5;Trojan.Pidief.X;Malware;Malware;Malware;001_0479.pdf;jaimecawley@caraemoore.co.uk;91.243.165.245;;;

7.6.2017 12:09;3372348d84c01a8441bf5a06b11205d5;Trojan.Pidief.X;Malware;Malware;Malware;001_5961.pdf;jeannewarcup@yijing.co.uk;139.0.165.191;;;

7.6.2017 12:09;3372348d84c01a8441bf5a06b11205d5;Trojan.Pidief.X;Malware;Malware;Malware;001_3828.pdf;lymangoulding@yourname.worldonline.co.uk;14.169.12.195;;;

7.6.2017 12:09;3372348d84c01a8441bf5a06b11205d5;Trojan.Pidief.X;Malware;Malware;Malware;001_2491.pdf;yeseniadonaldson@blanchardrecruitment.co.uk;112.196.77.218;;;

7.6.2017 12:09;390c347badee8db4dfff21a09dcf81e4;W2KM_DL.6C654D7E;Malware;Malware;Malware;001_4345.pdf;kathycurtis@118telecom.co.uk;122.176.81.111;;;

7.6.2017 12:09;390c347badee8db4dfff21a09dcf81e4;W2KM_DL.6C654D7E;Malware;Malware;Malware;001_6563.pdf;violaashford@kenton-primary.devon.sch.uk;213.177.10.50;;;

7.6.2017 12:09;bffca80e5fb7aff105e4aba6d3ad095b;W2KM_DL.6C654D7E;Malware;Malware;Malware;943RTBHXFBFS995.docm;violaashford@kenton-primary.devon.sch.uk;213.177.10.50;;;

7.6.2017 12:10;390c347badee8db4dfff21a09dcf81e4;W2KM_DL.6C654D7E;Malware;Malware;Malware;001_6886.pdf;suzannemarkham@ptfc.worldonline.co.uk;113.189.226.198;;;

7.6.2017 12:11;3372348d84c01a8441bf5a06b11205d5;Trojan.Pidief.X;Malware;Malware;Malware;001_0381.pdf;sophiechapmen@orgbox.co.uk;185.122.94.79;;;

7.6.2017 12:16;34c0dbd631b38c786f0570c3781cfff0;Trojan.Pidief.X;Malware;Malware;Malware;616MGMQLVRX737.docm;gerardsellers@themediasaleshouse.co.uk;122.173.223.72;;;

7.6.2017 12:16;d9c1e45b1df957615e18581e0fa45a1;Trojan.Pidief.X;Malware;Malware;Malware;001_8724.pdf;gerardsellers@themediasaleshouse.co.uk;122.173.223.72;;;

7.6.2017 12:19;5f8aeb77fde540615662564d5a32f63f;Trojan.Pidief.X;Malware;Malware;Malware;001_4328.pdf;lucilleamery@mvgnet.worldonline.co.uk;59.99.226.163;;;

7.6.2017
12:19;65f2c8011284409bb8843576abef0153;Trojan.Pidief.X;Malware;Malware;Malware;670CAPHMDR832.docm;;lucilleamery@mvgnetworkonline.co.uk;59.99.226.163;;
7.6.2017 12:28;ad7bc549bca65296d68d4ea434da87ee;Trojan.Pidief.X;Malware;Malware;Malware;001_9586.pdf;;carriemurgatroyd@shivuk.biz;112.196.17.28;;
7.6.2017 12:28;d4f29a7952f396293c550fd9c8d87e;Trojan.Pidief.X;Malware;Malware;Malware;765GRSMUDPP645.docm;;carriemurgatroyd@shivuk.biz;112.196.17.28;;
7.6.2017 12:29;3b7ad3e6373483cb61cf8612ad780004;Trojan.Pidief.X;Malware;Malware;Malware;001_1005.pdf;;deechurchill@dorafrankeldance.co.uk;182.187.69.191;;
7.6.2017
12:29;a795f5a741005bc3bce64fca377b4e88;W97M.Downloader;Malware;Malware;Malware;843BMJ69KSAS315.docm;;deechurchill@dorafrankeldance.co.uk;182.187.69.191;;
7.6.2017 12:32;;Malicious-URL;Malicious-URL;;sexy-dates.ru;noreply@starburst.com;195.140.195.194;;
7.6.2017 12:32;;Malicious-URL;Malicious-URL;;agileframeknowledge.com;info@FELSITE.it;113.175.188.164;;
7.6.2017 12:37;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;
7.6.2017 12:41;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;notification+bdz1xk68b5u5@northtoalaska.net;194.95.197.248;;
7.6.2017 12:51;;Malicious-URL;;ronwoodall.de;;
7.6.2017 12:52;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;support+azhs5hkagfer@dal.ca;195.208.245.157;;
7.6.2017 13:04;;Malicious-URL;Malicious-URL;;macartu.cn;lcjvbrg@vdtvtech.us;195.46.167.164;;
7.6.2017 13:06;;Malicious-URL;Malicious-URL;;macartu.cn;lvfwzmmmb@hmv-ahlen.de;49.140.201.102;;
7.6.2017 13:15;;Malicious-URL;Malicious-URL;;organictabletinc.ru;mautunes2011@gmail.com.br;198.20.107.90;;
7.6.2017 13:18;;Malicious-URL;Malicious-URL;;senerbuelbuel@yahoo.de;212.227.28.153;;
7.6.2017 13:32;13e4e95ac62bbe22b5ad49d615035d51;NO HIT;;Malware;Malware;931957239796527.zip;;jarib25@ono.com;84.125.216.72;;
7.6.2017 13:32;8f56f7f1b3acc1d540a81f18c8e8a2cc3;NO HIT;;Malware;Malware;2446.zip;;jarib25@ono.com;84.125.216.72;;
7.6.2017 13:32;8fe4cc8c657c7b46a19d3d431851a522;NO HIT;;Malware;Malware;2446.js;;jarib25@ono.com;84.125.216.72;;
7.6.2017 13:40;;Malicious-URL;;info@zimdom.ga;59.153.49.68;;
7.6.2017 13:41;6d168f39cc0a6586f47d16c9ab3dfef4;Trojan.Pidief.X;Malware;Malware;Malware;60681112.pdf;;Olive.4805@cygate.fi;113.162.177.90;;
7.6.2017 13:41;70792b014bf62c2f51c4cc7430907a5;NO HIT;;Malware;Malware;782PUSYMYD562.docm;;Olive.4805@cygate.fi;113.162.177.90;;
7.6.2017 13:42;02c47f04a5e4348d7c832e92dc1fbcbe;Trojan.Pidief.X;Malware;Malware;Malware;97198998.pdf;;Bennett.6065@cygate.fi;210.16.114.252;;
7.6.2017 13:42;438be071a2dbcf73b33ecfcac110ef3;W97M.Downloader;Malware;Malware;Malware;483JDKBRLV120.docm;;Bennett.6065@cygate.fi;210.16.114.252;;
7.6.2017 13:42;9fc9f943270e87cd891dcbf3103d0ced;Trojan.Pidief.X;Malware;Malware;Malware;13149529.pdf;;Tessa.9741@cygate.fi;202.67.42.26;;
7.6.2017 13:42;881b7b8e25b331dd84943dc5f3805;W97M.Downloader;Malware;Malware;Malware;715YMZH8ZEM685.docm;;Tessa.9741@cygate.fi;202.67.42.26;;
7.6.2017 13:43;3d8ed29a5dcd413611f422bba9818802;NO HIT;;Malware;Malware;882CPILZCF466.docm;;Valeria.2376@cygate.fi;14.98.167.161;;
7.6.2017 13:43;7a7a762d79daa5de587da19d21b7b21d;Trojan.Pidief.X;Malware;Malware;Malware;84747549.pdf;;Valeria.2376@cygate.fi;14.98.167.161;;
7.6.2017 13:43;9fc9f943270e87cd891dcbf3103d0ced;Trojan.Pidief.X;Malware;Malware;Malware;36371617.pdf;;Denver.3479@cygate.fi;212.154.17.54;;
7.6.2017 13:45;2ef063f90b7057126b0fce6ba4dfa290;Trojan.Pidief.X;Malware;Malware;Malware;41100360.pdf;;Karyn.8775@cygate.fi;42.114.17.236;;
7.6.2017 13:45;c8117f90c4da1e7ce7ba288dbfbc72af;W97M.Downloader;Malware;Malware;Malware;181MCPMAJ570.docm;;Karyn.8775@cygate.fi;42.114.17.236;;
7.6.2017 13:46;35e96ebf036f69de5b02e9b8c450d46;W97M.Downloader;Malware;Malware;Malware;879QE6LPHF617.docm;;Chi.6741@cygate.fi;197.221.251.23;;
7.6.2017 13:46;d4359e832321e4cd4b5f588ced93d355;Trojan.Pidief;Malware;Malware;Malware;49330324.pdf;;Chi.6741@cygate.fi;197.221.251.23;;
7.6.2017
13:47;06e64a73d5232affb3d5f876e2511558;W97M.Downloader;Malware;Malware;Malware;568MMHVOLX852.docm;;Angelina.5137@cygate.fi;192.140.241.23;;
7.6.2017 13:47;4145fa959f2037094adc75cd17bc521f;Trojan.Pidief;Malware;Malware;Malware;75158689.pdf;;Angelina.5137@cygate.fi;192.140.241.23;;
7.6.2017 13:51;;Malicious-URL;Malicious-URL;;masterlead.info;noreply@starburst.com;212.16.98.57;;
7.6.2017 13:59;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;
7.6.2017 14:05;;Malicious-URL;Malicious-URL;;macartu.cn;qfwrdsasid@hmv.at;49.140.201.102;;
7.6.2017 14:05;;Malicious-URL;;055093.com;;
7.6.2017 14:22;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;notification+wf02hn0x83xq@amazon.com;64.6.250.4;;
7.6.2017 14:31;;Malicious-URL;Malicious-URL;;organictabletinc.ru;;
7.6.2017 14:31;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;support+p0jktfgtwei0@planet.nl;85.91.32.64;;
7.6.2017 14:33;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;tmanderson@vegasrealtors.org;69.163.176.140;;
7.6.2017 14:35;;Malicious-URL;Malicious-URL;;organictabletinc.ru;support+o3i9nvzz5cn@accenture.com;85.25.198.248;;
7.6.2017 14:35;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;support+5ad0xfw408wi@netscape.net;62.113.236.99;;
7.6.2017 14:41;;Malicious-URL;Malicious-URL;;macartu.cn;foasasror@hmshost.com.au;91.134.253.214;;
7.6.2017 14:41;;Malicious-URL;;payzure.com;;
7.6.2017 14:43;;Malicious-URL;;blackyun.net;;
7.6.2017 14:43;;Malicious-URL;Malicious-URL;;medicemall.com;;
7.6.2017 14:47;;Malicious-URL;;info@rahoitustuki.fi;62.138.0.226;;
7.6.2017 15:10;9de451bcf1f9af27e5b5ef15f566cda;W97M.Downloader;Malware;Malware;Malware;SCAN_4392.doc;Marco@watermolenbels.nl;117.253.55.163;;
7.6.2017 15:11;a7efb54c2e5b22ef4cad5c3af375664;W97M.Downloader;Malware;Malware;Malware;SCAN_6968.doc;Betty@gabok.net;123.17.168.222;;
7.6.2017 15:12;d360109d170adf2d706313217349db1e;Trojan.Gen.NPE;Malware;Malware;Malware;SCAN_4393.doc;Theodore@apesoft.com;122.172.99.61;;
7.6.2017 15:13;d360109d170adf2d706313217349db1e;Trojan.Gen.NPE;Malware;Malware;Malware;SCAN_1062.doc;Quinn@diegotorroja.com;103.51.223.139;;
7.6.2017 15:14;094d2c69d3445677e4f74549e500daf5;W97M.Downloader;Malware;Malware;Malware;SCAN_9468.doc;Tiffany@sjjb.com;14.162.186.41;;
7.6.2017 15:15;3e5d63b93a68d715f7559f4228523f4;W97M.Downloader;Malware;Malware;Malware;SCAN_8406.doc;Graciela@digitaldecor.pt;122.168.113.128;;
7.6.2017 15:15;3e5d63b93a68d715f7559f4228523f4;W97M.Downloader;Malware;Malware;Malware;SCAN_2074.doc;Neil@roethlisberger.org;117.222.208.61;;
7.6.2017 15:15;cb563b18f432105ccbf0ecbb447013a;Trojan.Mdropper;Malware;Malware;B9BDY5Y8X.doc;daemon@localhost.localdomain;195.120.19.68;;
7.6.2017 15:16;;Malicious-URL;Malicious-URL;;medicalrxquality.su;myerscyn@dhhs.state.sc.us;198.154.249.187;;
7.6.2017 15:17;63a14d3a62e6b9c857b56e15fcfaa58;Trojan.Gen.NPE;Malware;Malware;Malware;SCAN_8210.doc;Gregorio@laserspot.ca;42.113.238.89;;
7.6.2017 15:17;6a7cf1a01e4f11c742e88866a207ead;W97M.Downloader;Malware;Malware;Malware;SCAN_9058.doc;Maude@facio.com;117.232.96.253;;
7.6.2017 15:25;f5b5dde909097af272a419c3cf72630;W97M.Downloader;Malware;Malware;Malware;SCAN_1082.doc;Roy@askmebot.com;93.66.231.78;;
7.6.2017 15:26;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;cnxusb@0428.net;49.140.87.162;;
7.6.2017 15:26;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;xmxdgicdd@0451.com;49.140.87.162;;
7.6.2017 15:26;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;hoplumsua@04s.com;49.140.87.162;;
7.6.2017 15:28;43a9d6e86d0f66fba7f8f715f7cb7a23;TROJ_GENZM.F299E00FD17;Malware;Malware;Malware;SCAN_2965.doc;Flossie@cho.com.tw;103.88.24.6;;
7.6.2017
15:29;43a9d6e86d0f66fba7f8f715f7cb7a23;TROJ_GENZM.F299E00FD17;Malware;Malware;Malware;SCAN_5911.doc;Pedro@lccolombia.com;217.21.146.149;;
7.6.2017 15:30;ceb968d2153051c3f800d8d941a7dcb;W97M.Downloader;Malware;Malware;Malware;SCAN_1001.doc;Josefina@rigdoninc.com;190.145.53.222;;
7.6.2017 15:47;;Malicious-URL;;info-disney@disneylandparis.magical-ears.com;195.154.153.211;;
7.6.2017 15:56;;Malicious-URL;;support@nikonoutlets.eu;212.16.98.57;;
7.6.2017 15:58;;Malicious-URL;;forums@developer.bmc.com;204.93.64.116;;
7.6.2017 16:00;;Malicious-URL;Malicious-URL;;macartu.cn;emrbjupvma@hmsheridan.co.uk;49.140.172.69;;
7.6.2017 16:03;;Malicious-URL;;arno@armati.nl;115.248.17.50;;
7.6.2017 16:08;;Malicious-URL;Malicious-URL;;macartu.cn;info@rahoitustuki.fi;95.211.241.74;;
7.6.2017 16:13;;Malicious-URL;;bdszgzvy@hmsinet.ca;51.254.49.147;;
7.6.2017 16:18;cb563b18f432105ccbf0ecbb447013a;Trojan.Mdropper;Malware;Malware;B9BDY5Y8X.doc;sales@customer-care.sap;195.120.19.68;;
7.6.2017 16:26;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;eivvysjw@08.com;27.197.185.128;;
7.6.2017 16:32;;Malicious-URL;Malicious-URL;;medicalrxquality.su;shelby.davis@microsoft.com;47.89.48.123;;
7.6.2017 16:47;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;meganstroud@live.co.uk;81.169.220.186;;
7.6.2017 16:53;;Malicious-URL;Malicious-URL;;amino-disqus.club;;
7.6.2017 16:57;ba992424ebf7e4cd1ecbc2130707cc4c;NO HIT;Malware;Malware;Malware;SCAN_4668.doc;Alejandro@uwin4u.com;14.165.65.44;;
7.6.2017 17:00;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e34934425810.zip;copier@cygate.fi;123.252.225.111;;
7.6.2017 17:00;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e78752584728.zip;copier@cygate.fi;58.187.69.249;;
7.6.2017 17:01;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e19858391379.zip;copier@cygate.fi;179.33.9.85;;
7.6.2017 17:01;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e72568308701.zip;copier@cygate.fi;179.33.9.85;;
7.6.2017 17:01;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e89481235114.zip;copier@cygate.fi;61.3.212.97;;
7.6.2017 17:02;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e41694211073.zip;copier@cygate.fi;106.76.70.245;;
7.6.2017 17:03;fc03609eaf5db69c3a064e0534ca5669;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_8689.doc;Nona@sablebooks.org;185.108.124.26;;
7.6.2017 17:04;af0f35811a769e4f12da663003fa8fb2;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_1498.doc;Allen@janditours.com;59.95.146.94;;
7.6.2017
17:04;fc03609eaf5db69c3a064e0534ca5669;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_8117.doc;Antonia@burrowlaw.com;190.143.131.219;;
7.6.2017 17:04;fc03609eaf5db69c3a064e0534ca5669;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_5774.doc;Asa@bebs.screaming.net;103.44.14.18;;

7.6.2017 17:04;fc03609eaf5db69c3a064e0534c5a669;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_7234.doc;;Carissa@howardkay.ca;62.120.1.77;;

7.6.2017 17:04;fc03609eaf5db69c3a064e0534c5a669;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_9362.doc;;Geraldine@badstue.edu;122.175.44.104;;

7.6.2017 17:04;;Malicious-URL;Malicious-URL;;organictabletinc.ru;update+wsxrvovyzc8@live.de;176.56.61.15;;

7.6.2017 17:05;15c654e355328e4aa8abc16042ec5af;NO HIT;Malware;Malware;Malware;SCAN_0029.doc;;Brigitte@web3d-fr.com;94.62.215.57;;

7.6.2017

17:05;fc03609eaf5db69c3a064e0534c5a669;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_4857.doc;;Herminia@timegoneamusements.com.au;197.2.20.5.228;;

7.6.2017 17:05;;Malicious-URL;Malicious-URL;;eveningmanga.com;info@eveningmanga.com;89.38.97.50;;

7.6.2017 17:15;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e63276006337.zip;;copier@cygate.fi;190.68.227.82;;

7.6.2017

17:16;5768d7f8c43a1c4c61437a7560bcc39a;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_3938.doc;;Chet@fitnessfocusclub.com;117.201.212.255;;

7.6.2017

17:16;5768d7f8c43a1c4c61437a7560bcc39a;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_4538.doc;;Stephanie@deasartcollection.com;113.160.148.38;;

7.6.2017 17:17;0fc6985f32bebb314de6293ae4ce26c;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_9424.doc;;Herbert@pixie-bobs.com;82.127.208.231;;

7.6.2017 17:17;0fc6985f32bebb314de6293ae4ce26c;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_7331.doc;;Marylou@jbfreeman.net;46.248.40.91;;

7.6.2017

17:17;0fc6985f32bebb314de6293ae4ce26c;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_6854.doc;;William@nalandacollege.lk;103.66.79.147;;

7.6.2017 17:17;0b23d3a6f94dd9f2299d9786b4e99b9f;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_5650.doc;;Pansy@espitia.net;114.134.189.166;;

7.6.2017

17:18;0fc6985f32bebb314de6293ae4ce26c;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_1231.doc;;Daren@hareonline.net;117.200.176.163;;

7.6.2017 17:21;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e18771888185.zip;;copier@cygate.fi;82.99.210.94;;

7.6.2017 17:24;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e3655727407.zip;;copier@rescom.fi;103.77.63.131;;

7.6.2017 17:24;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e17813789511.zip;;copier@cygate.fi;103.77.63.131;;

7.6.2017 17:25;5768d7f8c43a1c4c61437a7560bcc39a;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_9224.doc;;Jere@kma.ro;200.71.114.10;;

7.6.2017 17:26;;Malicious-URL;Malicious-URL;;familierabatnordic.dk;forums@developer.bmc.com;204.93.64.117;;

7.6.2017 17:28;;Malicious-URL;;hxxp://tee2green.org/viewdoc/file.php?document=YXpLmhvG9wYWluZW5AY3lnYXRlMzP;accounting@thomewaterproofing.com;12.217.198.82;;

7.6.2017 17:30;;Malicious-URL;Malicious-URL;;medicemail.com;;

7.6.2017 17:33;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e32164127735.zip;;copier@cygate.fi;106.66.138.234;;

7.6.2017 17:33;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e37504928777.zip;;copier@cygate.fi;78.188.96.189;;

7.6.2017 17:38;;Malicious-URL;;hxxp://PAMTRHELANDGAL.COM/viewdoc/file.php?document=cMvpbWUeUGvY9AY3lnYXRlMzP;accounting@thomewaterproofing.com;50.198.212.241;;

7.6.2017 17:39;;Malicious-URL;;hxxp://theglannfamily.com/viewdoc/file.php?document=YW50dGkuamFhc2l1bGZpbnVUQGN5Z2F0ZS5maQ==;accounting@thomewaterproofing.com;72.205.179.215;;

7.6.2017 17:40;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e31554426251.zip;;copier@cygate.fi;27.4.218.120;;

7.6.2017

17:40;af604b3209c19727d8c18574a0569fdc;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_3329.doc;;Sophia@memoriespreserve.com;14.184.56.124;;

7.6.2017 17:41;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e20713141085.zip;;copier@cygate.fi;115.79.210.230;;

7.6.2017 17:41;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e45925224201.zip;;copier@cygate.fi;202.179.279.230;;

7.6.2017 17:41;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e75207986532.zip;;copier@cygate.fi;27.106.100.130;;

7.6.2017

17:43;43a9d6e86d0f66b7a7f8f715f7cb7a23;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_1987.doc;;Lakisha@happyhewitts.com;103.207.131.103;;

7.6.2017

17:43;43a9d6e86d0f66b7a7f8f715f7cb7a23;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_6756.doc;;Saul@eru.user.lysator.liu.se;58.186.98.244;;

7.6.2017 17:43;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e45556479949.zip;;copier@cygate.fi;213.74.17.114;;

7.6.2017 17:43;;Malicious-URL;;hxxp://sandbaggersgolf.club/viewdoc/file.php?document=cGF1bGEucGFra2FuZW5AY3lnYXRlMzP;accounting@thomewaterproofing.com;70.61.88.106;;

7.6.2017 17:44;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e22812525269.zip;;copier@cygate.fi;42.115.192.34;;

7.6.2017 17:44;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e46123301802.zip;;copier@cygate.fi;102.164.77.42;;

7.6.2017 17:44;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e53399378188.zip;;copier@cygate.fi;154.70.88.120;;

7.6.2017 17:44;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e6972966280.zip;;copier@cygate.fi;190.7.159.178;;

7.6.2017

17:44;76e4b95338aa99c55d2c16a21d0e280;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_4763.doc;;Terra@consultingaxis.com;45.120.62.173;;

7.6.2017 17:45;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e3215363411.zip;;copier@cygate.fi;132.255.80.62;;

7.6.2017 17:45;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e68464086090.zip;;copier@cygate.fi;103.61.253.222;;

7.6.2017 17:45;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e97637902535.zip;;copier@cygate.fi;113.176.61.74;;

7.6.2017 17:46;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e10756437008.zip;;copier@cygate.fi;185.106.31.91;;

7.6.2017 17:46;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e39037994512.zip;;copier@cygate.fi;182.156.202.18;;

7.6.2017 17:47;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e15698400808.zip;;copier@cygate.fi;109.224.58.35;;

7.6.2017 17:47;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e71321685351.zip;;copier@cygate.fi;14.229.230.44;;

7.6.2017 17:48;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e94748015543.zip;;copier@cygate.fi;14.139.208.241;;

7.6.2017

17:49;57ccd4a0da1677b7f4de08eb97905285;TROJ_GENZM.F299E00F917;Malware;Malware;Malware;SCAN_7832.doc;;Glenda@levine19.com;103.219.244.166;;

7.6.2017

17:49;57ccd4a0da1677b7f4de08eb97905285;TROJ_GENZM.F299E00F917;Malware;Malware;Malware;SCAN_7457.doc;;Matt@antifashion.com.br;116.202.32.45;;

7.6.2017 17:51;f695ee8da9e9aecd2d0ec1bf0597582b;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_5154.doc;;Sasha@n3uij.com;113.174.159.133;;

7.6.2017 17:53;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e5711946970.zip;;copier@cygate.fi;14.182.108.13;;

7.6.2017 17:56;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e04121646551.zip;;copier@cygate.fi;190.96.220.84;;

7.6.2017 17:57;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e34486019724.zip;;copier@cygate.fi;82.17.252.55;;

7.6.2017 17:57;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e77113211395.zip;;copier@cygate.fi;14.187.112.31;;

7.6.2017 17:57;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e85141256440.zip;;copier@cygate.fi;118.137.216.82;;

7.6.2017 17:57;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e97313730010.zip;;copier@cygate.fi;113.23.20.255;;

7.6.2017 17:57;dc142463372f178be9894e2814f15218;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_2573.doc;;Stuart@glorysigns.com;1.186.46.26;;

7.6.2017 17:58;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e71125646920.zip;;copier@cygate.fi;41.136.200.198;;

7.6.2017 17:59;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e09423746937.zip;;copier@cygate.fi;210.210.72.154;;

7.6.2017 17:59;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e27712022736.zip;;copier@cygate.fi;37.26.81.146;;

7.6.2017 17:59;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e34308129888.zip;;copier@cygate.fi;113.22.171.174;;

7.6.2017 17:59;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e39695524022.zip;;copier@cygate.fi;143.137.206.66;;

7.6.2017 17:59;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e45525018027.zip;;copier@cygate.fi;203.115.107.117;;

7.6.2017 17:59;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e78915989241.zip;;copier@cygate.fi;195.142.102.202;;

7.6.2017 17:59;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e88444865380.zip;;copier@cygate.fi;14.166.230.133;;

7.6.2017

18:00;510bf0e2f47714de8a223a8901b6c254;TROJ_GENZM.F299E00F917;Malware;Malware;Malware;SCAN_8834.doc;;Ben@envirotechomes.com.au;123.176.6.250;;

7.6.2017 18:00;510bf0e2f47714de8a223a8901b6c254;TROJ_GENZM.F299E00F917;Malware;Malware;Malware;SCAN_8542.doc;;Herminia@bogent.com;123.176.6.250;;

7.6.2017 18:00;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e88455485190.zip;;copier@cygate.fi;125.99.169.242;;

7.6.2017 18:01;;Malicious-URL;;hxxp://tee2greenaz.com/viewdoc/file.php?document=cGV0cmkuaGZpbnVUZW5AY3lnYXRlMzP;accounting@thomewaterproofing.com;64.81.223.162;;

7.6.2017 18:04;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e01742076932.zip;;copier@cygate.fi;161.132.96.90;;

7.6.2017 18:11;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e88868107361.zip;;copier@cygate.fi;103.225.206.50;;

7.6.2017 18:11;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e918711103011.zip;;copier@cygate.fi;103.225.206.50;;

7.6.2017 18:11;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e94594957999.zip;;copier@cygate.fi;202.142.151.194;;

7.6.2017 18:12;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e86963246615.zip;;copier@cygate.fi;37.255.78.0;;

7.6.2017 18:12;;Malicious-URL;;hxxp://tee2green.co/viewdoc/file.php?document=YW50dGkudHVvbWVub2tZUBjeWdhdGUuZmk=;accounting@thomewaterproofing.com;70.60.68.118;;

7.6.2017 18:13;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e3227513612.zip;;copier@cygate.fi;189.90.246.113;;

7.6.2017 18:14;;;Malicious-URL;hxxp://tee2green.com/viewdoc/file.php?document=dMvZySSzWh0aW5lkb8jeWdhGUuZmk=;accounting@thomewaterproofing.com;75.144.55.73;;

7.6.2017 18:20;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e72585165374.zip;;copier@cygate.fi;190.0.51.46;;

7.6.2017 18:21;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e12259691619.zip;;copier@cygate.fi;113.190.16.214;;

7.6.2017 18:21;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e54596836009.zip;;copier@cygate.fi;27.5.64.111;;

7.6.2017 18:22;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e55318718229.zip;;copier@cygate.fi;213.14.44.38;;

7.6.2017 18:22;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e90130914885.zip;;copier@cygate.fi;113.184.178.168;;

7.6.2017 18:22;;;Malicious-URL;hxxp://fenixconnection.com/viewdoc/file.php?document=YW5kZjZlNnR2dZdGVyQGN5Z2F0Z55maQ=;accounting@thomewaterproofing.com;24.128.139.92;;

7.6.2017 18:22;;;Malicious-URL;hxxp://tee2green.com/viewdoc/file.php?document=cGV0cmkua2FuZjY2YUJjeWdhGUuZmk=;accounting@thomewaterproofing.com;98.26.73.22;;

7.6.2017 18:23;;;Malicious-URL;Malicious-URL;;medicalrxquality.su;yunal@turknet.com;46.253.206.217;;

7.6.2017 18:27;57e6901939708a1621b9c6d46edae2a4;TROJ_GENZM.F299E00F817;Malware;Malware;Malware;SCAN_8502.doc;;Anita@urbantool.com;106.200.219.127;;

7.6.2017 18:29;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e00279124973.zip;;copier@cygate.fi;119.76.101.117;;

7.6.2017 18:29;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e72041045338.zip;;copier@cygate.fi;112.133.245.109;;

7.6.2017 18:30;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e12518579441.zip;;copier@cygate.fi;77.29.117.108;;

7.6.2017 18:31;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e52022788044.zip;;copier@cygate.fi;61.0.136.237;;

7.6.2017 18:32;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e94874181052.zip;;copier@cygate.fi;200.58.75.221;;

7.6.2017 18:33;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e48453767973.zip;;copier@cygate.fi;37.6.1.182;;

7.6.2017 18:34;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e11738852692.zip;;copier@cygate.fi;197.27.71.250;;

7.6.2017 18:34;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e50776741666.zip;;copier@cygate.fi;14.163.151.76;;

7.6.2017 18:36;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e31874793044.zip;;copier@cygate.fi;143.137.206.3;;

7.6.2017 18:37;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e12956707928.zip;;copier@cygate.fi;190.143.1.14;;

7.6.2017 18:37;710d31d3ad854350b941814ba7c430fe;Trojan.Gen.7;Malware;Malware;Malware;SKM_C224e74063810364.zip;;copier@cygate.fi;123.252.222.174;;

7.6.2017 18:37;;;Malicious-URL;hxxp://tee2green.org/viewdoc/file.php?document=bGFyaS5wYWFzdGVsYUJjeWdhGUuZmk=;accounting@thomewaterproofing.com;109.66.153.223;;

7.6.2017 18:37;;;Malicious-URL;hxxp://tee2green.com/viewdoc/file.php?document=amFubmUucGVsdG9sYUJjeWdhGUuZmk=;accounting@thomewaterproofing.com;216.45.76.83;;

7.6.2017 18:39;;;Malicious-URL;hxxp://sandbaggersgolf.club/viewdoc/file.php?document=dmlsbGUuHVvdG9AY3InYXRlMzZp;accounting@thomewaterproofing.com;24.206.34.42;;

7.6.2017 18:40;;;Malicious-URL;hxxp://tee2green.co/viewdoc/file.php?document=amFyaS5iYWFyWfUuQGN5Z2F0Z55maQ=;accounting@thomewaterproofing.com;50.253.16.25;;

7.6.2017 18:42;;;Malicious-URL;Malicious-URL;amino-diskus.club;;

7.6.2017 19:05;;;Malicious-URL;Malicious-URL;;macartu.cn;647406844536801.XH38406@hii.ms Sheridan.co.uk;200.119.89.148;;

7.6.2017 19:11;;;Malicious-URL;Malicious-URL;Malicious-URL;hxxp://SOUTHLINEINDUSTRIAL.NET/viewdoc/file.php?document=cGF1bGEucGFra2FuZW5AY3InYXRlMzZp;accounting@thomewaterproofing.com;216.239.225.100;;

7.6.2017 19:13;;;Malicious-URL;Malicious-URL;;thaigooglerank.com;b874f46@sgcom.com.sg;171.229.83.171;;

7.6.2017 19:15;;;Malicious-URL;Malicious-URL;Malicious-URL;hxxp://SOUTHLINEINDUSTRIAL.CA/viewdoc/file.php?document=cGFzaS5iYWFtbnVuQGN5Z2F0Z55maQ=;accounting@thomewaterproofing.com;173.191.123.178;;

7.6.2017 19:19;;;Malicious-URL;Malicious-URL;Malicious-URL;hxxp://SOUTHLINEINDUSTRIAL.CA/viewdoc/file.php?document=YW50dGkubGVodG9uZW5AY3InYXRlMzZp;accounting@thomewaterproofing.com;173.24.224.220;;

7.6.2017 19:21;;;Malicious-URL;Malicious-URL;hxxp://BINFORDTOOL.COM/viewdoc/file.php?document=bWF0dGkua2FoaWxhQGN5Z2F0Z55maQ=;accounting@thomewaterproofing.com;96.94.65.61;;

7.6.2017 19:21;;;Malicious-URL;Malicious-URL;hxxp://fitnesssuperstore-bestbuy.com/viewdoc/file.php?document=amFubmUucGVsdG9sYUJjeWdhGUuZmk=;accounting@thomewaterproofing.com;74.92.209.62;;

7.6.2017 19:22;;;Malicious-URL;Malicious-URL;hxxp://fitnesssuperstore-bestbuy.com/viewdoc/file.php?document=dG9taS5rYXJsc3NvbK8jeWdhGUuZmk=;accounting@thomewaterproofing.com;207.172.210.14;;

7.6.2017 19:24;;;Malicious-URL;Malicious-URL;hxxp://BINFORDTOOL.COM/viewdoc/file.php?document=bGFyaS5wYWFzdGVsYUJjeWdhGUuZmk=;accounting@thomewaterproofing.com;70.116.162.251;;

7.6.2017 19:33;;;Malicious-URL;Malicious-URL;hxxp://CRAFTSDUJOUR.COM/viewdoc/file.php?document=dG9taS5iYWF0dGluZW5AY3InYXRlMzZp;accounting@thomewaterproofing.com;173.197.123.2;;

7.6.2017 19:38;;;Malicious-URL;Malicious-URL;Malicious-URL;hxxp://SOUTHLINEINDUSTRIAL.CA/viewdoc/file.php?document=bWF0dGkua2FoaWxhQGN5Z2F0Z55maQ=;accounting@thomewaterproofing.com;24.229.64.163;;

7.6.2017 19:38;;;Malicious-URL;Malicious-URL;hxxp://BINFORDTOOL.COM/viewdoc/file.php?document=dHVvbW8udHVya2tpQGN5Z2F0Z55maQ=;accounting@thomewaterproofing.com;204.9.127.114;;

7.6.2017 19:38;;;Malicious-URL;Malicious-URL;hxxp://CRAFTSDUJOUR.COM/viewdoc/file.php?document=YW50dGkua2FubmluZW5AY3InYXRlMzZp;accounting@thomewaterproofing.com;63.90.67.147;;

7.6.2017 19:39;;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;d.ziola@onet.eu;117.1.232.23;;

7.6.2017 19:40;;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;cfedgoajiji@000webhost.com;221.145.242.67;;

7.6.2017 19:40;;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;aoivfyo@006.com;101.75.36.244;;

7.6.2017 19:45;;;Malicious-URL;;vgqhiulua@002.com;60.215.154.34;;

7.6.2017 19:46;;;Malicious-URL;Malicious-URL;hxxp://CRAFTSDUJOUR.COM/viewdoc/file.php?document=YXJpLmhvbg9wYWluZW5AY3InYXRlMzZp;accounting@thomewaterproofing.com;98.109.70.33;;

7.6.2017 19:48;;;Malicious-URL;Malicious-URL;hxxp://fitnesssuperstore-bestbuy.com/viewdoc/file.php?document=YW50dGkubGVodG9uZW5AY3InYXRlMzZp;accounting@thomewaterproofing.com;66.37.80.210;;

7.6.2017 19:52;;;Malicious-URL;Malicious-URL;hxxp://fitnesssuperstore-bestbuy.com/viewdoc/file.php?document=YW50dGkuamFhc2t1bG9pbnVucGVsdG9sYUJjeWdhGUuZmk=;accounting@thomewaterproofing.com;173.220.28.90;;

7.6.2017 20:02;;;Malicious-URL;Malicious-URL;hxxp://fitnesssuperstore-bestbuy.com/viewdoc/file.php?document=bWlrYWVwLnNhbXZvbGFAY3InYXRlMzZp;accounting@thomewaterproofing.com;69.74.235.4;;

7.6.2017 20:04;;;Malicious-URL;Malicious-URL;hxxp://BINFORDTOOL.COM/viewdoc/file.php?document=cGV0cmkuaGVpbm9uZW5AY3InYXRlMzZp;accounting@thomewaterproofing.com;76.79.153.226;;

7.6.2017 20:06;;;Malicious-URL;Malicious-URL;hxxp://BEDFORDTOOL.COM/viewdoc/file.php?document=YXJ0b3Y5aXVra29uZW5AY3InYXRlMzZp;accounting@thomewaterproofing.com;75.148.31.230;;

7.6.2017 20:06;;;Malicious-URL;Malicious-URL;hxxp://CRAFTSDUJOUR.COM/viewdoc/file.php?document=YW5kZjZlNnR2dZdGVyQGN5Z2F0Z55maQ=;accounting@thomewaterproofing.com;67.133.88.52;;

7.6.2017 20:07;7bfbcc0db913ee68a85c3bdcc232;Trojan.Gen.2;;Malware;Malware;PO34215.zip;;mail@sawawada.com;84.38.129.169;;

7.6.2017 20:07;7d5855214b4b68b21d03ef57cc8d6182;CLEAN - False Positive;;Malware;Malware;PO34216.jar;;mail@sawawada.com;84.38.129.169;;

7.6.2017 20:07;b5eb5c83a1e7c41e9aee94769b710af;Trojan.Gen.2;;Malware;Malware;PO34215.exe;;mail@sawawada.com;84.38.129.169;;

7.6.2017 20:07;d4f39d0b25d8c1b0aa5e47701b4e453d;HEUR: Trojan.Java.Agent.gen;;Malware;Malware;PO34216.pdf.zip;;mail@sawawada.com;84.38.129.169;;

7.6.2017 20:12;;;Malicious-URL;Malicious-URL;Malicious-URL;hxxp://SOUTHLINEINDUSTRIAL.NET/viewdoc/file.php?document=aGFycmVudG9sYUJjeWdhGUuZmk=;accounting@thomewaterproofing.com;70.89.211.1;;

7.6.2017 20:12;;;Malicious-URL;;southlineindustrial.net;;

7.6.2017 20:16;;;Malicious-URL;Malicious-URL;hxxp://fitnesssuperstore-bestbuy.com/viewdoc/file.php?document=cHVyY2hc2VAY3InYXRlMzZp;accounting@thomewaterproofing.com;12.198.46.226;;

7.6.2017 20:25;;;Malicious-URL;Malicious-URL;;dock.email;kampanja@slowcolor.info;185.99.122.103;;

7.6.2017 20:36;;;Malicious-URL;Malicious-URL;hxxp://BINFORDTOOL.COM/viewdoc/file.php?document=bWlrYWVwLnNhbXZvbGFAY3InYXRlMzZp;accounting@thomewaterproofing.com;40.134.185.183;;

7.6.2017 20:52;;;Malicious-URL;Malicious-URL;hxxp://BEDFORDTOOL.COM/viewdoc/file.php?document=am9ha2ltLnVzWhYQGN5Z2F0Z55maQ=;accounting@thomewaterproofing.com;72.95.135.26;;

7.6.2017 20:52;;;Malicious-URL;Malicious-URL;hxxp://BINFORDTOOL.COM/viewdoc/file.php?document=dG9taS5rYXJsc3NvbK8jeWdhGUuZmk=;accounting@thomewaterproofing.com;50.199.82.209;;

7.6.2017 20:52;;;Malicious-URL;Malicious-URL;;binfordtool.com;cfbjpgwgnwm@ffguerins.us;64.90.88.50;;

7.6.2017 20:52;;;Malicious-URL;Malicious-URL;;macartu.cn;Farrell_Rick@bcoe.butte.k12.ca.us;64.90.88.50;;

7.6.2017 20:53;;;Malicious-URL;Malicious-URL;hxxp://fitnesssuperstore-bestbuy.com/viewdoc/file.php?document=dG9taS5rYXJsc3NvbK8jeWdhGUuZmk=;accounting@thomewaterproofing.com;70.166.4.228;;

7.6.2017 20:54;;Malicious-URL;;Malicious-URL;;hxxp://CRAFTSDUJOUR.COM/viewdoc/file.php?document=amFya2tVlnJpdmlub2phGNSZ2F0Z55maQ==;accounting@thomewaterproofing.com;192.119.249.166;;

7.6.2017 20:56;;Malicious-URL;;Malicious-URL;;hxxp://BINFORDTOOL.COM/viewdoc/file.php?document=YXJpLmhvbG9wYWUwZ5AY3InYXRlMzP;accounting@thomewaterproofing.com;12.204.205.22;;

7.6.2017 20:56;;Malicious-URL;;Malicious-URL;;hxxp://www.nutrisihidroponik.com/wp-content/plugins/woocommerce/includes/gateways/5966bcf593f.html;jpsnack@gleason.com;41.65.49.137;;

7.6.2017 20:57;;Malicious-URL;;Malicious-URL;;us-mkhandbags.com;no-reply@no-reply.xinshangmeng.top;134.119.212.189;;

7.6.2017 20:59;;Malicious-URL;;Malicious-URL;;us-mkhandbags.com;no-reply@no-reply.xinshangmeng.top;134.119.212.189;;

7.6.2017 21:01;;Malicious-URL;;Malicious-URL;;us-mkhandbags.com;no-reply@no-reply.xinshangmeng.top;134.119.212.180;;

7.6.2017 21:04;;Malicious-URL;;Malicious-URL;;Malicious-URL;;hxxp://SOUTHLINEINDUSTRIAL.NET/viewdoc/file.php?document=bWlrYWVwLnBhYXZvbGFAY3InYXRlMzP;accounting@thomewaterproofing.com;24.205.124.141;;

7.6.2017 21:07;;Malicious-URL;;Malicious-URL;;hxxp://BEDFORDTOOL.COM/viewdoc/file.php?document=YW5uZ55oZW5yaXRpdXNAY3InYXRlMzP;accounting@thomewaterproofing.com;208.80.208.4;;

7.6.2017 21:16;;Malicious-URL;;Malicious-URL;;organictabletinc.ru;vjlogo11@netzero.com;203.217.101.237;;

7.6.2017 21:26;;Malicious-URL;;Malicious-URL;;hxxp://fitnesssuperstore-bestbuy.com/viewdoc/file.php?document=YW50dGkua2FubmluZ5AY3InYXRlMzP;accounting@thomewaterproofing.com;75.134.86.178;;

7.6.2017 21:26;;Malicious-URL;;Malicious-URL;;macartu.cn;kslodkgs@hmsost.com.au;50.199.157.91;;

7.6.2017 21:37;;Malicious-URL;;Malicious-URL;;hxxp://fitnesssuperstore-bestbuy.com/viewdoc/file.php?document=anVoY550b2l2b25lkbjEwdhdGUuZmk=;accounting@thomewaterproofing.com;207.172.210.14;;

7.6.2017 21:54;;Malicious-URL;;Malicious-URL;;Malicious-URL;;hxxp://SOUTHLINEINDUSTRIAL.CA/viewdoc/file.php?document=YW5kZXJzLnNrb2d2dGVyQGN5Z2F0Z55maQ==;accounting@thomewaterproofing.com;70.119.148.233;;

7.6.2017 21:58;;Malicious-URL;;Malicious-URL;;medicalrxreward.ru;lenka.bohackova@seznam.cz;199.103.60.137;;

7.6.2017 22:08;;Malicious-URL;;Malicious-URL;;medicalrxquality.su;warranty@freenet.de;74.208.7.50;;

7.6.2017 22:10;;Malicious-URL;;Malicious-URL;;jclicks.space;ilona@srv.sendings.eu;207.154.228.13;;

7.6.2017 22:30;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

7.6.2017 22:32;;Malicious-URL;;Malicious-URL;;medicalrxquality.su;update+9j21fmil1sqy@edu.trosa.se;74.208.201.98;;

7.6.2017 22:41;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

7.6.2017 22:49;;Malicious-URL;;Malicious-URL;;medicalrxquality.su;smokeytm@consolidated.net;104.131.183.166;;

7.6.2017 22:53;;Malicious-URL;;Malicious-URL;;medicalrxquality.su;notification+f6j6pcfsdvy4@cs.com;202.78.200.106;;

7.6.2017 22:59;;Malicious-URL;;Malicious-URL;;basedbusinesstraffic.com;pedugufu5@gmail.com;180.178.44.250;;

7.6.2017 22:59;;Malicious-URL;;Malicious-URL;;organictabletinc.ru;notification+y055g2jeweo2@hotmail.fr;172.104.43.83;;

7.6.2017 22:59;;Malicious-URL;;Malicious-URL;;organictabletinc.ru;notification+g617qqmningx@sars.gov.za;104.236.201.222;;

7.6.2017 23:00;;Malicious-URL;;Malicious-URL;;dingzhijiu8.com;lizheng@handbb.com;121.12.119.42;;

7.6.2017 23:03;;Malicious-URL;;Malicious-URL;;medicalrxreward.ru;support+sirqphgsiarn@owens-minor.com;217.199.164.157;;

7.6.2017 23:25;;Malicious-URL;;Malicious-URL;;medicalrxquality.su;support+ss6mxo1na532@millenniumbcp.pt;87.106.30.195;;

7.6.2017 23:31;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

7.6.2017 23:57;;Malicious-URL;;hxxp://www.freshinfo.com.ng/wp-includes/js/tinymce/plugins/directionality/41130f95a7d.html;kittybennettow@excite.it;190.166.89.74;;

7.6.2017 23:58;;Malicious-URL;;Malicious-URL;;sexy-dates.ru;info@STREAM.it;87.155.239.178;;

8.6.2017 0:11;;Malicious-URL;;Malicious-URL;;macartu.cn;pkhfwmg@calabria.us;182.92.225.78;;

8.6.2017 0:11;;Malicious-URL;;Malicious-URL;;macartu.cn;ztgagkqqw@khayts.us;182.92.225.78;;

8.6.2017 0:13;;Malicious-URL;;Malicious-URL;;amino-disqus.club;info@teeforlinkedin.club;185.141.206.34;;

8.6.2017 0:40;;Malicious-URL;;Malicious-URL;;firstmedsprogram.ru;dmbrseyi@0126.com;110.242.155.131;;

8.6.2017 0:48;;Malicious-URL;;Malicious-URL;;firstmedsprogram.ru;lvypkpkxe@013.com;171.126.201.71;;

8.6.2017 0:54;;Malicious-URL;;Malicious-URL;;macartu.cn;136464568852068.WG23387@umu.hmsost.com;179.111.242.56;;

8.6.2017 1:10;;Malicious-URL;;Malicious-URL;;sexy-dates.ru;info@SYRINGE.it;189.192.250.205;;

8.6.2017 1:12;;Malicious-URL;;Malicious-URL;;sexy-dates.ru;info@SELENITE.nl;181.166.133.81;;

8.6.2017 1:15;;Malicious-URL;;Malicious-URL;;sexy-dates.ru;info@SHINY.br;41.248.247.161;;

8.6.2017 1:18;;Malicious-URL;;Malicious-URL;;sexy-dates.ru;info@TATE.pl;113.168.85.237;;

8.6.2017 1:21;;Malicious-URL;;Malicious-URL;;macartu.cn;345370704786040.MN64617@rndl.hmx.de;37.186.201.151;;

8.6.2017 1:21;;Malicious-URL;;Malicious-URL;;sexy-dates.ru;info@PROTESTANT.br;113.168.180.236;;

8.6.2017 1:29;;Malicious-URL;;Malicious-URL;;macartu.cn;hntketquql@benavente.us;178.174.199.124;;

8.6.2017 1:30;;Malicious-URL;;Malicious-URL;;macartu.cn;uygbctwies@hms.ru;42.7.26.38;;

8.6.2017 2:06;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

8.6.2017 2:09;;Malicious-URL;;mike@kupperSmith.com;145.249.201.63;;

8.6.2017 2:26;;Malicious-URL;;psstrust.com;;;

8.6.2017 2:28;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

8.6.2017 2:30;;Malicious-URL;;Malicious-URL;;onlinesmartsale.com;;;

8.6.2017 3:00;;Malicious-URL;;Malicious-URL;;amino-disqus.club;znfnte@hmsecurityservices.co.uk;115.231.16.138;;

8.6.2017 3:16;;Malicious-URL;;morgan@myarchimedes.com;123.24.205.206;;

8.6.2017 3:16;;Malicious-URL;;morgan@myarchimedes.com;123.20.98.128;;

8.6.2017 3:34;;Malicious-URL;;Malicious-URL;;macartu.cn;dkjope@hmsmakina.com.tr;59.37.22.82;;

8.6.2017 3:45;;Malicious-URL;;Malicious-URL;;macartu.cn;mcxvs@hmsheridan.co.uk;59.72.100.220;;

8.6.2017 3:47;;Malicious-URL;;aritory.ru;;;

8.6.2017 4:01;;Malicious-URL;;bmhall@bama.com;201.240.226.157;;

8.6.2017 4:10;;Malicious-URL;;Malicious-URL;;macartu.cn;vpopivvk@hmv-ahlen.de;110.153.16.148;;

8.6.2017 4:11;;Malicious-URL;;Malicious-URL;;macartu.cn;500662814535778.RX45210@uit.hmstrust.com;59.72.100.220;;

8.6.2017 4:35;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

8.6.2017 4:48;;Malicious-URL;;Malicious-URL;;macartu.cn;dxjgovrpo@hmsecurityservices.co.uk;50.199.157.91;;

8.6.2017 4:49;;Malicious-URL;;Malicious-URL;;macartu.cn;bdkuaonwjl@srpd.us;212.233.216.133;;

8.6.2017 4:49;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

8.6.2017 4:54;;Malicious-URL;;Malicious-URL;;macartu.cn;ipofmpsn@syno.nymo.us;112.124.50.85;;

8.6.2017 4:54;;Malicious-URL;;Malicious-URL;;macartu.cn;lemesbrqxen@chrisquinn.us;112.124.50.85;;

8.6.2017 5:00;;Malicious-URL;;Malicious-URL;;macartu.cn;aotlsvaew@hmsc.harvard.edu;47.90.4.23;;

8.6.2017 5:25;;Malicious-URL;;petrobtg@front.ru;113.172.172.35;;

8.6.2017 5:35;;Malicious-URL;;Malicious-URL;;firstmedsprogram.ru;eavuaomovu@03.com;52.169.224.103;;

8.6.2017 5:35;;Malicious-URL;;Malicious-URL;;firstmedsprogram.ru;frieily@0330.com;52.169.224.103;;

8.6.2017 5:36;;Malicious-URL;;hxxp://www.nuockhoanglavie.shop/wp-includes/js/tinymce/themes/modern/0643fb24f6a.html;dghjfd@aaa.de;103.3.82.232;;

8.6.2017 5:40;;Malicious-URL;;blackhat.agency;;;

8.6.2017 5:47;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

8.6.2017 6:43;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

8.6.2017 6:50;;Malicious-URL;;xujing@16ds.com;117.79.81.101;;

8.6.2017 6:51;;Malicious-URL;;Malicious-URL;;macartu.cn;ubnorayf@hmsc.harvard.edu;47.90.4.23;;

8.6.2017 6:54;90003bed49334b6eb0418cde73f4b156;NO HIT;Malware;Malware;10371.zip;sales@cygate.fi;115.84.93.195;;

8.6.2017 6:54;e98eadd76d0af67a1c91622dada50cc;NO HIT;Malware;Malware;192040.zip;sales@cygate.fi;115.84.93.195;;

8.6.2017 7:18;;Malicious-URL;;nordiskhandelsplads.dk;;;

8.6.2017 7:43;;Malicious-URL;;Malicious-URL;;scandigogo.com;;;

8.6.2017 7:45;;Malicious-URL;;Malicious-URL;;macartu.cn;frfvhefjism@hmt-ffb.de;80.249.187.178;;

8.6.2017 7:50;;Malicious-URL;;Malicious-URL;;macartu.cn;stryunmmagur@hmsheridan.co.uk;5.135.104.170;;

8.6.2017 7:52;;Malicious-URL;;Malicious-URL;;macartu.cn;kapormufzf@hmsost.com;213.32.112.88;;

8.6.2017 8:14;;Malicious-URL;;h476334@rppkn.com;14.229.101.234;;

8.6.2017 8:40;;Malicious-URL;;Malicious-URL;;macartu.cn;Sherlock_Meredith@sonne.us;138.117.121.10;;

8.6.2017 8:41;;Malicious-URL;;Malicious-URL;;organictabletinc.ru;alert@squarebitconsulting.com;198.252.78.105;;

8.6.2017 8:41;;Malicious-URL;;Malicious-URL;;macartu.cn;vlgrjrhfrx@pinepoint.k12.mn.us;138.117.121.10;;

8.6.2017 8:47;;Malicious-URL;;Malicious-URL;;amino-disqus.club;;;

8.6.2017 8:54;;Malicious-URL;;Malicious-URL;;medicalrxreward.ru;notification+zxf4210z4tsi@relief-allergy.com;94.72.4.242;;

8.6.2017 9:05;;Malicious-URL;;Malicious-URL;;organictabletinc.ru;alert@amazingstoriesinc.com;46.105.124.98;;

8.6.2017 9:05;;Malicious-URL;Malicious-URL;;jujialedlight.com;led@info.jujialedlight.com;211.159.66.88;;
8.6.2017 9:18;;Malicious-URL;;freedatekontakte.com;;;
8.6.2017 9:20;;Malicious-URL;Malicious-URL;;medicalrxquality.su;pending+7kj3u8fb01ui@144yipai.com;202.92.7.103;;
8.6.2017 9:23;;Malicious-URL;Malicious-URL;;medicalrxquality.su;support+zi7kkd4c7d1i@grants360.com;93.183.216.17;;
8.6.2017 9:56;;Malicious-URL;Malicious-URL;;scandigogo.com;;;
8.6.2017 9:58;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
8.6.2017 10:19;;Malicious-URL;;4charity.my;;;
8.6.2017 10:21;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;gtyobnub@14live.com;221.15.196.54;;
8.6.2017 10:21;;Malicious-URL;hxpp://www.555nm-hd.com/wp-content/plugins/cherry-plugin/admin/import-export/95660c0d0ce.html;eetheart@adig.de;14.164.22.155;;
8.6.2017 10:27;;Malicious-URL;Malicious-URL;;seamuseo.org;vqpuajablu@14ers.com;58.47.235.204;;
8.6.2017 10:27;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;;;
8.6.2017 10:29;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;rrmyue@14fm.net;60.19.10.44;;
8.6.2017 10:34;;Malicious-URL;;alwaysbemobile.nl;;;
8.6.2017 10:37;;Malicious-URL;;jama@mediazor.com;217.182.242.91;;
8.6.2017 10:37;;Malicious-URL;;info@sportsdoze.com;194.88.106.149;;
8.6.2017 10:37;;Malicious-URL;;jama@mediazor.com;217.182.242.91;;
8.6.2017 10:38;;Malicious-URL;;jama@mediazor.com;217.182.242.91;;
8.6.2017 10:43;;Malicious-URL;Malicious-URL;;macartu.cn;lxbrbpe@hmsheridan.co.uk;180.210.201.55;;
8.6.2017 10:46;;Malicious-URL;Malicious-URL;;organictabletinc.ru;pending+4a0ntpzaxe1r@northwestrangers.com;176.56.61.52;;
8.6.2017 10:48;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@formacionennavarra.com;199.101.98.50;;
8.6.2017 10:51;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@medicalwebsitepackage.com;67.69.228.122;;
8.6.2017 10:55;;Malicious-URL;hxpp://www.bestfares-travel.com/wp-content/plugins/contact-form-7/includes/js/jquery-ui/themes/96235cff9e6.html;waley5@topologix.de;221.215.199.125;;
8.6.2017 11:08;;Malicious-URL;Malicious-URL;;medicemail.com;;;
8.6.2017 11:13;;Malicious-URL;;canna-holdings.com;;;
8.6.2017 11:54;;Malicious-URL;;bert.mueller@rmg-poppenhausen.de;177.87.232.16;;
8.6.2017 12:16;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;roles9@comtrade.de;113.163.189.20;;
8.6.2017 12:30;;Malicious-URL;Malicious-URL;;nations-direct.com;information@nations-direct.com;217.182.207.103;;
8.6.2017 12:30;;Malicious-URL;Malicious-URL;;masterlead.info;;;
8.6.2017 12:39;;Malicious-URL;Malicious-URL;;macartu.cn;courttcm@rampartbuilders.us;74.194.96.172;;
8.6.2017 12:49;;Malicious-URL;;tracydowling@homechoice.co.uk;113.184.181.111;;
8.6.2017 12:53;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
8.6.2017 12:54;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
8.6.2017 12:57;;Malicious-URL;;lin@millio.com;51.254.33.52;;
8.6.2017 12:59;;Malicious-URL;;lin@millio.com;51.254.33.52;;
8.6.2017 13:02;;Malicious-URL;;lin@millio.com;51.254.33.52;;
8.6.2017 13:02;;Malicious-URL;;jesusandson@yahoo.com;123.21.31.116;;
8.6.2017 13:14;;Malicious-URL;Malicious-URL;hxpp://dameison.com/data/payment/xise/;sunting@afecc.com;220.178.32.196;;
8.6.2017 13:25;;Malicious-URL;Malicious-URL;;clicks.space;ilona@srv.erosends.eu;207.154.235.166;;
8.6.2017 13:30;;Malicious-URL;;info@zimdom.ga;59.153.49.69;;
8.6.2017 13:39;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;svnuh@1connect.com;47.52.3.154;;
8.6.2017 13:41;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;nhzqeadcg@1creation.com;101.69.15.114;;
8.6.2017 13:42;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;orbnjqurs@1dad.net;177.220.235.35;;
8.6.2017 14:09;;Malicious-URL;;OF21C7581E.977A7CD9-ON00258139.003D3BBA-00258139.003D4D2E@notes.na.collabserve.com;148.163.158.5;;
8.6.2017 14:28;;Malicious-URL;;noreply@starburst.com;195.140.195.194;;
8.6.2017 14:29;;Malicious-URL;Malicious-URL;;warz.pl;hsheldahl@excite.it;113.161.72.100;;
8.6.2017 14:32;;Malicious-URL;Malicious-URL;;macartu.cn;rpsauugvt@hmsinet.ca;185.81.40.219;;
8.6.2017 14:36;;Malicious-URL;;cozyaccommodations.com;;;
8.6.2017 14:43;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;jarkko.vepsalainen@with.fi;104.47.0.62;;
8.6.2017 14:51;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;scm_web@sc-melkendorf.de;62.75.251.202;;
8.6.2017
14:58;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;apache@proteusdynamic.com;81.142.110.244;;
8.6.2017 14:59;;Malicious-URL;Malicious-URL;;macartu.cn;yuaaxyjr@hms.harvard.edu;188.165.184.117;;
8.6.2017 15:01;;Malicious-URL;;lin@millio.com;51.254.33.52;;
8.6.2017 15:04;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;sales@customer-care.sap;207.246.241.253;;
8.6.2017 15:04;;Malicious-URL;Malicious-URL;;macartu.cn;dtqhbougay@hms.ru;51.255.59.221;;
8.6.2017 15:09;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;wwwrun@srv-web.site;90.182.157.205;;
8.6.2017 15:18;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;ec2-user@ip-172-31-21-42.sa-east-1.compute.internal;54.232.201.6;;
8.6.2017 15:28;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;cthixton@coa.coastbus.org;192.254.161.232;;
8.6.2017 15:45;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;cthixton@coa.coastbus.org;192.254.161.232;;
8.6.2017 15:48;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;webmaster@52sad.ru;91.240.86.75;;
8.6.2017 15:52;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;webmaster@rdc-karelia.ru;178.19.248.59;;
8.6.2017 15:59;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;cthixton@coa.coastbus.org;192.254.161.232;;
8.6.2017
16:09;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;sol@svm46108.vps.tagadab.com;80.241.49.114;;
8.6.2017 16:17;cb563b18f432105ccbf0ecbb447013a;TROJ_ARTIEFJEJOUZ;Malware;Malware;Malware;B9BDY5Y87X.doc;;byu1191480001@byu-119148.hichina.com;123.56.106.140;;
8.6.2017 16:35;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
8.6.2017 16:39;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
8.6.2017 16:41;1982b3777f50e653308808e0f80d037;CLEAN - False Positive;;Malware;;Couliaren.docx;;missarenbaly@gmail.com;208.70.128.176;;
8.6.2017 16:41;;Malicious-URL;;lin@millio.com;51.254.33.52;;
8.6.2017 16:41;;Malicious-URL;;missarenbaly@gmail.com;208.70.128.176;;
8.6.2017 17:22;;Malicious-URL;Malicious-URL;;organictabletinc.ru;support+040g76zr2g6n@1018.com;103.4.17.82;;
8.6.2017 17:57;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;alert@caribbean-house-for-sale.com;124.150.140.106;;
8.6.2017 17:57;;Malicious-URL;Malicious-URL;;medicalrxquality.su;;;
8.6.2017 18:14;;Malicious-URL;;hxpp://SAFELIFESENIORFSC.COM/viewdoc/file.php?document=cGV0cmkuaGVPbm9uZW5AY3lnYXRlMzZp;dropbox@veintrain.com;74.72.30.204;;
8.6.2017 18:15;;Malicious-URL;Malicious-URL;;organictabletinc.ru;pending+76gxpaddv88s@tekhhaus-studios.com;103.27.61.225;;
8.6.2017 18:17;;Malicious-URL;;Malicious-URL;;hxpp://gottliebfamilypartnership.com/viewdoc/file.php?document=dG9taS5rYXJsc3NvbkJjeWdhGduUzmk=;dropbox@veintrain.com;70.90.54.42;;
8.6.2017 18:18;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@sei-archi.com;80.88.88.152;;
8.6.2017 18:21;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@promanaint.com;31.185.7.22;;
8.6.2017 18:24;;Malicious-URL;hxpp://brri.in/viewdoc/file.php?document=bWZzaS50YWthbWFRaUJjeWdhGduUzmk=;dropbox@veintrain.com;50.39.0.10;;
8.6.2017 18:28;;Malicious-URL;;hxpp://SAFELIFESENIORFSC.COM/viewdoc/file.php?document=a2FyaS5rdXJraUJjeWdhGduUzmk=;dropbox@veintrain.com;96.82.73.121;;
8.6.2017 18:29;;Malicious-URL;Malicious-URL;;macartu.cn;gdxvfvj@hms-host.com.au;186.27.126.130;;
8.6.2017 18:34;;Malicious-URL;;hxpp://SAFELIFESENIORFSC.COM/viewdoc/file.php?document=YW5uZS5oZW5yaXRPdXNAY3lnYXRlMzZp;dropbox@veintrain.com;76.9.48.78;;
8.6.2017 18:37;;Malicious-URL;Malicious-URL;;organictabletinc.ru;notification+0vps5pttsbm@abstractaxandaccountingllc.com;217.147.86.121;;
8.6.2017 18:44;;Malicious-URL;hxpp://brri.in/viewdoc/file.php?document=dMzY5S5ZWh0aW5lbkJjeWdhGduUzmk=;dropbox@veintrain.com;81.142.129.101;;
8.6.2017 18:48;;Malicious-URL;Malicious-URL;Malicious-URL;;bucksrealstatecenter.com;kfoplm@0catch.com;42.229.57.253;;
8.6.2017 18:48;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;;;
8.6.2017 18:49;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;cbgrtai@Ocomcast.net;42.229.57.253;;
8.6.2017 18:52;;Malicious-URL;Malicious-URL;;firstmedsprogram.ru;zlnyb@Ocostmortgage.com;177.220.235.35;;
8.6.2017 18:53;;Malicious-URL;Malicious-URL;;flashpansimple.com;mailer@edm.flashpansimple.com;119.28.88.77;;

9.6.2017 5:36;;;Malicious-URL;;;sales@customer-care.sap;5.249.143.92;;
9.6.2017 5:46;f3432c9c24e8f01bb5f3305bfadbb4811;NO HIT;;Malware;Malware;17392.zip;;servicedesk@cygate.fi;117.253.202.191;;
9.6.2017 5:46;ff8b07e7b90d784cc8a53b28c7cf23;NO HIT;;Malware;Malware;19601037325.zip;;servicedesk@cygate.fi;117.253.202.191;;
9.6.2017 5:47;;;Malicious-URL;;;pasofinostereo@server123.usatelk.com;198.50.145.238;;
9.6.2017 5:52;;;Malicious-URL;;;frowziestkr8@uni-berlin.de;202.29.178.191;;
9.6.2017 5:59;;;Malicious-URL;;;msqym.com;;;
9.6.2017 6:12;;;Malicious-URL;;;admin@marrytags.de;51.254.238.130;;
9.6.2017 6:32;;;Malicious-URL;;;f0b1e4c@anfahren.ch;14.160.46.18;;
9.6.2017 6:45;;;Malicious-URL;;;admin@marrytags.de;178.32.60.137;;
9.6.2017 7:00;;;Malicious-URL;;;admin@marrytags.de;178.32.51.218;;
9.6.2017 7:06;;;Malicious-URL;;;kukareku-hostel.com;;;
9.6.2017 7:08;;;Malicious-URL;Malicious-URL;;;macartu.cn;btwougeyrc@hmshost.com;47.90.4.23;;
9.6.2017 7:16;;;Malicious-URL;;;lettnerdd@concept.at;113.160.37.143;;
9.6.2017 7:33;;;Malicious-URL;Malicious-URL;;;kristinamiliona.ml;rbuttler@106acht.de;189.215.157.5;;
9.6.2017 7:47;;;Malicious-URL;Malicious-URL;;;dock.email;noreply@runbenrun.info;93.90.123.203;;
9.6.2017 8:01;da0b704ba8aa2537c00d2fcb7c5a634;Trojan.Gen.NPE;;Malware;Malware;SCAN_0911-PDF.arj;;admin@vps.com;94.177.230.224;;
9.6.2017 8:02;;;Malicious-URL;Malicious-URL;;;macartu.cn;mntre@take.us;101.200.151.23;;
9.6.2017 8:02;;;Malicious-URL;Malicious-URL;;;macartu.cn;uqiofloanmmqj@mrhds.k12.mo.us;101.200.151.23;;
9.6.2017 8:04;;;Malicious-URL;Malicious-URL;;;superdirect.su;marten@hantra.com;213.182.207.49;;
9.6.2017 8:04;;;Malicious-URL;;;jean-pierre.dauwalderd@freesulf.de;190.219.125.163;;
9.6.2017 8:09;;;Malicious-URL;Malicious-URL;;;okeyby.com;no-reply@no-reply.98989.net.cn;195.140.195.194;;
9.6.2017 8:35;;;Malicious-URL;Malicious-URL;;;superdirect.su;floppierzq330@stadler.de;14.161.4.46;;
9.6.2017 8:46;;;Malicious-URL;Malicious-URL;;;herbaltabssassit.ru;ngpmas@0395.net;195.140.195.194;;
9.6.2017 9:04;;;Malicious-URL;;;nordiskhandelsplads.dk;;;
9.6.2017 9:10;;;Malicious-URL;;;hbhlgsw.com;;;
9.6.2017 9:23;;;Malicious-URL;Malicious-URL;;;sexy-dates.ru;info@OCCULTATE.br;103.63.11.74;;
9.6.2017 9:34;;;Malicious-URL;Malicious-URL;;;scandigogo.com;;;
9.6.2017 9:38;;;Malicious-URL;;;info@sportsdoze.com;194.88.106.149;;
9.6.2017 9:40;;;Malicious-URL;Malicious-URL;;;macartu.cn;830244271547275.SH30654@pww.hmshost.com.au;212.83.56.87;;
9.6.2017 9:46;;;Malicious-URL;;;kayleen@intelisell.com;147.135.204.183;;
9.6.2017 10:05;;;Malicious-URL;Malicious-URL;;;superdirect.su;therbein@doverdowns.com;182.75.199.74;;
9.6.2017 10:08;;;Malicious-URL;Malicious-URL;;;bcontacts.net;;;
9.6.2017 10:13;;;Malicious-URL;;;yetta@intelisell.com;147.135.204.184;;
9.6.2017 10:15;188663907c707fe59daaa1fbfc4ce277;W97M.Downloader;Malware;Malware;Malware;IMG_3627.ZIP;;Jerri@arlingtonchiroclinic.com;36.37.247.141;;
9.6.2017 10:15;;;Malicious-URL;;;yetta@intelisell.com;147.135.204.184;;
9.6.2017 10:19;bccb4e6cfa347d1e9b7a76965ed96ff5;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_2756.ZIP;;Darius@ballygowanyouthclub.co.uk;123.252.195.229;
9.6.2017 10:20;bccb4e6cfa347d1e9b7a76965ed96ff5;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_1305.ZIP;;Avery@udinknoodverlichting.nl;180.92.171.17;;
9.6.2017 10:20;bccb4e6cfa347d1e9b7a76965ed96ff5;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_2228.ZIP;;Gladys@bureau-balans.nl;117.218.126.139;;
9.6.2017 10:20;bccb4e6cfa347d1e9b7a76965ed96ff5;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_1065.ZIP;;Katheryn@guidaminas.com;41.33.44.99;;
9.6.2017 10:20;bccb4e6cfa347d1e9b7a76965ed96ff5;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_7703.ZIP;;Leta@gizmotec.co.uk;61.0.136.184;;
9.6.2017 10:20;bccb4e6cfa347d1e9b7a76965ed96ff5;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_9076.ZIP;;Renee@awintersfoto.com;115.79.102.183;;
9.6.2017 10:20;bccb4e6cfa347d1e9b7a76965ed96ff5;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_5121.ZIP;;Shaun@brblfc.com;113.161.19.129;;
9.6.2017 10:20;;;Malicious-URL;;;Mindaugas.Mosteika@outokumpu.com;131.207.48.201;;
9.6.2017 10:21;d0f708fd033906ee58785d2a0efaa0b8;W97M.Downloader;Malware;Malware;Malware;IMG_1828.ZIP;;Elvia@antelpescara.net;103.85.112.130;;
9.6.2017 10:21;d0f708fd033906ee58785d2a0efaa0b8;W97M.Downloader;Malware;Malware;Malware;IMG_6624.ZIP;;Van@antarlink.com;91.187.102.8;;
9.6.2017 10:22;70db9c80afe679c6a5c8820672fd08ae;W97M.Downloader;Malware;Malware;Malware;IMG_1911.ZIP;;Jimmy@sindpubrj.com.br;120.138.115.69;;
9.6.2017 10:23;f0906dfcd86a9e8e013c3c3499f417e9;W97M.Downloader;Malware;Malware;Malware;IMG_6191.ZIP;;Miquel@marinergoffclub.nl;113.174.101.249;;
9.6.2017 10:24;f0906dfcd86a9e8e013c3c3499f417e9;W97M.Downloader;Malware;Malware;Malware;IMG_4068.ZIP;;Damion@commandos.nl;118.68.149.103;;
9.6.2017 10:25;a16a2bba91b2c9aa5cbb8282d637b8e1;W97M.Downloader;Malware;Malware;Malware;IMG_0316.ZIP;;Jackson@globenetttoyage.ch;146.60.60.193;;
9.6.2017 10:25;f1334bade47f9fac156dd3e52b5c1a3;W97M.Downloader;Malware;Malware;Malware;IMG_9342.ZIP;;Rolland@coachingterapia.com.br;202.93.213.82;;
9.6.2017 10:26;36c4bcb6c1581b67b43003d54a350c331;W97M.Downloader;Malware;Malware;Malware;IMG_9478.ZIP;;Ezekiel@tightloop.tuccoemail.com;27.62.27.83;;
9.6.2017 10:26;a16a2bba91b2c9aa5cbb8282d637b8e1;W97M.Downloader;Malware;Malware;Malware;IMG_3277.ZIP;;Deirdre@kookjiook.nl;42.117.13.105;;
9.6.2017 10:26;f1334bade47f9fac156dd3e52b5c1a3;W97M.Downloader;Malware;Malware;Malware;IMG_4798.ZIP;;Greta@howards.edu.au;79.124.11.5;;
9.6.2017 10:27;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_5987.ZIP;;Beth@alanrynhall.com;103.242.56.124;;
9.6.2017 10:27;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_7135.ZIP;;Shelby@furgoninternational.com;197.243.40.122;;
9.6.2017 10:28;36c4bcb6c1581b67b43003d54a350c331;W97M.Downloader;Malware;Malware;Malware;IMG_5866.ZIP;;Rosalind@sandfields.info;103.253.38.4;;
9.6.2017 10:28;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_9322.ZIP;;Carol@cheaplightboxes.com;171.79.100.154;;
9.6.2017 10:28;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_9433.ZIP;;Earline@lunardsbuffet.com.br;113.161.218.221;;
9.6.2017 10:28;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_2549.ZIP;;Edna@foreverfabulous.ie;122.55.59.240;;
9.6.2017 10:28;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_2524.ZIP;;Gladys@epidotiseis.com;117.211.20.148;;
9.6.2017 10:29;7d7fbb83ce3e74f8cd135872ef524fa;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_0067.ZIP;;Julia@kangooclubofnorthamerica.com;1.23.145.18;;
9.6.2017 10:29;7d7fbb83ce3e74f8cd135872ef524fa;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_5851.ZIP;;Janine@livedimedia.biz;103.200.95.11;;
9.6.2017 10:29;7d7fbb83ce3e74f8cd135872ef524fa;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_5165.ZIP;;Vivian@hotm.tv;116.108.77.195;;
9.6.2017 10:29;7d7fbb83ce3e74f8cd135872ef524fa;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_1153.ZIP;;Young@jeannebaggen.nl;113.175.131.86;;
9.6.2017 10:29;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_1574.ZIP;;Louie@travelhoststexas.com;61.8.152.100;;
9.6.2017 10:30;4054abcc1aac91326fd73c9deabdfed2;W97M.Downloader;Malware;Malware;Malware;IMG_8682.ZIP;;Mildred@butlerscontracting.ca;182.65.212.68;;
9.6.2017 10:30;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_5563.ZIP;;Angela@kettnerexchange.com;157.119.106.187;;
9.6.2017 10:31;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_5470.ZIP;;Ericka@marysvillechirowellness.com;112.197.224.23
9.6.2017 10:31;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_2695.ZIP;;Jacqueline@fondducroix.org;45.116.230.242;;
9.6.2017 10:31;b6afafdcc33f03dc94abd25076978d36;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_1287.ZIP;;Reynaldo@papillonmandarina.com;117.6.162.58;;
9.6.2017 10:32;1f3c60f328f1a0e94eff8e1e1b9005f3;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_5532.ZIP;;Janine@select-m.ru;203.128.69.130;;
9.6.2017 10:33;1f3c60f328f1a0e94eff8e1e1b9005f3;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_3973.ZIP;;Edna@wisewriting.ca;139.228.115.90;;
9.6.2017 10:33;476e2fea9b89d5335b6b6d99b06b40c;W97M.Downloader;Malware;Malware;Malware;IMG_8659.ZIP;;Ofelia@whiskeyboy.us;117.218.155.150;;
9.6.2017 10:34;1f3c60f328f1a0e94eff8e1e1b9005f3;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_6678.ZIP;;Chuck@whatology.org;178.135.40.30;;
9.6.2017 10:34;69c9a1a411342f0382f0b698b96bb0ca;W97M.Downloader;Malware;Malware;Malware;IMG_5893.ZIP;;Rosella@agilecapibara.com;82.77.64.215;;
9.6.2017 10:35;014833ff40fe2d22572e9b857609e889;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_0225.ZIP;;Christina@moxnintextiles.com;190.247.37.125;;
9.6.2017 10:35;014833ff40fe2d22572e9b857609e889;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_5375.ZIP;;Dale@luciol.com;106.201.78.24;;
9.6.2017 10:35;014833ff40fe2d22572e9b857609e889;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_4577.ZIP;;Freida@luciocosta.com;115.99.17.124;;
9.6.2017 10:35;014833ff40fe2d22572e9b857609e889;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_1834.ZIP;;Rae@tac-shop.com;110.172.173.234;;
9.6.2017 10:35;69c9a1a411342f0382f0b698b96bb0ca;W97M.Downloader;Malware;Malware;Malware;IMG_8036.ZIP;;Benita@hioki.nl;117.221.222.34;;
9.6.2017 10:35;69c9a1a411342f0382f0b698b96bb0ca;W97M.Downloader;Malware;Malware;Malware;IMG_3587.ZIP;;Corrine@efficiency.do;182.72.153.202;;
9.6.2017 10:36;e37171d2833c320eba3d600c460f3a78;W97M.Downloader;Malware;Malware;Malware;IMG_6157.ZIP;;Rosie@thegaiety.ie;59.93.103.202;;
9.6.2017 10:37;1213cc450b9ab82826af2746fbf204;W97M.Downloader.M;Malware;Malware;Malware;IMG_0245.ZIP;;Jessie@prodmed.nl;82.222.40.98;;

9.6.2017 10:37;e37171d2833c320eba3d600c460f3a78;W97M.Downloader;Malware;Malware;Malware;IMG_2226.ZIP;;Dallas@advicegraphics.com;113.165.66.242;;
9.6.2017 10:38;39717c31739cfcdbd4c4c23af7217455;W97M.Downloader;Malware;Malware;Malware;IMG_7687.ZIP;;Aileen@hohorst.net;213.55.114.186;;
9.6.2017 10:38;39717c31739cfcdbd4c4c23af7217455;W97M.Downloader;Malware;Malware;Malware;IMG_9422.ZIP;;Callie@redlinetireco.com;89.165.82.23;;
9.6.2017 10:39;39717c31739cfcdbd4c4c23af7217455;W97M.Downloader;Malware;Malware;Malware;IMG_1345.ZIP;;Edmund@infobrasil.com.br;182.176.178.22;;
9.6.2017 10:39;b84fd3495504565fc662a36f833d7d3c;TROJ_GENZM.F299E00FB17;Malware;Malware;Malware;IMG_1908.ZIP;;Todd@algebra101.com;14.175.74.14;;
9.6.2017 10:39;f212c4da28086f32dc6d081a84d4afb;W97M.Downloader.M;Malware;Malware;Malware;IMG_8499.ZIP;;Kayla@schmidvidpro.com;31.59.36.131;;
9.6.2017 10:40;b84fd3495504565fc662a36f833d7d3c;TROJ_GENZM.F299E00FB17;Malware;Malware;Malware;IMG_7524.ZIP;;Carly@permitpro.com;122.171.107.28;;
9.6.2017 10:40;b84fd3495504565fc662a36f833d7d3c;TROJ_GENZM.F299E00FB17;Malware;Malware;Malware;IMG_9593.ZIP;;Rosalyn@housecallsofamerica.com;117.219.201.7;;
9.6.2017 10:40;f212c4da28086f32dc6d081a84d4afb;W97M.Downloader.M;Malware;Malware;Malware;IMG_8343.ZIP;;Lucy@a01.com.uy;117.98.138.126;;
9.6.2017 10:41;b84fd3495504565fc662a36f833d7d3c;TROJ_GENZM.F299E00FB17;Malware;Malware;Malware;IMG_6324.ZIP;;Lane@bellemaisonsolutions.com;210.212.43.202;;
9.6.2017 10:41;f9024e76dc01ea6528f3bd951a5f964e;W97M.Downloader.M;Malware;Malware;Malware;IMG_1732.ZIP;;Bettye@loboassessoria.com.br;14.182.112.187;;
9.6.2017 10:41;f9024e76dc01ea6528f3bd951a5f964e;W97M.Downloader.M;Malware;Malware;Malware;IMG_9681.ZIP;;Jeri@rbgrealstate.com;1.54.214.176;;
9.6.2017 10:42;848acd01e2736f469cb3b1911f74f009;W97M.Downloader.M;Malware;Malware;Malware;IMG_5632.ZIP;;Shia@oepvc.com;124.108.17.178;;
9.6.2017 10:42;848acd01e2736f469cb3b1911f74f009;W97M.Downloader.M;Malware;Malware;Malware;IMG_7908.ZIP;;Thellememg;27.56.134.55;;
9.6.2017 10:43;31cde49053dade986c7a321a7e522e08;W97M.Downloader.M;Malware;Malware;Malware;IMG_6411.ZIP;;Lourdes@911transport.com;14.96.190.76;;
9.6.2017 10:43;ed0e6b9886120049d4f8f182def8213;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_9238.ZIP;;Tomas@selectivebusiness.se;103.68.216.29;;
9.6.2017 10:44;ed0e6b9886120049d4f8f182def8213;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_4007.ZIP;;Chandra@bdp.rs;84.54.132.58;;
9.6.2017 10:44;ed0e6b9886120049d4f8f182def8213;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_6615.ZIP;;Harry@ministrylinks.org;14.188.60.213;;
9.6.2017 10:44;ed0e6b9886120049d4f8f182def8213;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_3959.ZIP;;Morgan@abdrivewayrepair.com;27.111.28.246;;
9.6.2017 10:45;7d7fbb83ce3e74f8cd135872ef524fa;TROJ_GENZM.F299E00FB17;Malware;Malware;Malware;IMG_1314.ZIP;;Velma@satchelsocaring.org;103.59.193.104;;
9.6.2017 10:46;476e2fea9b89d5335b6bd99b06b40c;W97M.Downloader;Malware;Malware;Malware;IMG_3905.ZIP;;Casandra@eeneneen.nl;43.243.152.70;;
9.6.2017 10:49;6a0f93f9d71c6d9c613c43a891072d1f;W97M.Downloader.M;Malware;Malware;Malware;IMG_5530.ZIP;;Evangeline@jcrassociates.net;182.188.90.163;;
9.6.2017 10:50;27c624576388b5d766cb3ea28caea47f;W97M.Downloader.M;Malware;Malware;Malware;IMG_5883.ZIP;;Bertie@arrows.screaming.net;164.100.146.66;;
9.6.2017 10:51;4054abcc1aac91326fd73c9deabdfed2;W97M.Downloader;Malware;Malware;Malware;IMG_0230.ZIP;;Johnie@betterbusinessknowhow.com;117.247.128.46;;
9.6.2017 10:53;4e8616f0d912d4c94bc8ee5213622;W97M.Downloader;Malware;Malware;Malware;IMG_2862.ZIP;;Lavonne@p1s.com;118.71.106.38;;
9.6.2017 10:53;edc0ff21904020e6e5e0e56bcd801ed;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_2536.ZIP;;Fern@1pcn.com;14.167.21.49;;
9.6.2017 10:53;edc0ff21904020e6e5e0e56bcd801ed;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_3639.ZIP;;Jamal@boxdobrafil.com.br;171.78.205.118;;
9.6.2017 10:53;edc0ff21904020e6e5e0e56bcd801ed;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_0951.ZIP;;jenifer@clmadvogados.com.br;190.117.125.212;;
9.6.2017 10:53;edc0ff21904020e6e5e0e56bcd801ed;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_4884.ZIP;;Margo@harvardcoilprocessing.com;202.90.137.27;;
9.6.2017 10:53;edc0ff21904020e6e5e0e56bcd801ed;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_9928.ZIP;;Reva@sibdo.com;113.164.94.179;;
9.6.2017 10:54;b89767b057daab1fb0f6514b11a391e7;W97M.Downloader.M;Malware;Malware;Malware;IMG_0960.ZIP;;Moises@benmarcus.com;203.171.245.214;;
9.6.2017 10:55;b89767b057daab1fb0f6514b11a391e7;W97M.Downloader.M;Malware;Malware;Malware;IMG_8942.ZIP;;Clarence@hotairfun.com;117.3.66.114;;
9.6.2017 10:55;b89767b057daab1fb0f6514b11a391e7;W97M.Downloader.M;Malware;Malware;Malware;IMG_6573.ZIP;;Laurel@slvphonotworld.com;45.117.1.60;;
9.6.2017 10:56;b177d4066fad253b8875d965bc30d6af;W2KM_CRYPTAJFF.QGA;Malware;Malware;Malware;IMG_0613.ZIP;;Esmeralda@exenbil.com;117.7.216.145;;
9.6.2017 10:56;b177d4066fad253b8875d965bc30d6af;W2KM_CRYPTAJFF.QGA;Malware;Malware;Malware;IMG_1003.ZIP;;Joann@netsonic.net;177.136.103.172;;
9.6.2017 10:57;4864f7384d420bd8087c4817683c27b;W2KM_CRYPTAJFF.QGA;Malware;Malware;Malware;IMG_5609.ZIP;;Margo@jsmithlawns.com;103.70.109.161;;
9.6.2017 10:57;b177d4066fad253b8875d965bc30d6af;W2KM_CRYPTAJFF.QGA;Malware;Malware;Malware;IMG_0030.ZIP;;Clint@pennsylvania-personal-injury-law.com;49.248.131.124;;
9.6.2017 10:57;b177d4066fad253b8875d965bc30d6af;W2KM_CRYPTAJFF.QGA;Malware;Malware;Malware;IMG_1695.ZIP;;Fausto@bnbitumen.com;130.193.213.80;;
9.6.2017 10:57;b177d4066fad253b8875d965bc30d6af;W2KM_CRYPTAJFF.QGA;Malware;Malware;Malware;IMG_3671.ZIP;;Sallie@ic-bec.com;189.202.66.236;;
9.6.2017 10:58;4864f7384d420bd8087c4817683c27b;W2KM_CRYPTAJFF.QGA;Malware;Malware;Malware;IMG_8697.ZIP;;Amparo@halocreativestudios.com;118.137.209.34;;
9.6.2017 10:58;4864f7384d420bd8087c4817683c27b;W2KM_CRYPTAJFF.QGA;Malware;Malware;Malware;IMG_2015.ZIP;;Meredith@bhik.worldonline.co.uk;14.162.200.36;;
9.6.2017 10:58;e229d53471172d7974c957cdebb53d07;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_8094.ZIP;;Cruz@ropaydeporte.com;183.81.155.27;;
9.6.2017 10:59;e229d53471172d7974c957cdebb53d07;TROJ_GENZM.F299E00F17;Malware;Malware;Malware;IMG_8217.ZIP;;Bessie@montgomerywardsrugs.com;189.216.64.62;;
9.6.2017 11:11;5614a172e6c18b02b031fdd5143c3ad;TROJ_GENZM.F299E00FB17;Malware;Malware;Malware;DOC_7288.docm;;Anne@peircemortgage.com;36.37.219.108;;
9.6.2017 11:14;83f2ac7fa3f4623c7143170bda389ab;TROJ_GENZM.F299E00FB17;Malware;Malware;Malware;DOC_9369.docm;;Rudy@cuoro.com;117.239.242.34;;
9.6.2017 11:15;85de9f13e398f7c6293944f73875e82e;TROJ_GENZM.F299E00FB17;Malware;Malware;Malware;DOC_7969.docm;;Dora@kidslanguageclub.co.uk;14.188.175.251;;
9.6.2017 11:17;83f2ac7fa3f4623c7143170bda389ab;TROJ_GENZM.F299E00FB17;Malware;Malware;Malware;DOC_7819.docm;;Lily@geoanalitica.com;46.62.187.23;;
9.6.2017 11:20;;Malicious-URL;Malicious-URL;;;medicemail.com;;;
9.6.2017 11:28;;Malicious-URL;;;admin@marrtags.de;178.32.60.137;;
9.6.2017 11:31;;Malicious-URL;Malicious-URL;;;macartu.com;majpmblpvf@postini.us;112.124.50.85;;
9.6.2017 11:42;;Malicious-URL;Malicious-URL;;;bcontacts.net;;;
9.6.2017 11:49;;Malicious-URL;;;admin@marrtags.de;178.32.60.137;;
9.6.2017 12:05;;Malicious-URL;Malicious-URL;;;scbudgetroofing.com;;;
9.6.2017 12:09;3974279cf62044a09f5cbb7d51d7c47;JS_NEMUCOD.SMK17;Malware;;Malware;AA-175-RR.wsf;;anna.mills@lauraandersonphotography.co.uk;49.128.161.81;;
9.6.2017 12:09;7eb9c50254ba1e38c82358f9566366a;JS_NEMUCOD.SMK17;Malware;;Malware;AA-175-RR.zip;;anna.mills@lauraandersonphotography.co.uk;49.128.161.81;;
9.6.2017 12:09;7f35413209cb8bcfb17c983f08a63d92;JS_NEMUCOD.SMK17;Malware;;Malware;2607287.zip;;anna.mills@lauraandersonphotography.co.uk;49.128.161.81;;
9.6.2017 12:10;7f35413209cb8bcfb17c983f08a63d92;JS_NEMUCOD.SMK17;Malware;;Malware;3591912.zip;;anna.mills@asset-bus-consulting.co.uk;223.196.72.222;;
9.6.2017 12:10;7f35413209cb8bcfb17c983f08a63d92;JS_NEMUCOD.SMK17;Malware;;Malware;1124023.zip;;anna.mills@cafedata.co.uk;203.235.23.35;;
9.6.2017 12:10;7f35413209cb8bcfb17c983f08a63d92;JS_NEMUCOD.SMK17;Malware;;Malware;547802.zip;;anna.mills@petplays.co.uk;41.0.164.136;;
9.6.2017 12:10;7f35413209cb8bcfb17c983f08a63d92;JS_NEMUCOD.SMK17;Malware;;Malware;184201.zip;;anna.mills@setyres.co.uk;59.99.97.198;;
9.6.2017 12:10;7f35413209cb8bcfb17c983f08a63d92;JS_NEMUCOD.SMK17;Malware;;Malware;2555591.zip;;anna.mills@slades24.worldonline.co.uk;79.55.158.157;;
9.6.2017 12:10;7f35413209cb8bcfb17c983f08a63d92;JS_NEMUCOD.SMK17;Malware;;Malware;3773212.zip;;anna.mills@southcoastpackaging.co.uk;122.160.196.86;;
9.6.2017 12:10;a8c187fe09fd268df048109fd6340f4c;JS_NEMUCOD.SMK17;Malware;;Malware;AA-091-RR.zip;;anna.mills@martisteenon.co.uk;14.142.94.246;;
9.6.2017 12:10;ba6859255394da91c0a5e9d7877c0940;JS_NEMUCOD.SMK17;Malware;;Malware;8209588.zip;;anna.mills@anthonyhnt.co.uk;113.190.36.238;;
9.6.2017 12:10;ba6859255394da91c0a5e9d7877c0940;JS_NEMUCOD.SMK17;Malware;;Malware;0346811.zip;;anna.mills@grovesautos.co.uk;59.91.80.247;;
9.6.2017 12:10;ba6859255394da91c0a5e9d7877c0940;JS_NEMUCOD.SMK17;Malware;;Malware;9046546.zip;;anna.mills@martisteenon.co.uk;14.142.94.246;;
9.6.2017 12:10;ba6859255394da91c0a5e9d7877c0940;JS_NEMUCOD.SMK17;Malware;;Malware;1726582.zip;;anna.mills@mightykinemovie.com;43.231.240.210;;
9.6.2017 12:10;ba6859255394da91c0a5e9d7877c0940;JS_NEMUCOD.SMK17;Malware;;Malware;1307894.zip;;anna.mills@speedlineimports.co.uk;123.238.241.182;;
9.6.2017 12:10;dbs21a5a0fc3c403771fe50662280b3;JS_NEMUCOD.SMK17;Malware;;Malware;AA-091-RR.wsf;;anna.mills@martisteenon.co.uk;14.142.94.246;;
9.6.2017 12:10;;Malicious-URL;Malicious-URL;;;medicalrxeward.ru;alert@abneysolarelectrix.com;74.208.110.207;;
9.6.2017 12:11;821c846404d2d3217410a3a5ac85a269;JS_NEMUCOD.SMK17;Malware;;Malware;AA-246-RR.zip;;anna.mills@real.worldonline.co.uk;88.255.171.82;;
9.6.2017 12:11;835b911b1545768b29652b5c16c02549;JS_NEMUCOD.SMK17;Malware;;Malware;247396.zip;;anna.mills@real.worldonline.co.uk;88.255.171.82;;
9.6.2017 12:11;b1d90636904fc961ac7a532895d9e0b9;JS_NEMUCOD.SMK17;Malware;;Malware;AA-246-RR.wsf;;anna.mills@real.worldonline.co.uk;88.255.171.82;;
9.6.2017 12:12;;Malicious-URL;;;admin@marrtags.de;178.32.51.218;;
9.6.2017 12:15;;Malicious-URL;Malicious-URL;;;dealydo.com;;;
9.6.2017 12:16;25a6110741e5c0943bd878fc100a6749;JS_NEMUCOD.SMK17;Malware;;Malware;AA-224-RR.zip;;anna.mills@eatsme.co.uk;223.186.209.90;;
9.6.2017 12:16;6f0ae1ae0c5b0e0e9eef4ac3b278b32b;JS_NEMUCOD.SMK17;Malware;;Malware;AA-224-RR.wsf;;anna.mills@eatsme.co.uk;223.186.209.90;;
9.6.2017 12:16;eb89e0e5d1c4cc7f4387da2732a0dc;JS_NEMUCOD.SMK17;Malware;;Malware;8061270.zip;;anna.mills@eatsme.co.uk;223.186.209.90;;

9.6.2017 12:20;020685d954f63a56744d1d6f0b4ba6a1;JS_NEMUCOD.SMK17;Malware;Malware;602869.zip;anna.mills@hornbyphillips.co.uk;59.99.103.248;;

9.6.2017 12:20;020685d954f63a56744d1d6f0b4ba6a1;JS_NEMUCOD.SMK17;Malware;Malware;481900.zip;anna.mills@incheochfarm.ndo.co.uk;94.187.48.95;;

9.6.2017 12:20;020685d954f63a56744d1d6f0b4ba6a1;JS_NEMUCOD.SMK17;Malware;Malware;2424689.zip;anna.mills@sr-accounts.co.uk;103.48.108.165;;

9.6.2017 12:20;2d1f82fb61a1153064bb538f0b0443cd;JS_NEMUCOD.SMK17;Malware;Malware;818617.zip;anna.mills@dandjcarpentryltd.co.uk;41.191.104.85;;

9.6.2017 12:20;56b6907f9d9a16b0966c1014653eebd;JS_NEMUCOD.SMK17;Malware;Malware;AA-267-RR.zip;anna.mills@dandjcarpentryltd.co.uk;41.191.104.85;;

9.6.2017 12:20;6819a9d5f6e1e8ea0c619f316d50b56b;JS_NEMUCOD.SMK17;Malware;Malware;AA-268-RR.zip;anna.mills@incheochfarm.ndo.co.uk;94.187.48.95;;

9.6.2017 12:20;94188f92ce3bdf2b9c433d64c50b27f8;JS_NEMUCOD.SMK17;Malware;Malware;AA-267-RR.wsf;anna.mills@dandjcarpentryltd.co.uk;41.191.104.85;;

9.6.2017 12:20;af4d052904e15b72bcd951bc393b77af;JS_NEMUCOD.SMK17;Malware;Malware;AA-268-RR.wsf;anna.mills@incheochfarm.ndo.co.uk;94.187.48.95;;

9.6.2017 12:23;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;support+wmy1hd5s3arn@telematica-group.com;206.225.87.131;;

9.6.2017 12:32;;Malicious-URL;Malicious-URL;;onlinesmartsale.com;45q267f6xb8zSof0i01r0Sgm2488t1@ANGY73;113.4.136.142;;

9.6.2017 12:32;;Malicious-URL;Malicious-URL;;onlinesmartsale.com;uensorl@heijmans.nl;113.4.136.142;;

9.6.2017 12:36;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@donseigal.com;103.11.74.25;;

9.6.2017 12:41;;Malicious-URL;;marketing@sw.solarwinds.com;199.15.214.39;;

9.6.2017 12:43;;Malicious-URL;;ackiemorse67@gmn.de;14.191.20.43;;

9.6.2017 12:45;;Malicious-URL;;marketing@sw.solarwinds.com;199.15.214.39;;

9.6.2017 12:47;;Malicious-URL;;marketing@sw.solarwinds.com;199.15.214.39;;

9.6.2017 12:50;;Malicious-URL;Malicious-URL;;organictabletinc.ru;notification+wj8vixmtm70t@duraplatexd35.com;74.208.250.177;;

9.6.2017 12:51;;Malicious-URL;Malicious-URL;;herbalbabsassist.ru;dgppjogqt@08742.com;120.6.134.236;;

9.6.2017 12:52;;Malicious-URL;Malicious-URL;;herbalbabsassist.ru;kshukcxm@0879232511.com;101.24.229.229;;

9.6.2017 13:00;;Malicious-URL;;admin@marrytags.de;178.32.51.218;;

9.6.2017 13:05;;Malicious-URL;;admin@marrytags.de;51.254.238.130;;

9.6.2017 13:22;;Malicious-URL;Malicious-URL;;aoyosj.com;zhangdi@hztbc.com;115.238.55.242;;

9.6.2017 13:22;;Malicious-URL;;lophinde.com;;;

9.6.2017 13:38;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

9.6.2017 13:43;;Malicious-URL;;s.gerchel@avh-untere-ohre.de;77.127.10.166;;

9.6.2017 13:50;;Malicious-URL;Malicious-URL;;fenghuang3.top;hr@fjtb.cn;59.56.182.81;;

9.6.2017 14:01;;Malicious-URL;Malicious-URL;;dock.email;noreply@runbenrun.info;93.90.123.200;;

9.6.2017 14:03;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club ;;;

9.6.2017 14:10;;Malicious-URL;;info@balticemail.com;89.40.112.8;;

9.6.2017 14:11;;Malicious-URL;;info@balticemail.com;89.40.112.8;;

9.6.2017 14:13;6bdc8df155073aac0330e129f62ba08e;JS_NEMUCOD.SMK17;Malware;Malware;836498.zip;anna.mills@mygmail.co.uk;182.185.151.79;;

9.6.2017 14:13;8d7eeb69249ed7f7f9b315209e5ff6b4;JS_NEMUCOD.SMK17;Malware;Malware;AA-095-RR.zip;anna.mills@mygmail.co.uk;182.185.151.79;;

9.6.2017 14:13;b66c914f67a0b4e040a4a746f44144b6;JS_NEMUCOD.SMK17;Malware;Malware;AA-095-RR.wsf;anna.mills@mygmail.co.uk;182.185.151.79;;

9.6.2017 14:13;;Malicious-URL;Malicious-URL;;contacts.net;;;

9.6.2017 14:14;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@hnga111.com;198.1.105.36;;

9.6.2017 14:15;056027e22a2bf892c2cae24d828c36b14;JS_NEMUCOD.SMK17;Malware;Malware;Malware;9459970.zip;anna.mills@360engineering.co.uk;175.158.52.35;;

9.6.2017 14:15;2102aa4f32512c2b49510e03b94e2d00;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-255-RR.wsf;anna.mills@bypublicdemand.co.uk;115.78.1.255;;

9.6.2017 14:15;2754c1e8ddce0f17be4d22d86d6613c0;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-255-RR.zip;anna.mills@bypublicdemand.co.uk;115.78.1.255;;

9.6.2017 14:15;2b5033852c65dc0cbf83986d7c96500c;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-229-RR.wsf;anna.mills@360engineering.co.uk;175.158.52.35;;

9.6.2017 14:15;579ec53e02ce9726ad5d72934df4a383;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-229-RR.zip;anna.mills@360engineering.co.uk;175.158.52.35;;

9.6.2017 14:15;76c4548c10169c36e7502efc011b0bc8;JS_NEMUCOD.SMK17;Malware;Malware;Malware;6003950.zip;anna.mills@bypublicdemand.co.uk;115.78.1.255;;

9.6.2017 14:18;6206e0adcc2f798c7fda40b68227c382;JS_NEMUCOD.SMK17;Malware;Malware;Malware;1323249.zip;anna.mills@sandjabbottceramicsplus.co.uk;223.227.118.197

9.6.2017 14:18;6341a8896435a41d8373d85cd9058307;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-013-RR.zip;anna.mills@sandjabbottceramicsplus.co.uk;223.227.118.197;;

9.6.2017 14:18;7343c5720b18320c52e9b5d876e257c;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-013-RR.wsf;anna.mills@sandjabbottceramicsplus.co.uk;223.227.118.197;;

9.6.2017 14:20;365511ea226a3628b19e31965e020f8;JS_NEMUCOD.SMK17;Malware;Malware;Malware;557062.zip;anna.mills@garratt-tiling.co.uk;213.74.95.138;;

9.6.2017 14:20;3cc86df94b473a322f9d4ec5c0c6f77;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-062-RR.wsf;anna.mills@garratt-tiling.co.uk;213.74.95.138;;

9.6.2017 14:20;a6debd3e78aac0b07ec0ee63db2fb0;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-062-RR.zip;anna.mills@garratt-tiling.co.uk;213.74.95.138;;

9.6.2017 14:23;1a7abc8e566dad3bd6309b1b6cc9d4a;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-067-RR.wsf;anna.mills@paroh.co.uk;111.91.4.60;;

9.6.2017 14:23;3e92b1b3584ad75695ab2231ca328f78;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-067-RR.zip;anna.mills@paroh.co.uk;111.91.4.60;;

9.6.2017 14:23;6fdc51d1d870c2249271988f6d4a1a6c;JS_NEMUCOD.SMK17;Malware;Malware;Malware;082493.zip;anna.mills@paroh.co.uk;111.91.4.60;;

9.6.2017 14:24;7444f622e8ed0b5ce7dbbe7f077cdae;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-253-RR.wsf;anna.mills@buksetrolden.dk;188.241.204.38;;

9.6.2017 14:24;9af713da471952dde1418e1d86f9447;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-253-RR.zip;anna.mills@buksetrolden.dk;188.241.204.38;;

9.6.2017 14:24;d15f2e3aaa9bfd2d457515b3c6bd5af;JS_NEMUCOD.SMK17;Malware;Malware;Malware;2342828.zip;anna.mills@buksetrolden.dk;188.241.204.38;;

9.6.2017 14:24;d15f2e3aaa9bfd2d457515b3c6bd5af;JS_NEMUCOD.SMK17;Malware;Malware;Malware;2838358.zip;anna.mills@buksetrolden.dk;188.241.204.38;;

9.6.2017 14:25;0337b81990559c306dd3bc872565e23b;JS_NEMUCOD.SMK17;Malware;Malware;Malware;852894.zip;anna.mills@harrogate.gov.uk;49.248.217.170;;

9.6.2017 14:25;0337b81990559c306dd3bc872565e23b;JS_NEMUCOD.SMK17;Malware;Malware;Malware;0924788.zip;anna.mills@headforsuccess.org.uk;122.175.220.179;;

9.6.2017 14:25;471847ba8771581443d293bc3b6518;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-047-RR.wsf;anna.mills@harrogate.gov.uk;49.248.217.170;;

9.6.2017 14:25;63104ee94fd51a97219dd133d0a839c5;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-047-RR.zip;anna.mills@harrogate.gov.uk;49.248.217.170;;

9.6.2017 14:26;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@stayathomefranchises.com;46.235.42.178;;

9.6.2017 14:28;8fde6c72377616b78327bb7ac3899ff4;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-016-RR.zip;anna.mills@denyarfreemanelec.co.uk;103.254.98.186;;

9.6.2017 14:28;d3c8975316f32955e78e92f6d7a5a107;JS_NEMUCOD.SMK17;Malware;Malware;Malware;2278625.zip;anna.mills@denyarfreemanelec.co.uk;103.254.98.186;;

9.6.2017 14:28;f8d8eadc114d6505be7ffb103765f4e9;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-016-RR.wsf;anna.mills@denyarfreemanelec.co.uk;103.254.98.186;;

9.6.2017 14:29;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@xn-w9zs14c.com;185.28.189.11;;

9.6.2017 14:29;;Malicious-URL;Malicious-URL;;organictabletinc.ru;support+74e7vtap0188@daniellelambinon.com;85.94.194.168;;

9.6.2017 14:30;;Malicious-URL;Malicious-URL;;macartu.cn;vdmilulf@hmshost.com.au;151.253.17.60;;

9.6.2017 14:36;;Malicious-URL;Malicious-URL;;yourtransparentministry.com;info@balticemail.com;217.61.2.141;;

9.6.2017 14:38;86a2ca5f68fd63bd66dbbfc516d7bb21;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-194-RR.zip;anna.mills@premiumstocksltd.co.uk;113.184.143.108;;

9.6.2017 14:38;9bbe0089bb76ab84cecf1044bfdbcf40;JS_NEMUCOD.SMK17;Malware;Malware;Malware;058882.zip;anna.mills@minster.york.sch.uk;154.66.162.138;;

9.6.2017 14:38;aaa33aceb49507611ea6c6850ff10f9d;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-079-RR.wsf;anna.mills@minster.york.sch.uk;154.66.162.138;;

9.6.2017 14:38;b8b95c8fa0f7cd1250616ad460353033;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-079-RR.zip;anna.mills@minster.york.sch.uk;154.66.162.138;;

9.6.2017 14:38;d195ab72d0fbdab3d510f741c731f4fb;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-194-RR.wsf;anna.mills@premiumstocksltd.co.uk;113.184.143.108;;

9.6.2017 14:38;f1ad38887d6b85c5f475de1272650fe8;JS_NEMUCOD.SMK17;Malware;Malware;Malware;6723283.zip;anna.mills@premiumstocksltd.co.uk;113.184.143.108;;

9.6.2017 14:39;020438035d3e22bf243ba1aafde98266;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-027-RR.wsf;anna.mills@epcrepair.co.uk;196.207.126.158;;

9.6.2017 14:39;76cf11239fe42bb6f0723a21b49a3467;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-027-RR.zip;anna.mills@epcrepair.co.uk;196.207.126.158;;

9.6.2017 14:39;8001159aa6429cb815ed57f36ff0bf;JS_NEMUCOD.SMK17;Malware;Malware;Malware;5015758.zip;anna.mills@epcrepair.co.uk;196.207.126.158;;

9.6.2017 14:40;;Malicious-URL;;info@balticemail.com;89.40.112.8;;

9.6.2017 14:41;6d070b40699278e11781ff0a7019fd0e;JS_NEMUCOD.SMK17;Malware;Malware;Malware;726399.zip;anna.mills@glasgowdogtrainingclub.org.uk;125.99.178.116;;

9.6.2017 14:41;6d070b40699278e11781ff0a7019fd0e;JS_NEMUCOD.SMK17;Malware;Malware;Malware;425736.zip;anna.mills@robormerod.co.uk;125.234.99.98;;

9.6.2017 14:41;78215a8414b7638c93a9b4e2b9e55c76;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-120-RR.wsf;anna.mills@glasgowdogtrainingclub.org.uk;125.99.178.116;;

9.6.2017 14:41;900e2d6a61d8e4d31027204f29b3efcf;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-120-RR.zip;anna.mills@glasgowdogtrainingclub.org.uk;125.99.178.116;;

9.6.2017 14:44;JS_NEMUCOD.SMK17;Malware;Malware;7608026.zip;anna.mills@enjoyspanish.co.uk;;;

9.6.2017 14:45;066da017763b8ba36ee6aed40c977ec9;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-129-RR.wsf;anna.mills@enjoyspanish.co.uk;223.31.114.158;;

9.6.2017 14:45;d96edba7afb12cd3745eb70087ef5df;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-129-RR.zip;anna.mills@enjoyspanish.co.uk;223.31.114.158;;

9.6.2017 14:45;709302bbf49b19398f8a921ec9db411d;JS_NEMUCOD.SMK17;Malware;Malware;Malware;7608026.zip;anna.mills@enjoyspanish.co.uk;223.31.114.158;;

9.6.2017 14:47;;Malicious-URL;;test@hntstjst.com;113.240.230.62;;

9.6.2017 14:50;;Malicious-URL;;admin@marrytags.de;178.32.51.218;;

9.6.2017 14:51;176f9aa02d1bc5189d7e29d66a082b7c;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-147-RR.zip;anna.mills@symphonycom.co.uk;117.208.203.18;;

9.6.2017 14:51;c83fd4fdaffb1bcd89d25cc4b27b1bc7;JS_NEMUCOD.SMK17;Malware;Malware;Malware;955293.zip;anna.mills@symphonycom.co.uk;117.208.203.18;;

9.6.2017 14:51;fd8aadacafea5d8869f496cf00f1971;JS_NEMUCOD.SMK17;Malware;Malware;Malware;AA-147-RR.wsf;anna.mills@symphonycom.co.uk;117.208.203.18;;

9.6.2017 14:54;;Malicious-URL;Malicious-URL;;macartu.cn;kbqrapusyu@ballerand.us;217.10.204.238;;

9.6.2017 14:54;;Malicious-URL;Malicious-URL;;macartu.cn;mzribz@dfll.us;217.10.204.238;;

9.6.2017 14:55;;Malicious-URL;Malicious-URL;Malicious-URL;;hxxp://www.3thirdeye.com/blog/wp-content/themes/sketch/6496199b783.html;info@mmtransportation.com;59.95.127.73;;

9.6.2017 14:57;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

9.6.2017 14:58;;Malicious-URL;Malicious-URL;;medicemail.com;;;

9.6.2017 15:03;;Malicious-URL;Malicious-URL;;bcontacts.net;admin@marrytags.de;178.32.60.137;;

9.6.2017 15:09;;Malicious-URL;Malicious-URL;;macartu.cn;nnbuzdekv@hmsa.org.uk;164.132.191.254;;

9.6.2017 15:12;;Malicious-URL;;rbsuxa.com;;;

9.6.2017 15:17;;Malicious-URL;Malicious-URL;;organictabletinc.ru;update+i8q8uia59hh0@coridas.com;87.106.191.206;;

9.6.2017 15:42;;Malicious-URL;Malicious-URL;;hxxp://www.connectedglobalgroup.com/wp-content/themes/pagelines-template-theme/8204b076331.html;christian.schoeggel@stmk.gv.at;171.249.59.128;;

9.6.2017 15:45;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

9.6.2017 15:59;;Malicious-URL;;contact@hasamx.com;93.90.122.53;;

9.6.2017 16:06;;Malicious-URL;;olesmains.ch;;;

9.6.2017 16:21;;Malicious-URL;;support@4poketshow.net;195.140.195.194;;

9.6.2017 16:25;;Malicious-URL;;info@balticemail.com;217.61.2.141;;

9.6.2017 16:27;;Malicious-URL;;muasurabaya.com;;;

9.6.2017 16:37;;Malicious-URL;Malicious-URL;;bcontacts.net;;;

9.6.2017 16:51;;Malicious-URL;;desink.com.mx;;;

9.6.2017 16:52;;Malicious-URL;;desink.com.mx;;;

9.6.2017 16:55;;Malicious-URL;Malicious-URL;;bogproduct.kz;eleniwilladw@excite.it;14.174.250.34;;

9.6.2017 16:55;;Malicious-URL;Malicious-URL;;spygrit.com;essio@fraport.de;187.177.36.227;;

9.6.2017 16:55;;Malicious-URL;Malicious-URL;;bogproduct.kz;;;

9.6.2017 16:57;;Malicious-URL;;springfieldcleaningsupply.com;;;

9.6.2017 17:03;;Malicious-URL;;magiccleansandra.com;;;

9.6.2017 17:08;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

9.6.2017 17:11;;Malicious-URL;;mellisa@correlaserver.com;185.171.232.235;;

9.6.2017 17:11;;Malicious-URL;;ferne@correlaserver.com;185.171.232.241;;

9.6.2017 17:11;;Malicious-URL;;mellisa@correlaserver.com;185.171.232.235;;

9.6.2017 17:12;;Malicious-URL;;mellisa@correlaserver.com;185.171.232.235;;

9.6.2017 17:16;;Malicious-URL;;agueda@correlaserver.com;185.171.232.234;;

9.6.2017 17:16;;Malicious-URL;;mellisa@correlaserver.com;185.171.232.235;;

9.6.2017 17:17;;Malicious-URL;Malicious-URL;;bogproduct.kz;gsod@l8s.co.uk;180.176.164.196;;

9.6.2017 17:17;;Malicious-URL;;mellisa@correlaserver.com;185.171.232.235;;

9.6.2017 17:20;;Malicious-URL;;admin@marrytags.de;51.255.15.239;;

9.6.2017 17:30;;Malicious-URL;;itreportandnews.net;;;

9.6.2017 17:33;;Malicious-URL;Malicious-URL;;medicemail.com;;;

9.6.2017 17:36;;Malicious-URL;;mellisa@correlaserver.com;185.171.232.235;;

9.6.2017 17:37;;Malicious-URL;;info@firetrainingsolution.com;194.88.106.148;;

9.6.2017 18:01;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

9.6.2017 18:25;;Malicious-URL;Malicious-URL;;masterlead.info;;;

9.6.2017 18:26;;Malicious-URL;;panessgroup.com;;;

9.6.2017 18:33;;Malicious-URL;;info@rahoitustuki.fi;95.211.162.142;;

9.6.2017 18:35;;Malicious-URL;Malicious-URL;;hxxp://www.membership.newmarketcs.com/wp-includes/js/tinymce/themes/inlite/5506d46af35.html;dymnpnamckay@patons.org.uk;1.52.126.46;;

9.6.2017 18:36;;Malicious-URL;;kshemadiagnostics.com;;;

9.6.2017 18:38;;Malicious-URL;;kshemadiagnostics.com;;;

9.6.2017 18:51;;Malicious-URL;;archive-authority.com;;;

9.6.2017 18:55;;Malicious-URL;;canmakingsolutions.es;;;

9.6.2017 18:57;;Malicious-URL;;hxxp://www.truhlarstvi-acer.cz/administrator/huez/6743c509ae3.html;rhyssettles1441@mailcatch.com;123.22.140.219;;

9.6.2017 19:06;;Malicious-URL;;admin@marrytags.de;178.32.58.252;;

9.6.2017 19:30;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

9.6.2017 19:32;;Malicious-URL;Malicious-URL;;aoyosj.com;xujing@16ds.com;117.79.81.101;;

9.6.2017 19:33;;Malicious-URL;;postmaster@bureau101.ns.utoronto.ca;128.100.132.18;;

9.6.2017 19:34;;Malicious-URL;;volkovrn@k66.ru;125.33.234.180;;

9.6.2017 19:45;;Malicious-URL;;admin@marrytags.de;178.32.58.252;;

9.6.2017 19:58;;Malicious-URL;Malicious-URL;;univac.ci;joakim@unge.se;195.191.39.49;;

9.6.2017 19:59;;Malicious-URL;Malicious-URL;;macartu.cn;tddfxmrioi@ci.walnut-creek.ca.us;112.124.50.85;;

9.6.2017 19:59;;Malicious-URL;Malicious-URL;;macartu.cn;uulzieruchal@jonesent.us;112.124.50.85;;

9.6.2017 20:13;;Malicious-URL;Malicious-URL;;thequantumcodes.trade;Mailer-Daemon@muvu.de;213.239.221.150;;

9.6.2017 20:13;;Malicious-URL;;admin@marrytags.de;51.255.15.239;;

9.6.2017 20:20;;Malicious-URL;;wicky@heartlandhomehealth.net;183.80.86.16;;

9.6.2017 20:24;;Malicious-URL;Malicious-URL;;macartu.cn;clqwp@ci.south-pasadena.ca.us;61.141.21.34;;

9.6.2017 20:45;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@decoratem.com;83.172.21.22;;

9.6.2017 20:46;;Malicious-URL;;sales@customercare.sap;169.55.59.69;;

9.6.2017 21:17;;Malicious-URL;;mcfadden5@nsc.eu.com;201.176.11.148;;

9.6.2017 21:18;;Malicious-URL;;owedyajqghwmkyqkvh@swissonline.ch;191.103.244.99;;

9.6.2017 21:25;;Malicious-URL;;guwc@surdeu.de;190.144.26.125;;

9.6.2017 21:26;;Malicious-URL;Malicious-URL;;hxxp://www.connectedglobalgroup.com/wp-content/themes/pagelines-template-theme/8204b076331.html;guwc@surdeu.de;190.144.26.125;;

9.6.2017 21:38;;Malicious-URL;Malicious-URL;;medicalrxquality.su;pending+9f5tg97n87@costur-art.com;93.159.141.100;;

9.6.2017 21:44;;Malicious-URL;Malicious-URL;;medicalrxquality.su;support+87t8jb5bck9q@mrusb.com;128.199.197.111;;

9.6.2017 22:00;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@thebull-prints.com;5.2.27.27;;

9.6.2017 22:13;;Malicious-URL;;fonari-park.com.ua;;;

9.6.2017 22:23;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;admin@marrytags.de;178.32.58.252;;

9.6.2017 22:52;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

9.6.2017 23:00;;Malicious-URL;Malicious-URL;;koko-go.com;kut@tb.com;113.90.35.216;;

9.6.2017 23:09;;Malicious-URL;;info@balticemail.com;89.40.112.8;;

9.6.2017 23:34;;Malicious-URL;Malicious-URL;;xurl.es;dimitroff.yaroslav@yandex.ru;14.36.1.142;;

9.6.2017 23:36;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@xn--1-Oga.com;46.101.72.178;;

9.6.2017 23:36;;Malicious-URL;Malicious-URL;;macartu.cn;ipfvssrpl@hmsherdan.co.uk;221.192.134.92;;

9.6.2017 23:36;;Malicious-URL;;dealydid.com;;;

9.6.2017 23:46;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

9.6.2017 23:51;;Malicious-URL;;;muasurabaya.com;;;
 9.6.2017 23:52;;Malicious-URL;;;muasurabaya.com;;;
 9.6.2017 23:59;;Malicious-URL;Malicious-URL;;;mynaka.me;agrigg@activeware.com;203.209.122.219;;
 10.6.2017 0:04;;Malicious-URL;;;admin@marrytags.de;178.32.60.137;;
 10.6.2017 0:14;;Malicious-URL;Malicious-URL;;;macartu.cn;xjxitd@hmtrust.com;217.61.123.233;;
 10.6.2017 0:18;;Malicious-URL;;;info@balticemail.com;89.40.112.8;;
 10.6.2017 0:23;;Malicious-URL;;;info@balticemail.com;89.46.78.104;;
 10.6.2017 0:33;;Malicious-URL;Malicious-URL;;;uoteuch.ru;admin@marrytags.de;51.255.15.239;;
 10.6.2017 0:34;;Malicious-URL;;;hxxp://sosh9.uoteuch.ru/administrator/components/com_checkin/views/checkin/tmpl/sitemap.html;afxfhfhqm@sernomadadigital.com;83.44.28.171;;
 10.6.2017 0:35;;Malicious-URL;;;info@balticemail.com;217.61.2.141;;
 10.6.2017 0:36;;Malicious-URL;Malicious-URL;;;macartu.cn;ipcndo@chatline.us;119.61.13.242;;
 10.6.2017 0:36;;Malicious-URL;Malicious-URL;;;macartu.cn;ytdrqrqfauo@neosho.k12.mo.us;119.61.13.242;;
 10.6.2017 0:37;;Malicious-URL;;;info@rahoitustuki.fi;195.140.195.194;;
 10.6.2017 0:42;;Malicious-URL;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 0:43;;Malicious-URL;;;alberta.pettry@pcgame.de;168.195.13.13;;
 10.6.2017 0:43;;Malicious-URL;;;info@balticemail.com;89.40.112.8;;
 10.6.2017 0:49;;Malicious-URL;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 0:52;;Malicious-URL;;;saglikbandi.com;;;
 10.6.2017 0:52;;Malicious-URL;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 0:58;;Malicious-URL;;;john.macintb@striker.ottawa.on.ca;46.2.26.177;;
 10.6.2017 1:02;;Malicious-URL;;;shawonislam.com;;;
 10.6.2017 1:08;;Malicious-URL;;;ntmwrnga@free-236-72.mediaworksit.net;178.253.236.72;;
 10.6.2017 1:09;;Malicious-URL;;;info@balticemail.com;89.40.112.8;;
 10.6.2017 1:28;;Malicious-URL;;;xujing@16ds.com;117.79.81.101;;
 10.6.2017 1:32;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;apache@srvweb3lin.stream-es.com;37.46.73.27;;
 10.6.2017 1:42;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;tamanbud@server55.wowrack.com;208.115.97.35;;
 10.6.2017 1:45;;Malicious-URL;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 1:50;;Malicious-URL;Malicious-URL;;;macartu.cn;877666448248467.QD31108@rkhz.hmshost.com.au;202.110.97.170;;
 10.6.2017 2:01;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;rgirewh@021fy.com;115.44.103.134;;
 10.6.2017 2:19;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;nobody@mob.mobilshareholders.com;198.154.193.110;;
 10.6.2017 2:22;;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 2:27;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;tar1@194-58-96-96.ovz.vps.regruhosting.ru;194.58.96.96;;
 10.6.2017 2:34;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;sol@svm46108.vps.tagadab.com;80.241.49.114;;
 10.6.2017 2:35;;Malicious-URL;Malicious-URL;;;borsrtty.info;;;
 10.6.2017 2:39;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;byu1191480001@byu-119148.hichina.com;123.56.106.140;;
 10.6.2017 2:39;;Malicious-URL;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 2:39;;Malicious-URL;Malicious-URL;;;borsrtty.info;;;
 10.6.2017 2:40;;Malicious-URL;Malicious-URL;;;borsrtty.info;;;
 10.6.2017 2:43;;Malicious-URL;Malicious-URL;;;borsrtty.info;;;
 10.6.2017 2:45;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;webmaster@52sad.ru;91.240.86.75;;
 10.6.2017 2:47;;Malicious-URL;Malicious-URL;;;macartu.cn;okwraos@hmtel.com;50.199.157.91;;
 10.6.2017 2:53;;Malicious-URL;Malicious-URL;;;borsrtty.info;uixjq@007mundo.com;212.16.98.57;;
 10.6.2017 2:53;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;;;
 10.6.2017 2:56;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;apache@srvweb3lin.stream-es.com;37.46.73.27;;
 10.6.2017 2:58;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;qyu1251330001@qyu-125133.hichina.com;118.190.173.87;;
 10.6.2017 3:07;;Malicious-URL;;;admin@marrytags.de;178.32.58.252;;
 10.6.2017 3:11;;Malicious-URL;Malicious-URL;;;borsrtty.info;admin@marrytags.de;51.255.15.239;;
 10.6.2017 3:22;;Malicious-URL;Malicious-URL;;;macartu.cn;tddbiiid@hmsc.harvard.edu;120.24.164.247;;
 10.6.2017 3:23;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;spmentone@ctwebhost01-melm.ctsvs.com.au;119.31.231.198;;
 10.6.2017 3:26;;Malicious-URL;Malicious-URL;;;macartu.cn;pdrpm@hms.harvard.edu;113.4.136.142;;
 10.6.2017 3:28;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;platform@buergerexperten.de;91.250.99.64;;
 10.6.2017 3:28;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;wwwrun@srv-web.site;90.182.157.205;;
 10.6.2017 3:44;;Malicious-URL;;;ningazetteer@bautec.de;115.254.23.114;;
 10.6.2017 3:49;;Malicious-URL;;;cheriet@biw-ag.de;190.237.181.191;;
 10.6.2017 3:58;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;spmentone@ctwebhost01-melm.ctsvs.com.au;119.31.231.198;;
 10.6.2017 4:08;;Malicious-URL;;;reply@gedonte.com;195.140.195.194;;
 10.6.2017 4:21;a067db7d400132e07201e412ab49c04d;Trojan.Mdropper;Malware;Malware;Malware;A4EHAJ20EY.doc;;apache@lobster.deltapath.com;202.130.106.38;;
 10.6.2017 5:09;;Malicious-URL;Malicious-URL;;;canaryboutique.com;robk@bmerhbc.bnr.ca;202.29.183.5;;
 10.6.2017 5:10;;Malicious-URL;;;fedikson@biw-ag.de;113.175.43.213;;
 10.6.2017 5:13;;Malicious-URL;Malicious-URL;;;canaryboutique.com;gunho@surdeu.de;111.93.6.126;;
 10.6.2017 5:14;;Malicious-URL;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 5:15;;Malicious-URL;Malicious-URL;;;macartu.cn;yyvabngoakwp@westottawa.k12.mi.us;24.238.122.11;;
 10.6.2017 5:43;;Malicious-URL;;;admin@marrytags.de;51.254.238.130;;
 10.6.2017 5:49;;Malicious-URL;Malicious-URL;;;hxxp://www.contrerasasesores.com/wp-includes/js/tinymce/plugins/tabfocus/245594fb32d.html;mail@dreams2success.com;27.64.181.9;;
 10.6.2017 5:54;;Malicious-URL;;;pgraves@bmersb17.bnr.ca;203.81.71.66;;
 10.6.2017 6:02;;Malicious-URL;;;admin@marrytags.de;178.32.51.218;;
 10.6.2017 6:08;;Malicious-URL;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 6:21;;Malicious-URL;Malicious-URL;;;eveningmanga.com;info@HUACK.br;113.186.227.91;;
 10.6.2017 6:21;;Malicious-URL;Malicious-URL;;;sexy-dates.ru;;;
 10.6.2017 6:44;;Malicious-URL;Malicious-URL;;;senderer.ru;efcundar@nuovicittadini.com;84.232.76.184;;
 10.6.2017 6:52;;Malicious-URL;Malicious-URL;;;biosc.com;info@019710.com;76.164.223.106;;
 10.6.2017 6:55;;Malicious-URL;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 6:57;;Malicious-URL;Malicious-URL;;;basedbusinesstraffic.com;ninabuck952@gmail.com;180.178.44.250;;
 10.6.2017 6:57;;Malicious-URL;;;brians-house.org;;;
 10.6.2017 7:05;;Malicious-URL;Malicious-URL;;;hxxp://www.shop.consultaustrianz.com/wp-includes/js/tinymce/skins/lightgray/62543d1e844.html;df2f31a9f7573e8b5@frugo.de;14.167.85.237;;
 10.6.2017 7:20;;Malicious-URL;Malicious-URL;;;dealydo.com;info@pyridio.com;109.201.141.157;;
 10.6.2017 7:38;;Malicious-URL;;;info@extraweb.info;195.140.195.194;;
 10.6.2017 7:38;;Malicious-URL;;;emyrrehc@morgner.de;113.186.0.133;;
 10.6.2017 7:39;;Malicious-URL;Malicious-URL;;;macartu.cn;mtdrbeehga@hmsheridan.co.uk;94.20.21.38;;
 10.6.2017 7:40;;Malicious-URL;;;kupxcvzf@rappa.de;171.226.42.89;;
 10.6.2017 7:46;;Malicious-URL;;;vyshki.com;;;
 10.6.2017 7:49;;Malicious-URL;;;fwd.1258743003nnez@anzeigenschleuder.com;113.180.95.239;;
 10.6.2017 8:00;;Malicious-URL;Malicious-URL;;;belamine.com;czunz@konflikthfen.de;103.38.175.61;;
 10.6.2017 8:26;;Malicious-URL;Malicious-URL;;;familierabatnordic.dk;;;
 10.6.2017 8:34;;Malicious-URL;;;xrjo.cn;;;
 10.6.2017 8:37;;Malicious-URL;Malicious-URL;Malicious-URL;;;amino-disqus.club;;;
 10.6.2017 8:45;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;brpuwciye@01.net;49.140.162.133;;
 10.6.2017 8:45;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;czuezwo@009191.com;61.159.15.198;;

10.6.2017 9:01;;Malicious-URL;;;softwaredestination.org;;;
 10.6.2017 9:04;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;admin@marrytags.de;178.32.58.252;;
 10.6.2017 9:05;;Malicious-URL;Malicious-URL;;;twebglobal.com;jsemsrott@freesulf.de;171.235.72.77;;
 10.6.2017 9:21;;Malicious-URL;;;nordiskhandelsplads.dk;;;
 10.6.2017 9:28;;Malicious-URL;Malicious-URL;;;macartu.cn;bvfrgrgfrbrq@durand.k12.wi.us;186.117.156.147;;
 10.6.2017 9:28;;Malicious-URL;Malicious-URL;;;macartu.cn;dbmzuyrxuun@ago.us;186.117.156.147;;
 10.6.2017 9:38;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 9:43;;Malicious-URL;Malicious-URL;;hxxp://www.glamourgabon.com/wp-includes/js/tinymce/plugins/compat3x/./0054b59d796.html;rrohac@techreps.com;186.133.205.202;;
 10.6.2017 9:45;;Malicious-URL;Malicious-URL;;hxxp://www.glamourgabon.com/wp-includes/js/tinymce/plugins/compat3x/./0054b59d796.html;mushaway@quik.com;27.3.1.204;;
 10.6.2017 9:48;;Malicious-URL;Malicious-URL;;;macartu.cn;yurfrgugik@hmveng.com;49.140.212.37;;
 10.6.2017 9:54;;Malicious-URL;Malicious-URL;;;scandigogo.com;;;
 10.6.2017 9:57;;Malicious-URL;Malicious-URL;;;scandigogo.com;;;
 10.6.2017 10:05;;Malicious-URL;;;payzure.com;;;
 10.6.2017 10:10;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 10:12;;Malicious-URL;Malicious-URL;;senderer.ru;gjzrix@yokaribas.com;62.28.83.97;;
 10.6.2017 10:58;;Malicious-URL;;;kina@intelisell.com;94.23.76.90;;
 10.6.2017 11:05;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 11:11;;Malicious-URL;Malicious-URL;;;scandigogo.com;;;
 10.6.2017 11:22;;Malicious-URL;Malicious-URL;;;medicemail.com;;;
 10.6.2017 11:24;;Malicious-URL;Malicious-URL;;;macartu.cn;761224106100314.NT63143@och.htmel.com;49.140.88.204;;
 10.6.2017 11:26;;Malicious-URL;Malicious-URL;;;organictabletinc.ru;;;
 10.6.2017 11:36;;Malicious-URL;Malicious-URL;;;macartu.cn;ddefqu@hmsheridan.co.uk;149.202.237.218;;
 10.6.2017 11:45;;Malware;Malicious-URL;;;admin@firmram.com;212.16.98.57;;
 10.6.2017 11:48;;Malicious-URL;Malicious-URL;;;sexy-dates.ru;info@HEIGH.nl;39.54.153.3;;
 10.6.2017 11:49;;Malicious-URL;Malicious-URL;;;blackhat.agency;anittiff04@gmail.com;180.178.42.82;;
 10.6.2017 11:53;;Malicious-URL;Malicious-URL;;;macartu.cn;mvknjbbesih@hmsheridan.co.uk;59.72.109.47;;
 10.6.2017 12:02;;Malicious-URL;Malicious-URL;;;sexy-dates.ru;info@PRICKLE.pl;14.176.105.47;;
 10.6.2017 12:08;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 12:09;;Malicious-URL;Malicious-URL;;;myinstabuzz.com;lambertkeng249@gmail.com;203.255.31.195;;
 10.6.2017 12:11;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 12:14;;Malicious-URL;Malicious-URL;;;medicalrxreward.ru;pending+gu2495nkfa0t@edmonton-marketing.com;87.117.195.8;;
 10.6.2017 12:17;;Malicious-URL;Malicious-URL;;;sexy-dates.ru;info@ILLUSORY.pl;185.43.189.104;;
 10.6.2017 12:27;;Malicious-URL;;;admin@marrytags.de;178.32.51.218;;
 10.6.2017 12:29;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 12:39;;Malicious-URL;;;admin@marrytags.de;178.32.60.137;;
 10.6.2017 12:59;;Malicious-URL;Malicious-URL;;;negativeseos.agency;buviregi380@gmail.com;112.121.187.170;;
 10.6.2017 13:03;;Malicious-URL;;;seoient.org;;;
 10.6.2017 13:03;;Malicious-URL;;;extraordines.com;;;
 10.6.2017 13:06;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;noreply@starburst.com;195.140.195.194;;
 10.6.2017 13:14;;Malicious-URL;Malicious-URL;;;medicalrxquality.su;alert@coordinategear.com;153.122.2.161;;
 10.6.2017 13:18;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 13:19;;Malicious-URL;Malicious-URL;;;medicalrxquality.su;alert@geomediablog.com;174.138.76.166;;
 10.6.2017 13:25;;Malicious-URL;Malicious-URL;;;macartu.cn;ixtbozcnl@hms.ru;213.32.113.189;;
 10.6.2017 13:26;;Malicious-URL;Malicious-URL;;;medicalrxquality.su;support+cv0k9nhr7ko0@speed-car-services.com;94.136.55.207;;
 10.6.2017 13:26;;Malicious-URL;Malicious-URL;;;organictabletinc.ru;update+ujdjq1zt93v@rodagolfproperties.com;185.45.75.235;;
 10.6.2017 13:31;;Malicious-URL;Malicious-URL;;;medicalrxreward.ru;alert@disaney.com;103.4.17.82;;
 10.6.2017 13:43;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 13:45;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 13:52;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 13:57;;Malicious-URL;Malicious-URL;;;organictabletinc.ru;pending+norkxt6os7j3@truthconsulting.com;153.122.150.109;;
 10.6.2017 14:07;;Malicious-URL;;;admin@marrytags.de;178.32.58.252;;
 10.6.2017 14:11;;Malicious-URL;;;zhangdi@hztbc.com;115.238.55.242;;
 10.6.2017 14:14;;Malicious-URL;Malicious-URL;;;medicalrxreward.ru;alert@troutfits.com;81.4.127.214;;
 10.6.2017 14:47;;Malicious-URL;Malicious-URL;;;medicalrxquality.su;alert@swansbooks.com;46.235.42.124;;
 10.6.2017 14:49;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 14:52;;Malicious-URL;Malicious-URL;;;macartu.cn;yvmfahg@bankserv.us;203.142.48.188;;
 10.6.2017 14:53;;Malicious-URL;Malicious-URL;;;macartu.cn;irrtptvqh@hmt-electric.com;5.135.195.166;;
 10.6.2017 14:53;;Malicious-URL;Malicious-URL;;;macartu.cn;uaqgwxf@hmt-ffb.de;50.199.157.91;;
 10.6.2017 14:54;;Malicious-URL;Malicious-URL;;;medicemail.com;;;
 10.6.2017 14:58;;Malicious-URL;;;admin@farmser.com;212.16.98.57;;
 10.6.2017 14:59;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;uamsgmpez@Odunet.com;94.20.21.38;;
 10.6.2017 15:00;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;dbsehi@0energylighting.com;182.88.189.127;;
 10.6.2017 15:00;;Malicious-URL;Malicious-URL;;;sexy-dates.ru;info@PUCK.it;1.52.122.75;;
 10.6.2017 15:00;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;visstik@0gmail.com;182.88.128.58;;
 10.6.2017 15:19;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 15:23;;Malicious-URL;;;admin@marrytags.de;178.32.58.252;;
 10.6.2017 15:35;;Malicious-URL;;;admin@marrytags.de;178.32.58.252;;
 10.6.2017 15:37;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 15:58;;Malicious-URL;;;nordiskhandelsplads.dk;;;
 10.6.2017 16:12;;Malicious-URL;;;lophinde.com;;;
 10.6.2017 16:16;;Malicious-URL;Malicious-URL;;;macartu.cn;sxkgchclzffc@tot.us;216.8.223.52;;
 10.6.2017 16:17;;Malicious-URL;;;admin@marrytags.de;51.255.15.239;;
 10.6.2017 16:33;;Malicious-URL;;;admin@marrytags.de;178.32.58.252;;
 10.6.2017 16:37;;Malicious-URL;;;admin@marrytags.de;51.254.238.130;;
 10.6.2017 17:04;;Malicious-URL;Malicious-URL;;;macartu.cn;aaunqs@hmveng.com;221.145.242.67;;
 10.6.2017 17:04;;Malicious-URL;Malicious-URL;;;macartu.cn;awronussg@hmv.at;221.145.242.67;;
 10.6.2017 17:13;;Malicious-URL;;;rambler.ws;;;
 10.6.2017 17:13;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 17:20;;Malicious-URL;Malicious-URL;;;hospitaliers.eu;;;
 10.6.2017 17:37;;Malicious-URL;Malicious-URL;;;medicemail.com;;;
 10.6.2017 17:59;;Malicious-URL;Malicious-URL;;;macartu.cn;gnyjie@hmtel.com;47.90.9.61;;
 10.6.2017 18:03;;Malicious-URL;;;admin@marrytags.de;178.32.51.218;;
 10.6.2017 18:04;;Malicious-URL;;;admin@marrytags.de;51.255.15.239;;
 10.6.2017 18:18;;Malicious-URL;Malicious-URL;;;rbiosc.com;info@019710.com;76.164.223.112;;
 10.6.2017 18:19;;Malicious-URL;;;infohoon@nate.com;117.53.114.172;;
 10.6.2017 18:57;;Malicious-URL;;;admin@marrytags.de;51.255.15.239;;
 10.6.2017 19:03;;Malicious-URL;Malicious-URL;;;macartu.cn;Foster_Jess@andrightetti.us;101.200.151.233;;
 10.6.2017 19:37;;Malicious-URL;;;msqym.com;;;
 10.6.2017 19:39;;Malicious-URL;;;admin@marrytags.de;178.32.51.218;;
 10.6.2017 19:43;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 19:44;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;tjcoobyeeqx@1065thebeat.com;123.122.63.121;;
 10.6.2017 19:55;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;mmbwpxwg@106db.com;121.232.53.120;;
 10.6.2017 20:05;;Malicious-URL;;;admin@marrytags.de;51.254.238.130;;
 10.6.2017 20:31;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;tybyveu@0769art.com;195.140.195.194;;
 10.6.2017 21:15;;Malicious-URL;Malicious-URL;;;macartu.cn;xbgvvp@jpm.us;101.200.151.233;;
 10.6.2017 21:22;;Malicious-URL;Malicious-URL;;;herbaltabsassist.ru;abmgkn@029cn.com;212.16.98.57;;

10.6.2017 21:22;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 21:26;;Malicious-URL;Malicious-URL;;marrytags.de;admin@marrytags.de;178.32.51.218;;;
 10.6.2017 21:33;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 21:36;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 21:44;;Malicious-URL;Malicious-URL;;newsmktg.com;abuse@gmail.com;103.63.2.204;;;
 10.6.2017 22:13;;Malicious-URL;Malicious-URL;;masterlead.info;;;
 10.6.2017 23:18;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 10.6.2017 23:35;;Malicious-URL;Malicious-URL;;newsmktg.com;abuse-crescom.fi@gmail.com;103.63.2.239;;;
 10.6.2017 23:47;;Malicious-URL;Malicious-URL;;medicalrxquality.su;update+aaawp7bb674k@transcriptiontech.com;85.236.61.236;;;
 10.6.2017 23:48;;Malicious-URL;Malicious-URL;;newsmktg.com;antti.jarvenpaa-cygate.fi@gmail.com;103.63.2.239;;;
 10.6.2017 23:57;;Malicious-URL;;peterblack@infoweb.cz;171.229.199.180;;;
 11.6.2017 0:27;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@westporttownhouses.com;62.149.143.55;;;
 11.6.2017 0:30;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;support+cfii45njmky@mastershares.com;103.241.128.100;;;
 11.6.2017 0:57;;Malicious-URL;Malicious-URL;;macartu.cn;bfpuclsegain@huan.us;222.133.16.134;;;
 11.6.2017 0:57;;Malicious-URL;Malicious-URL;;macartu.cn;yaosagpzcuf@aaroe.us;222.133.16.134;;;
 11.6.2017 1:01;;Malicious-URL;Malicious-URL;;gunsuji.cn;gaot@sddy.com;113.128.207.170;;;
 11.6.2017 1:11;;Malicious-URL;Malicious-URL;;herbalabsassist.ru;vayodxteyo@09.myspace.com;120.6.35.24;;;
 11.6.2017 1:17;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 1:25;;Malicious-URL;;cackbobo.info;;;
 11.6.2017 1:26;;Malicious-URL;;cackbobo.info;;;
 11.6.2017 1:42;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 1:48;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@beautifulabel.com;195.138.217.155;;;
 11.6.2017 1:53;;Malicious-URL;Malicious-URL;;macartu.cn;aoakftlo@hmshost.com;59.37.22.82;;;
 11.6.2017 1:58;;Malicious-URL;Malicious-URL;;medicalrxquality.su;notification+x5460cqbd05@usedofficefurniturebatonrouge.com;185.4.29.216;;;
 11.6.2017 2:00;;Malicious-URL;Malicious-URL;;organictabletinc.ru;pending+y4y6rcx75nog@etcsteakhouse.com;85.25.210.227;;;
 11.6.2017 2:17;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 2:18;;Malicious-URL;Malicious-URL;;macartu.cn;aidawbdl@hmshost.com.au;213.32.108.109;;;
 11.6.2017 2:18;;Malicious-URL;;sem-store.com;;;
 11.6.2017 3:27;;Malicious-URL;;info@zimdrom.ga;59.153.49.84;;;
 11.6.2017 3:58;;Malicious-URL;Malicious-URL;;macartu.cn;282206666470351.XV60533@ign.hmshost.com;51.254.55.246;;;
 11.6.2017 4:04;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 4:20;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 5:07;;Malicious-URL;;daniel-beer.de;;;
 11.6.2017 5:26;;Malicious-URL;;msqym.com;;;
 11.6.2017 5:31;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 5:45;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@ROADHOUSE.it;14.186.73.4;;;
 11.6.2017 6:12;;Malicious-URL;Malicious-URL;;herbalabsassist.ru;qbirorgwl@gmail.com;46.4.76.104;;;
 11.6.2017 6:15;;Malicious-URL;Malicious-URL;;herbalabsassist.ru;lgzxbmva@Oenergylighting.com;14.109.117.146;;;
 11.6.2017 6:27;;Malicious-URL;Malicious-URL;;macartu.cn;udhlf@hmsinet.ca;112.140.187.82;;;
 11.6.2017 6:31;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 7:05;;Malicious-URL;Malicious-URL;;familierabatnordic.dk;;;
 11.6.2017 7:22;;Malicious-URL;Malicious-URL;;dealydo.com;;;
 11.6.2017 8:16;;Malicious-URL;Malicious-URL;;macartu.cn;orhggvqde@soundscapes.us;119.61.13.242;;;
 11.6.2017 8:48;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;alert@freewheelinbiketours.com;212.90.174.166;;;
 11.6.2017 8:53;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;;;
 11.6.2017 8:57;;Malicious-URL;Malicious-URL;;macartu.cn;apojclhd@hmx.de;153.0.163.18;;;
 11.6.2017 9:27;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@barcelona-audio-guide.com;128.199.219.127;;;
 11.6.2017 9:44;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@verticalgreenpanel.com;176.227.172.72;;;
 11.6.2017 9:47;;Malicious-URL;Malicious-URL;;medicalrxquality.su;pending+78btpm58wsv@aventurescoquines.com;158.255.102.155;;;
 11.6.2017 9:51;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@drivingeasy.com;211.39.130.33;;;
 11.6.2017 10:07;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 10:12;;Malicious-URL;Malicious-URL;;macartu.cn;bosdgaht@hmv.at;49.140.162.133;;;
 11.6.2017 10:14;8f50ec2539e04018eb2727812a87c4e1;JS_NEMU.B2B35B1C;Malware;Malware;5947358765087.zip;villessot.michel@csloxinfo.net;58.136.168.50;;;
 11.6.2017 10:14;a2f2ae03e4280c6cd312970cea40e94;JS_NEMU.B2B35B1C;Malware;Malware;10091.zip;villessot.michel@csloxinfo.net;58.136.168.50;;;
 11.6.2017 10:56;;Malicious-URL;Malicious-URL;;macartu.cn;anbdqapu@hmsinet.com.au;213.32.63.81;;;
 11.6.2017 11:07;;Malicious-URL;Malicious-URL;;familierabatnordic.dk;;;
 11.6.2017 11:10;;Malicious-URL;Malicious-URL;;scandigogo.com;;;
 11.6.2017 11:24;;Malicious-URL;Malicious-URL;;medicemail.com;;;
 11.6.2017 11:29;;Malicious-URL;Malicious-URL;;herbalabsassist.ru;modxbdit@1126.com;113.121.41.140;;;
 11.6.2017 11:30;;Malicious-URL;Malicious-URL;;herbalabsassist.ru;onsuiczn@11400inc.com;182.91.27.110;;;
 11.6.2017 11:30;;Malicious-URL;Malicious-URL;;herbalabsassist.ru;roxvcyngn@113.com;113.121.41.140;;;
 11.6.2017 11:39;;Malicious-URL;Malicious-URL;;medicalrxquality.su;notification+kttwg6ct0nuz@industrycleaningsystems.com;68.168.96.103;;;
 11.6.2017 11:44;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;notification+8j2uf6p7fi4y@absorbing-modernity.com;91.236.73.195;;;
 11.6.2017 12:18;;Malicious-URL;;xujing@16ds.com;117.79.81.101;;;
 11.6.2017 12:36;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 12:59;;Malicious-URL;Malicious-URL;;macartu.cn;lulpin@hmsinet.ca;213.222.246.78;;;
 11.6.2017 13:07;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 13:08;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 14:37;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@RANCID.pl;113.174.12.193;;;
 11.6.2017 14:49;;Malicious-URL;Malicious-URL;;dock.email;kampanja@slowcolor.info;185.99.122.103;;;
 11.6.2017 15:01;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 15:04;;Malicious-URL;;extraordines.com;;;
 11.6.2017 15:04;;Malicious-URL;;extraordines.com;;;
 11.6.2017 15:30;;Malicious-URL;Malicious-URL;;macartu.cn;buufgzeg@smartcity.us;104.218.124.115;;;
 11.6.2017 16:03;;Malicious-URL;;fneseo.org;;;
 11.6.2017 16:10;;Malicious-URL;Malicious-URL;;macartu.cn;ppeml@hmsecurityservices.co.uk;5.135.195.166;;;
 11.6.2017 16:12;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@NARY.co.uk;123.24.80.118;;;
 11.6.2017 16:12;;Malicious-URL;Malicious-URL;;softwarevisit.org;info@saresh.org;118.107.180.233;;;
 11.6.2017 16:21;;Malicious-URL;Malicious-URL;;macartu.cn;wjoatjra@hmsfabrics.com;67.79.124.198;;;
 11.6.2017 17:04;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 17:11;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 17:15;;Malicious-URL;Malicious-URL;;jsly-tea.com;;;
 11.6.2017 17:46;;Malicious-URL;Malicious-URL;;macartu.cn;joeatxv@richardahallpc.us;120.234.15.130;;;
 11.6.2017 17:46;;Malicious-URL;Malicious-URL;;macartu.cn;opcvitmn@purpleamerica.us;120.234.15.130;;;
 11.6.2017 17:59;;Malicious-URL;;rayanventures.com;;;
 11.6.2017 18:13;;Malicious-URL;;hxxp://lesovichok96.ru/administrator/components/com_menus/views/menutypes/tmpl/sitemap.html;riadionwd@kurumpadamtamil.com;118.174.19.29;;;
 11.6.2017 18:17;;Malicious-URL;;vikusha.86@qip.ru;123.120.70.219;;;
 11.6.2017 18:24;;Malicious-URL;;sem-store.com;;;
 11.6.2017 18:27;;Malicious-URL;;bounce@slimdrops.de;198.1.66.239;;;
 11.6.2017 18:32;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 11.6.2017 18:58;;Malicious-URL;Malicious-URL;;macartu.cn;wmmaa@hmshost.com.au;91.134.233.249;;;
 11.6.2017 18:58;;Malicious-URL;Malicious-URL;;macartu.cn;xrlqbsfice@hmsinet.ca;91.134.233.249;;;
 11.6.2017 19:07;;Malicious-URL;Malicious-URL;;iloasterio.com;admin@bevespa.cf;94.177.204.22;;;
 11.6.2017 19:09;3c0d0aa2e06abb56a8ae0c8fb9655b8f;JS_NEMU.B2B35B1C;Malware;Malware;18104.zip;info@cygate.fi;117.255.209.207;;;
 11.6.2017 19:09;a6db49af4651542ec06b48bea75e1f63;JS_NEMU.B2B35B1C;Malware;Malware;6922136.zip;info@cygate.fi;117.255.209.207;;;
 11.6.2017 19:09;;Malicious-URL;;spygrit.com;;;
 11.6.2017 19:49;;Malicious-URL;Malicious-URL;;macartu.cn;oyrzbccn@hmsinet.com.au;51.254.215.0;;

11.6.2017 20:00;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@1stopink.com;82.165.150.155;;
11.6.2017 20:08;;Malicious-URL;Malicious-URL;;macartu.cn;ouzirkuqzg@hmsmakina.com.tr;80.249.187.178;;
11.6.2017 20:49;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@hbfangyuanj.com;221.132.35.150;;
11.6.2017 21:17;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@IMPROVISATION.it;187.63.198.202;;
11.6.2017 21:19;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@WHEREUPON.fr;194.213.23.103;;
11.6.2017 21:20;;Malicious-URL;Malicious-URL;;macartu.cn;pyptjae@hmsinet.ca;181.49.171.178;;
11.6.2017 21:21;;Malicious-URL;Malicious-URL;;macartu.cn;gioknazsw@airhart.us;122.4.254.54;;
11.6.2017 21:22;;Malicious-URL;Malicious-URL;;macartu.cn;bbtudyqlqnooa@laminar.us;122.4.254.54;;
11.6.2017 21:23;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@OSTEOPATHIC.br;187.84.41.98;;
11.6.2017 21:28;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@webmdhealthexchange.com;45.64.1.113;;
11.6.2017 21:29;;Malicious-URL;Malicious-URL;;macartu.cn;ggpfkmobesh@hmsinet.ca;89.175.148.162;;
11.6.2017 21:35;;Malicious-URL;Malicious-URL;;macartu.cn;xdgerzcgiv@hmshost.com.au;119.84.15.210;;
11.6.2017 21:39;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@WHEREUPON.nl;113.166.35.145;;
11.6.2017 21:53;;Malicious-URL;Malicious-URL;;macartu.cn;onuzzg@hmshost.com.au;80.249.187.178;;
11.6.2017 21:53;;Malicious-URL;Malicious-URL;;organictabletinc.ru;update+5e7k36166a7p@thefilmcompanies.com;64.111.100.50;;
11.6.2017 22:00;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@scifitrader.com;178.20.155.246;;
11.6.2017 22:04;;Malicious-URL;Malicious-URL;;organictabletinc.ru;pending+89sz8rv2hy2k@boostaz.com;217.160.236.161;;
11.6.2017 22:06;;Malicious-URL;;055017.com;;
11.6.2017 22:11;;Malicious-URL;Malicious-URL;;masterlead.info;;
11.6.2017 22:21;;Malicious-URL;Malicious-URL;;organictabletinc.ru;pending+3jwjys11e0i4@hostful.com;31.210.60.250;;
11.6.2017 22:29;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@chakrahairstudio.com;103.215.136.16;;
11.6.2017 22:36;3f136f5c9f8744226f010589653321;JS_NEMU.B2B35B1C;Malware;Malware;25477.zip;ropa.fgbxdbp@cygate.fi;115.84.93.218;;
11.6.2017 22:36;e725365c2e360db21f939aaea7472868;JS_NEMU.B2B35B1C;Malware;Malware;78354211197.zip;ropa.fgbxdbp@cygate.fi;115.84.93.218;;
11.6.2017 22:37;;Malicious-URL;;viralidaze.com;;
11.6.2017 22:38;;Malicious-URL;Malicious-URL;;itstrcks.ltd;sober97@sohu.com;222.131.118.25;;
11.6.2017 22:41;;Malicious-URL;;viralidaze.com;;
11.6.2017 22:42;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;pending+jnrtod9o6rye@midwestservicebureau.com;92.185.49.210;;
11.6.2017 22:42;;Malicious-URL;Malicious-URL;;itstrcks.ltd;;
11.6.2017 22:52;;Malicious-URL;Malicious-URL;;whsx.cn;hr@boosen.com;218.240.43.184;;
11.6.2017 23:55;;Malicious-URL;;okedmvrtime@schage.de;177.241.38.143;;
11.6.2017 23:56;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@senhoraneis.com;122.160.113.225;;
12.6.2017 0:05;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;
12.6.2017 0:06;;Malicious-URL;Malicious-URL;;organictabletinc.ru;support+b5djwdfwsowtc@kerrysbodywrapsandmore.com;109.104.93.252;;
12.6.2017 0:15;;Malicious-URL;Malicious-URL;;macartu.cn;babbrcwvbd@hmshost.com.au;180.210.201.55;;
12.6.2017 0:19;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@acharmingparty.com;38.96.175.221;;
12.6.2017 0:22;;Malicious-URL;Malicious-URL;;organictabletinc.ru;pending+4brn91esm765@makinarya.com;45.55.161.179;;
12.6.2017 0:34;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;
12.6.2017 0:49;;Malicious-URL;;swfwz@static.vnpt-hanoi.com.vn;113.190.238.57;;
12.6.2017 0:53;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;
12.6.2017 1:05;;Malicious-URL;Malicious-URL;;tbwjlx.com;xujing@16ds.com;117.79.81.101;;
12.6.2017 1:07;;Malicious-URL;Malicious-URL;;serp-boost.com;fadecice330@gmail.com;221.160.34.117;;
12.6.2017 1:15;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@patriciavegarealty.com;47.44.11.156;;
12.6.2017 1:16;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@silverthornenews.com;185.12.110.132;;
12.6.2017 1:18;;Malicious-URL;Malicious-URL;;medicalrxquality.su;support+qev838fax5bz@ecoledeemediationculturelle.com;223.27.22.112;;
12.6.2017 1:18;;Malicious-URL;Malicious-URL;;medicalrxquality.su;update+mmhhz5831fp@fastbracesvancouver.com;193.194.80.101;;
12.6.2017 1:19;;Malicious-URL;Malicious-URL;;basedbusinesstraffic.com;golasage265@gmail.com;180.178.44.250;;
12.6.2017 1:21;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;
12.6.2017 1:43;;Malicious-URL;Malicious-URL;;macartu.cn;iphpmb@hmstn.com;192.129.236.172;;
12.6.2017 1:43;;Malicious-URL;Malicious-URL;;macartu.cn;okntzsgoj@hmsoldies.org.uk;192.129.236.172;;
12.6.2017 1:45;;Malicious-URL;Malicious-URL;;organictabletinc.ru;pending+ibt5iokme71@7338000.com;87.106.241.93;;
12.6.2017 1:52;;Malicious-URL;Malicious-URL;;macartu.cn;cyvzrme@hmsinet.ca;178.32.130.80;;
12.6.2017 2:17;;Malicious-URL;;dealydid.com;;
12.6.2017 2:20;cd81aa2e305a2212e51c429ccfa42b05;JS_NEMU.B2B35B1C;Malware;Malware;9924036.zip;sales@vnpt-hanoi.com.vn;113.190.254.86;;
12.6.2017 2:20;e890ab3e05ae6cbe7ce8c9daafc300ea;JS_NEMU.B2B35B1C;Malware;Malware;29196.zip;sales@vnpt-hanoi.com.vn;113.190.254.86;;
12.6.2017 2:22;;Malicious-URL;;vrganji.com.cn;;
12.6.2017 2:23;;Malicious-URL;Malicious-URL;Malicious-URL;;amino-disqus.club;;
12.6.2017 2:41;;Malicious-URL;;hxxp://www.perf1climited.com/wp-content/themes/twentyxixteen/8328b22318b.html;postmaster@s16960577.onlinehome-server.info;87.106.24.123;;
12.6.2017 2:52;;Malicious-URL;;nrockwell@rockinfo.com.au;116.96.28.137;;
12.6.2017 2:53;;Malicious-URL;;info@ds.emailsent2u.com;109.167.22.191;;
12.6.2017 3:34;952c0bc8a46d51ce385deba65f3e6cf;JS_NEMU.B2B35B1C;Malware;Malware;2028.js;jmk372@cygate.fi;188.19.41.127;;
12.6.2017 3:34;983e200a51f3d16dca9f14afcf903e;JS_NEMU.B2B35B1C;Malware;Malware;2028.zip;jmk372@cygate.fi;188.19.41.127;;
12.6.2017 3:34;ee894bc33cc86d00071d3113d6fba462;JS_NEMU.B2B35B1C;Malware;Malware;506557084495898.zip;jmk372@cygate.fi;188.19.41.127;;
12.6.2017 4:12;;Malicious-URL;Malicious-URL;;smartrxshop.su;;
12.6.2017 4:25;;Malicious-URL;Malicious-URL;;macartu.cn;zkigsgueik@hna.ch;115.231.16.175;;
12.6.2017 4:26;;Malicious-URL;Malicious-URL;;smartrxshop.su;;
12.6.2017 4:49;;Malicious-URL;Malicious-URL;;xurl.es;kempbells@bk.ru;104.219.251.135;;
12.6.2017 4:52;;Malicious-URL;Malicious-URL;;macartu.cn;fvmybea@hmshost.com;50.199.157.91;;
12.6.2017 4:56;0dd344ea0a1312bcfee767225cc26e6;JS_NEMU.B2B35B1C;Malware;Malware;11514.zip;rmcginnis@zaural.ru;31.163.170.22;;
12.6.2017 4:56;531f117913e2286fa9a0cb911767486a;JS_NEMU.B2B35B1C;Malware;Malware;03267576987501.zip;rmcginnis@zaural.ru;31.163.170.22;;
12.6.2017 5:31;;Malicious-URL;Malicious-URL;;smartrxshop.su;ausleherb@mucola.de;138.0.190.158;;
12.6.2017 5:33;;Malicious-URL;Malicious-URL;;smartrxshop.su;schenmler@tohit.de;123.28.27.37;;
12.6.2017 5:40;;Malicious-URL;Malicious-URL;;smartrxshop.su;gett@excite.it;112.72.86.116;;
12.6.2017 5:45;;Malicious-URL;Malicious-URL;;smartrxshop.su;c215cb2b@nutrivie.ch;14.176.152.244;;
12.6.2017 5:49;;Malicious-URL;;ceaxu@static.vnpt.vn;14.186.132.35;;
12.6.2017 5:51;;Malicious-URL;Malicious-URL;;smartrxshop.su;mail@braunmarc.de;197.2.17.25;;
12.6.2017 5:54;;Malicious-URL;Malicious-URL;;smartrxshop.su;noplkf318c2u1@uni-berlin.de;197.129.179.202;;
12.6.2017 6:09;;Malicious-URL;Malicious-URL;;smartrxshop.su;ebay@priz24.de;171.234.47.94;;
12.6.2017 6:12;;Malicious-URL;Malicious-URL;;macartu.cn;askstao@hmshost.com;51.255.38.52;;
12.6.2017 6:14;;Malicious-URL;Malicious-URL;;smartrxshop.su;jodizedturns@abdsb.bayern.de;42.112.144.100;;
12.6.2017 6:21;;Malicious-URL;Malicious-URL;;smartrxshop.su;donamac@world.net;154.243.20.73;;
12.6.2017 6:34;;Malicious-URL;Malicious-URL;;smartrxshop.su;fertigung@straschu-ie.de;117.5.128.68;;
12.6.2017 6:36;;Malicious-URL;Malicious-URL;;onlinesmartsale.com;kepsu@akis.at;213.222.246.78;;
12.6.2017 6:40;;Malicious-URL;Malicious-URL;;onlinesmartsale.com;dyveaocm@akis.at;91.134.203.125;;
12.6.2017 6:43;;Malicious-URL;Malicious-URL;;blackhatseos.com;kingarr459@gmail.com;112.121.181.66;;
12.6.2017 6:53;;Malicious-URL;Malicious-URL;;rxaqov.top;vgpzcj8729@mail13.chanceofcheap.vip;108.171.246.38;;
12.6.2017 7:21;;Malicious-URL;Malicious-URL;;dealydo.com;;
12.6.2017 8:07;;Malicious-URL;Malicious-URL;;negativeseos.agency;pedugju5@gmail.com;112.121.187.170;;
12.6.2017 8:32;;Malicious-URL;Malicious-URL;;smartrxshop.su;dmpslh@expressfind.com;14.186.236.153;;
12.6.2017 8:34;;Malicious-URL;Malicious-URL;;express-catalogs.com;;
12.6.2017 8:35;;Malicious-URL;Malicious-URL;;express-catalogs.com;messages@fiflirts.agency;185.132.51.66;;
12.6.2017 8:51;;Malicious-URL;Malicious-URL;;express-catalogs.com;;
12.6.2017 8:57;;Malicious-URL;Malicious-URL;;smartrxshop.su;n00827091@netplay-news.de;77.31.233.212;;
12.6.2017 8:59;;Malicious-URL;;messages@fiflirts.agency;185.132.51.61;;
12.6.2017 9:00;;Malicious-URL;Malicious-URL;;express-catalogs.com;;
12.6.2017 9:22;;Malicious-URL;;info@ds.emailsent2u.com;109.167.22.193;;
12.6.2017 9:24;;Malicious-URL;Malicious-URL;;express-catalogs.com;;
12.6.2017 9:25;;Malicious-URL;Malicious-URL;;express-catalogs.com;;

12.6.2017 9:25;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 9:31;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 9:50;;Malicious-URL;Malicious-URL;;smartrxshop.su;contact@ebert-jacobi.de;116.111.134.53;;
 12.6.2017 9:51;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 9:51;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 10:04;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 10:29;;Malicious-URL;Malicious-URL;;smartrxshop.su;neue-medien@listserv.tu-bs.de;179.41.166.82;;
 12.6.2017 10:30;;Malicious-URL;;pandawintoday.com;;;
 12.6.2017 10:31;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 10:34;;Malicious-URL;Malicious-URL;;smartrxshop.su;andrelevert@quante-netzwerke.de;122.165.109.60;;
 12.6.2017 10:34;;Malicious-URL;;gexinmeng@shanghaihida.com;222.73.105.170;;
 12.6.2017 10:37;;Malicious-URL;Malicious-URL;;macartu.cn;vojxvamp@hmvllp.com;94.20.21.38;;
 12.6.2017 10:37;;Malicious-URL;Malicious-URL;;macartu.cn;vyxiwuyloc@hmveng.com;94.20.21.38;;
 12.6.2017 10:39;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@givefarm.com;37.59.79.246;;
 12.6.2017 10:39;;Malicious-URL;Malicious-URL;;smartrxshop.su;dieter.sengstock@vsr-consult.de;123.24.209.187;;
 12.6.2017 10:40;;Malicious-URL;;info@trendhim.fi;23.253.183.136;;
 12.6.2017 10:44;;Malicious-URL;Malicious-URL;;smartrxshop.su;agnetaeduff@eac-consulting.de;14.177.14.214;;
 12.6.2017 10:45;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 10:54;;Malicious-URL;Malicious-URL;;smartrxshop.su;j.h.dortmundd@freesulf.de;1.52.125.253;;
 12.6.2017 11:00;;Malicious-URL;Malicious-URL;;organictabletinc.ru;notification+y14wafus1qaf@lincaicraft.com;212.227.251.179;;
 12.6.2017 11:10;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@watchthese.com;188.165.199.98;;
 12.6.2017 11:10;;Malicious-URL;Malicious-URL;;smartrxshop.su;chahles@orangemail.ch;1.20.133.205;;
 12.6.2017 11:12;;Malicious-URL;;lfcopellegrino.com;;;
 12.6.2017 11:14;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@orange-county-drug-rehab.com;109.238.11.32;;
 12.6.2017 11:14;;Malicious-URL;Malicious-URL;;smartrxshop.su;leopold.beck@surdeu.de;116.108.196.111;;
 12.6.2017 11:21;;Malicious-URL;Malicious-URL;;medicemail.com;;;
 12.6.2017 11:23;;Malicious-URL;Malicious-URL;;smartrxshop.su;dkjan@luk.de;123.24.106.93;;
 12.6.2017 11:33;;Malicious-URL;Malicious-URL;;smartrxshop.su;urba@bg-rams.ac.at;123.30.38.90;;
 12.6.2017 11:41;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 11:48;;Malicious-URL;;maurids@snued.com;195.140.195.194;;
 12.6.2017 11:50;66614c34ff93519f4bf2e7e68f5e4c4;JS_NEMU.B2B35B1C;Malware;;Malware;17148.zip;;m.verhart@cygate.fi;46.250.86.101;;
 12.6.2017 11:50;72057378a6ea153a8d6fea65e9f0e491;JS_NEMU.B2B35B1C;Malware;;Malware;968374248767.zip;;m.verhart@cygate.fi;46.250.86.101;;
 12.6.2017 11:50;75a60e87b1ae0ee6248623f7a97bbe71;JS_NEMU.B2B35B1C;Malware;;Malware;17148.js;;m.verhart@cygate.fi;46.250.86.101;;
 12.6.2017 11:51;;Malicious-URL;;jannet@hadongtoyota.com;195.140.195.194;;
 12.6.2017 12:04;;Malicious-URL;;elabs13.com;;;
 12.6.2017 12:19;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;pending+hwjn2973pvig@buysellhomesbrowardcountyfl.com;162.144.65.65;;
 12.6.2017 12:21;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 12:25;;Malicious-URL;;mercedez@intelisell.com;147.135.204.185;;
 12.6.2017 12:27;;Malicious-URL;;marketing@sw.solarwinds.com;199.15.214.42;;
 12.6.2017 12:29;;Malicious-URL;;marketing@sw.solarwinds.com;199.15.214.42;;
 12.6.2017 12:31;;Malicious-URL;;bcontactsc.com;;;
 12.6.2017 12:32;;Malicious-URL;;marketing@sw.solarwinds.com;199.15.214.42;;
 12.6.2017 12:34;;Malicious-URL;;marketing@sw.solarwinds.com;199.15.214.42;;
 12.6.2017 12:55;;Malicious-URL;Malicious-URL;;macartu.cn;zghybkre@hmsoldies.org.uk;153.0.163.18;;
 12.6.2017 12:56;;Malicious-URL;Malicious-URL;;macartu.cn;116503171126331.QO45212@vkyw.hmstn.com;153.0.163.18;;
 12.6.2017 13:10;831bdc0cf9f784df3c715ea8cae69685;JS_NEMU.B2B35B1C;Malware;;Malware;5201.zip;;lilbird@cygate.fi;37.79.188.226;;
 12.6.2017 13:10;c6eb9cf8b7ffa0825902b5e9fe5dd258;JS_NEMU.B2B35B1C;Malware;;Malware;5201.js;;lilbird@cygate.fi;37.79.188.226;;
 12.6.2017 13:10;ca1dd4d32d52734fb9ecda1a246f9b54;JS_NEMU.B2B35B1C;Malware;;Malware;795943906.zip;;lilbird@cygate.fi;37.79.188.226;;
 12.6.2017 13:16;;Malicious-URL;Malicious-URL;;smartrxshop.su;redmond@verwaltung.uni-marburg.de;93.152.141.211;;
 12.6.2017 13:22;;Malicious-URL;;domainmancer.org;;;
 12.6.2017 13:37;8dd32c13ec5e1d1491eb884bdc500ef9;JS_NEMU.B2B35B1C;Malware;;Malware;12203.zip;;paul@hinet.net;111.253.6.159;;
 12.6.2017 13:37;95cbb92043e0c22d6c5830f2154c7b0b;JS_NEMU.B2B35B1C;Malware;;Malware;7350342761395.zip;;paul@hinet.net;111.253.6.159;;
 12.6.2017 13:43;;Malicious-URL;Malicious-URL;;smartrxshop.su;adsiegerutia@bense.de;60.254.7.186;;
 12.6.2017 13:44;;Malicious-URL;Malicious-URL;;macartu.cn;ibkupzi@hmt-electric.com;159.203.164.107;;
 12.6.2017 13:46;;Malicious-URL;;alexa-packages.com;;;
 12.6.2017 13:56;;Malicious-URL;Malicious-URL;;iclicks.space;erot@srv.hotaduldate.com;207.154.249.66;;
 12.6.2017 14:11;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 14:15;;Malicious-URL;;bcontactsc.com;;;
 12.6.2017 14:29;;Malicious-URL;;bcontactsc.com;;;
 12.6.2017 14:31;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 14:43;c233552e5c56e59150dff2a854649993;JS_NEMU.B2B35B1C;Malware;;Malware;1624.zip;;web@cygate.fi;168.194.82.174;;
 12.6.2017 14:43;d4e26b5218648f3f0c7c9179af9c38;JS_NEMU.B2B35B1C;Malware;;Malware;7539006.zip;;web@cygate.fi;168.194.82.174;;
 12.6.2017 14:45;;Malicious-URL;Malicious-URL;;dealydo.com;;;
 12.6.2017 14:49;;Malicious-URL;Malicious-URL;;express-catalogs.com;;lorriane@homeei.com;147.135.207.234;;
 12.6.2017 15:06;;Malicious-URL;Malicious-URL;;medicemail.com;;;
 12.6.2017 15:08;234866d3a64e6c5ec577f3ee2855ead2;JS_NEMU.B2B35B1C;Malware;;Malware;13850.zip;;bonomo.g@cygate.fi;31.163.31.89;;
 12.6.2017 15:08;26d50d13e0412d5644128c3971dffe;JS_NEMU.B2B35B1C;Malware;;Malware;2918904231.zip;;bonomo.g@cygate.fi;31.163.31.89;;
 12.6.2017 15:08;c6eb9cf8b7ffa0825902b5e9fe5dd258;JS_NEMU.B2B35B1C;Malware;;Malware;13850.js;;bonomo.g@cygate.fi;31.163.31.89;;
 12.6.2017 15:08;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 15:29;;Malicious-URL;;bcontactsc.com;;;
 12.6.2017 15:31;;Malicious-URL;;extraordines.com;;;
 12.6.2017 15:31;;Malicious-URL;;outletype.com;;;
 12.6.2017 15:39;;Malicious-URL;;bcontactsc.com;;;
 12.6.2017 15:58;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 16:00;;Malicious-URL;Malicious-URL;;amino-disqus.club;;;
 12.6.2017 16:02;1571677c5c56ff33a6ee8211513e7b76;JS_NEMU.B2B35B1C;Malware;;Malware;23801.zip;;timo-mueller@cygate.fi;117.244.24.212;;
 12.6.2017 16:02;79cc326b39c312feba2fd1b5e34cad9e;JS_NEMU.B2B35B1C;Malware;;Malware;46871282.zip;;timo-mueller@cygate.fi;117.244.24.212;;
 12.6.2017 16:09;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 16:29;;Malicious-URL;Malware;;BL;sales1@qq.com;;;
 12.6.2017 16:38;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@fortlauderdaleuidefenslawyer.com;162.214.1.51;;
 12.6.2017 16:39;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
 12.6.2017 16:41;;Malicious-URL;;coloramani.com;;;
 12.6.2017 17:08;;Malicious-URL;Malicious-URL;;organictabletinc.ru;support+brmfaa0yfgp0@bayoudat.com;212.224.70.26;;
 12.6.2017 17:16;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@cityofboardman.com;87.106.104.80;;
 12.6.2017 17:41;;Malicious-URL;Malicious-URL;;medicemail.com;;;
 12.6.2017 17:45;;Malicious-URL;Malicious-URL;;medicalrxquality.su;update+y6uy43x5x9@vitoshaexpress.com;104.156.226.176;;
 12.6.2017 17:48;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@theamericandj.com;62.149.141.85;;
 12.6.2017 17:52;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@cuddelecooks.com;128.127.66.91;;
 12.6.2017 17:52;;Malicious-URL;Malicious-URL;;medicalrxquality.su;notification+8ks4fhqkb6s@cheddarspizzeria.com;103.22.180.250;;
 12.6.2017 17:55;;Malicious-URL;Malicious-URL;;macartu.cn;qyawdba@hmsinet.ca;59.37.22.82;;
 12.6.2017 18:06;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@freshlooksalon.com;82.223.107.61;;
 12.6.2017 18:07;;Malicious-URL;Malicious-URL;;macartu.cn;whvfpdpo@hmshost.com.au;185.73.114.126;;
 12.6.2017 18:11;;Malicious-URL;Malicious-URL;;organictabletinc.ru;notification+keh5capx4bm7@hilfe-bei-sodsbrennen.com;103.52.146.66;;
 12.6.2017 18:14;;Malicious-URL;;mtgros.net;;;
 12.6.2017 18:18;;Malicious-URL;;bounce@slimdrops.de;198.1.66.239;;
 12.6.2017 18:31;;Malicious-URL;Malicious-URL;;macartu.cn;mbooe@hmsmakina.com.tr;89.175.148.162;;
 12.6.2017 18:36;;Malicious-URL;;hxxp://MYSAFERETIREMENT.COM/file.php?document=am9ha21tLnJvZWhyQGN5Z2F0Z55maQ==;william_scott@flexoviportal.com;12.207.181.251;;

12.6.2017 18:52;;;Malicious-URL;Malicious-URL;;hxxp://digitalactionist.com/file.php?document=anVoY5S0b2l2b25lkbJewDhdGUuZmk=;william_scott@flexovitportal.com;24.158.246.22;;

12.6.2017 19:00;;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@skaring.com;223.27.22.112;;

12.6.2017 19:02;;;Malicious-URL;Malicious-URL;;hxxp://digitalactionist.com/file.php?document=cGF1bGUCGFr2FuZW5AY3lnYXRlMzpw;william_scott@flexovitportal.com;96.94.105.41;;

12.6.2017 19:08;;;Malicious-URL;Malicious-URL;;hxxp://digitalactionist.com/file.php?document=YW50dGkuamFhc2ltbGZlbnVudG9NS2ZlZ0Z5SmaQ=;william_scott@flexovitportal.com;98.90.42.145;;

12.6.2017 19:11;;;Malicious-URL;;hxxp://MYSAFERRETIREMENT.COM/file.php?document=YXJpLmhvbG9wYWluZW5AY3lnYXRlMzpw;william_scott@flexovitportal.com;69.75.85.114;;

12.6.2017 19:16;;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@hqueen.com;82.220.34.146;;

12.6.2017 19:16;;;Malicious-URL;Malicious-URL;;hxxp://UN-TIREMENT.COM/file.php?document=cHVyY2hhc2VAY3lnYXRlMzpw;william_scott@flexovitportal.com;184.0.79.231;;

12.6.2017 19:25;;;Malicious-URL;Malicious-URL;;macartu.cn;etjdrqewxw@hmsinet.ca;173.212.203.168;;

12.6.2017 19:26;;;Malicious-URL;Malicious-URL;;macartu.cn;vcxro@hmshost.com.au;47.90.4.23;;

12.6.2017 19:28;;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@xn-trigueus-i3a.com;103.18.45.23;;

12.6.2017 19:35;;;Malicious-URL;Malicious-URL;;hxxp://digitalactionist.com/file.php?document=dmlsbGUubHVvdG9AY3lnYXRlMzpw;william_scott@flexovitportal.com;184.0.79.231;;

12.6.2017 19:37;;;Malicious-URL;;hxxp://ASAFERRETIREMENT.COM/file.php?document=am9ha2ltLjVzWhYQGN5Z2F0Z5SmaQ=;william_scott@flexovitportal.com;96.33.148.40;;

12.6.2017 19:39;;;Malicious-URL;;hxxp://ankitbiyani.com/file.php?document=cGFzaS5tYWtpbmVudG9NS2ZlZ0Z5SmaQ=;william_scott@flexovitportal.com;199.68.233.78;;

12.6.2017 19:42;;;Malicious-URL;;hxxp://ASAFERRETIREMENT.COM/file.php?document=c2FtdS52aXJ0YW1vQGN5Z2F0Z5SmaQ=;william_scott@flexovitportal.com;86.143.157.160;;

12.6.2017 19:47;;;Malicious-URL;;hxxp://MYSAFERRETIREMENT.COM/file.php?document=cGVra2Euc29sZWhwYWluZW5AY3lnYXRlMzpw;william_scott@flexovitportal.com;50.197.222.33;;

12.6.2017 19:55;;;Malicious-URL;;hxxp://ankitbiyani.com/file.php?document=ZW5zdGkuaz2VudGF5YUBjeWdhGUuZmk=;william_scott@flexovitportal.com;40.134.184.79;;

12.6.2017 20:00;;;Malicious-URL;;hxxp://ASAFERRETIREMENT.COM/file.php?document=YW50ZS50ZW5AY3lnYXRlMzpw;william_scott@flexovitportal.com;72.73.109.226;;

12.6.2017 20:14;;;Malicious-URL;Malicious-URL;;hxxp://UN-TIREMENT.COM/file.php?document=ZWV2YS52aWh2b2hOGN5Z2F0Z5SmaQ=;william_scott@flexovitportal.com;137.119.110.227;;

12.6.2017 20:15;;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@sophiasthaicuisineparadise.com;103.57.222.10;;

12.6.2017 20:18;;;Malicious-URL;;hxxp://MYSAFERRETIREMENT.COM/file.php?document=cGFzaS5tYWtpbmVudG9NS2ZlZ0Z5SmaQ=;william_scott@flexovitportal.com;216.81.115.48;;

12.6.2017 20:21;;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;pending+5q4dsjj1mp88@macrodegeneration.com;212.117.124.19;;

12.6.2017 20:22;;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@queenslandbeachhotels.com;112.137.162.102;;

12.6.2017 20:24;;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;notification-rv3e7wq5et@intersecao.com;198.211.31.12;;

12.6.2017 20:24;;;Malicious-URL;;coloramani.com;;

12.6.2017 20:24;;;Malicious-URL;Malicious-URL;;organictabletinc.ru;;

12.6.2017 20:24;;;Malicious-URL;;update+yv1dv3xkpb9@ihpsystem.com;103.6.196.122;;

12.6.2017 20:39;;;Malicious-URL;;hxxp://ankitbiyani.com/file.php?document=c2FrdS5va3NhbWVudG9NS2ZlZ0Z5SmaQ=;william_scott@flexovitportal.com;73.152.221.169;;

12.6.2017 20:43;;;Malicious-URL;;rsxuba@static.vnpt.vn;14.177.220.129;;

12.6.2017 20:49;;;Malicious-URL;;anrrkky@static.vnpt.vn;14.186.200.69;;

12.6.2017 20:51;;;Malicious-URL;;rbsuxa.com;;

12.6.2017 20:52;;;Malicious-URL;Malicious-URL;;organictabletinc.ru;support+hfnfdtmb087f@lavillat.com;209.54.52.85;;

12.6.2017 20:55;;;Malicious-URL;Malicious-URL;;hxxp://UN-TIREMENT.COM/file.php?document=amFya2tVlnJpdmlub2phQGN5Z2F0Z5SmaQ=;william_scott@flexovitportal.com;70.44.211.162;;

12.6.2017 21:06;;;Malicious-URL;Malicious-URL;;onlinesmartsale.com;omsqydidgc@heijmans.nl;42.81.36.152;;

12.6.2017 21:08;;;Malicious-URL;Malicious-URL;;macartu.cn;246886380532846.AJ60624@umqe.hmshost.com.au;47.90.4.23;;

12.6.2017 21:08;;;Malicious-URL;Malicious-URL;;macartu.cn;647853604707204.ONO2351@oea.hmshost.com;47.89.208.49;;

12.6.2017 21:11;;;Malicious-URL;Malicious-URL;;hxxp://digitalactionist.com/file.php?document=dG9taS5yYWV0dGluZW5AY3lnYXRlMzpw;william_scott@flexovitportal.com;69.131.250.54;;

12.6.2017 21:29;;;Malicious-URL;Malicious-URL;;hxxp://EXPLORIST.IN/file.php?document=bWfya3VzLmt1aXZhbGZlbnVudG9NS2ZlZ0Z5SmaQ=;william_scott@flexovitportal.com;50.82.234.231;;

12.6.2017 21:33;;;Malicious-URL;Malicious-URL;;hxxp://digitalactionist.com/file.php?document=bm9va2Uua29uc3RpZ0JjeWdhGUuZmk=;william_scott@flexovitportal.com;192.67.88.5;;

12.6.2017 21:42;;;Malicious-URL;Malicious-URL;;hxxp://UN-TIREMENT.COM/file.php?document=dG9taS5yYXJsc3NvbkJjeWdhGUuZmk=;william_scott@flexovitportal.com;73.111.141.187;;

12.6.2017 21:45;;;Malicious-URL;Malicious-URL;;hxxp://MYSAFERRETIREMENT.COM/file.php?document=ZW5zdGkuaz2VudGF5YUBjeWdhGUuZmk=;william_scott@flexovitportal.com;208.201.235.130;;

12.6.2017 21:53;;;Malicious-URL;Malicious-URL;;hxxp://EXPLORIST.IN/file.php?document=amFya2tVlnJpdmlub2phQGN5Z2F0Z5SmaQ=;william_scott@flexovitportal.com;24.182.213.253;;

12.6.2017 21:56;;;Malicious-URL;;coloramani.com;;

12.6.2017 21:58;;;Malicious-URL;;coloramani.com;;

12.6.2017 22:08;;;Malicious-URL;Malicious-URL;;hxxp://UN-TIREMENT.COM/file.php?document=dmlsbGUubHVvdG9AY3lnYXRlMzpw;william_scott@flexovitportal.com;65.31.39.3;;

12.6.2017 22:17;;;Malicious-URL;;hxxp://MYSAFERRETIREMENT.COM/file.php?document=YW50dGkuamFhc2ltbGZlbnVudG9NS2ZlZ0Z5SmaQ=;william_scott@flexovitportal.com;216.189.216.180;;

12.6.2017 22:18;;;Malicious-URL;Malicious-URL;;blackhatseos.com;andralb54@gmail.com;112.121.181.66;;

12.6.2017 22:48;;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@metrographicsreporter.com;103.48.81.28;;

12.6.2017 22:54;;;Malicious-URL;;hxxp://constructionmanagersgroup.net/file.php?document=am9ha2ltLjVzWhYQGN5Z2F0Z5SmaQ=;william_scott@flexovitportal.com;165.228.171.126;;

12.6.2017 22:59;;;Malicious-URL;;hxxp://floretdubai.com/file.php?document=a2FyaS52aXJ0YW5lbnkBJeWdhGUuZmk=;william_scott@flexovitportal.com;24.64.81.0;;

12.6.2017 23:10;;;Malicious-URL;Malicious-URL;;organictabletinc.ru;update+wdvz9if9eb6s@branddrivencommunity.com;216.15.232.100;;

12.6.2017 23:21;;;Malicious-URL;Malicious-URL;;organictabletinc.ru;support+ju23c69t6m0o@guinter.com;188.93.228.50;;

12.6.2017 23:23;;;Malicious-URL;Malicious-URL;;medicalrxquality.su;notification+r5mgug0skoup@presidentialelectionpolls.com;62.210.88.161;;

12.6.2017 23:25;;;Malicious-URL;;hxxp://krishnadress.com/file.php?document=amFubmUuamFhc2ltbGZlbnVudG9NS2ZlZ0Z5SmaQ=;william_scott@flexovitportal.com;216.189.184.32;;

12.6.2017 23:25;;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@juicedblog.com;178.16.24.75;;

12.6.2017 23:25;;;Malicious-URL;Malicious-URL;;bestdater.ru;alert@juicedblog.com;178.16.24.75;;

12.6.2017 23:25;;;Malicious-URL;Malicious-URL;;rusbestdate.ru;alert@juicedblog.com;178.16.24.75;;

12.6.2017 23:35;;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@juicedblog.com;178.16.24.75;;

12.6.2017 23:35;;;Malicious-URL;;update+awwromzn3nwa@coalla.com;87.106.21.25;;

12.6.2017 23:40;;;Malicious-URL;;hxxp://REDBLOSSOM.CO.UK/file.php?document=bm9va2Uua29uc3RpZ0JjeWdhGUuZmk=;william_scott@flexovitportal.com;173.92.94.104;;

12.6.2017 23:43;;;Malicious-URL;Malicious-URL;;hxxp://CMGPLACEMENT.COM/file.php?document=bWfyaS50YWhbWFrAUjjeWdhGUuZmk=;william_scott@flexovitportal.com;50.96.83.221;;

12.6.2017 23:45;;;Malicious-URL;;gexinmeng@shanghaizhida.com;222.73.105.170;;

12.6.2017 23:46;;;Malicious-URL;Malicious-URL;;hxxp://CMGPLACEMENT.NET/file.php?document=YW50dGkuaz2FubmluZW5AY3lnYXRlMzpw;william_scott@flexovitportal.com;205.201.72.24;;

12.6.2017 23:51;;;Malicious-URL;;hxxp://krishnadress.com/file.php?document=c2FtdS52aXJ0YW1vQGN5Z2F0Z5SmaQ=;william_scott@flexovitportal.com;24.163.80.221;;

13.6.2017 0:00;;;Malicious-URL;;hxxp://constructionmanagersgroup.net/file.php?document=dG9taS5yYXJsc3NvbkJjeWdhGUuZmk=;william_scott@flexovitportal.com;73.183.34.144;;

13.6.2017 0:10;;;Malicious-URL;Malicious-URL;;hxxp://CMGPLACEMENT.NET/file.php?document=bWfya3VzLmt1aXZhbGZlbnVudG9NS2ZlZ0Z5SmaQ=;william_scott@flexovitportal.com;66.42.178.189;;

13.6.2017 0:15;;Malicious-URL;;Malicious-URL;;hxxp://CMGPLACEMENT.COM/file.php?document=cGV0cmkuaGVpbm9uZW5AY3lnYXRlMzpw;william_scott@flexovitportal.com;50.235.56.154;;

13.6.2017 0:21;;Malicious-URL;;Malicious-URL;;;rbiosc.com;info@019710.com;104.194.28.202;;

13.6.2017 0:38;;Malicious-URL;;Malicious-URL;;;medicalrxreward.ru;alert@insuredbysammy.com;91.221.71.204;;

13.6.2017 2:38;;Malicious-URL;;;keisuke_falling_gimmy@yahoo.co.jp;113.172.161.175;;

13.6.2017 3:13;;Malicious-URL;;Malicious-URL;;;macartu.cn;nkogeisqka@hmveng.com;202.39.79.161;;

13.6.2017 3:46;;Malicious-URL;;;wuyhi.com;;;

13.6.2017 3:48;;Malicious-URL;;Malicious-URL;;;wuyhi.com;;;

13.6.2017 4:51;;Malicious-URL;;;eka_mdk@yahoo.co.id;123.24.181.226;;

13.6.2017 4:54;;Malicious-URL;;Malicious-URL;;;wuyhi.com;czlbuokiwmw@heijmans.nl;50.199.157.91;;

13.6.2017 4:54;;Malicious-URL;;Malicious-URL;;;onlinesmartsale.com;dikspwjke@heijmans.nl;50.199.157.91;;

13.6.2017 4:54;;Malicious-URL;;Malicious-URL;;;onlinesmartsale.com;;;

13.6.2017 5:14;;Malicious-URL;;Malicious-URL;;;sexy-dates.ru;info@HIGHBALL.fr;113.160.200.116;;

13.6.2017 6:35;;Malicious-URL;;;dealydid.com;;;

13.6.2017 6:59;;Malicious-URL;;Malicious-URL;;;sexy-dates.ru;info@SALARIED.nl;110.164.158.137;;

13.6.2017 7:22;;Malicious-URL;;Malicious-URL;;;dealydo.com;;;

13.6.2017 7:55;;Malicious-URL;;Malicious-URL;;;macartu.cn;lbtswtttnze@hmsoldies.org.uk;180.210.205.107;;

13.6.2017 7:55;;Malicious-URL;;Malicious-URL;;;macartu.cn;qeswvpyfo@hmsoldies.org.uk;180.210.205.107;;

13.6.2017 8:24;;Malicious-URL;;Malicious-URL;;;nations-direct.com;information@nations-direct.com;178.32.46.58;;

13.6.2017 8:34;;Malicious-URL;;Malicious-URL;;;sexy-dates.ru;sales@applixure.com;88.151.98.62;;

13.6.2017 8:38;46c1223e7b1f0b91ebc52e111802733a;JS_NEMU.B2B35B1C;Malware;Malicious-URL;Malware;23308.js;;jens.marcus-moeller@thomasville.com;208.66.204.4;;

13.6.2017 8:38;98bc956c17d66e9d685e75e9efe55584;JS_NEMU.B2B35B1C;Malware;Malicious-URL;Malware;835338.zip;;jens.marcus-moeller@thomasville.com;208.66.204.4;;

13.6.2017 8:38;e6836cad27b9a9c01b36726b317a6b02;JS_NEMU.B2B35B1C;Malware;Malicious-URL;Malware;23308.zip;;jens.marcus-moeller@thomasville.com;208.66.204.4;;

13.6.2017 8:51;;Malicious-URL;;;messages@fiflirts.agency;185.132.51.67;;

13.6.2017 8:59;;Malicious-URL;;Malicious-URL;;;familierabatnordic.dk;;;

13.6.2017 9:16;;Malicious-URL;;;lelah@faitunes.com;185.171.235.15;;

13.6.2017 9:27;;Malicious-URL;;Malicious-URL;;;dock.email;noreply@runbenrun.info;93.90.123.202;;

13.6.2017 9:36;;Malicious-URL;;Malicious-URL;;;medicalrxreward.ru;alert@destination-image.com;64.64.6.45;;

13.6.2017 9:39;;Malicious-URL;;;daniel-beer.de;;;

13.6.2017 9:48;;Malicious-URL;;Malicious-URL;;;sexy-dates.ru;info@LANE.fr;14.176.60.26;;

13.6.2017 10:09;;Malicious-URL;;Malicious-URL;;;medicalrxreward.ru;notification+3rtxcw6dpot@smilevictorville.com;188.165.207.150;;

13.6.2017 10:11;;Malicious-URL;;Malicious-URL;;;shipproductions.org;info@bfcitc.org;115.49.66.100;;

13.6.2017 10:11;;Malicious-URL;;Malicious-URL;;;familierabatnordic.dk;;;

13.6.2017 10:17;;Malicious-URL;;Malicious-URL;;;organictabletinc.ru;alert@turtlescostume.com;104.131.94.142;;

13.6.2017 10:24;;Malicious-URL;;Malicious-URL;;;sexy-dates.ru;info@OSPNEY.nl;113.163.216.227;;

13.6.2017 10:35;;Malicious-URL;;Malicious-URL;;;organictabletinc.ru;alert@Gateway.com;112.78.2.109;;

13.6.2017 10:50;;Malicious-URL;;Malicious-URL;;;medicalrxreward.ru;alert@productfilters.com;203.170.192.64;;

13.6.2017 10:52;;Malicious-URL;;;martinrepyto@mail.com;185.127.18.204;;

13.6.2017 10:54;;Malicious-URL;;Malicious-URL;;;medicalrxquality.su;alert@autoxchangeinc.com;185.45.75.235;;

13.6.2017 10:54;;Malicious-URL;;Malicious-URL;;;medicalrxreward.ru;support+o9otmzouwdbf@ajitbetageri.com;178.77.103.62;;

13.6.2017 10:57;;Malicious-URL;;Malicious-URL;;;medicalrxquality.su;pending+9dk7vk2m7z8o@macauleymarketing.com;81.22.98.225;;

13.6.2017 11:03;;Malicious-URL;;Malicious-URL;;;scandigogo.com;;;

13.6.2017 11:08;;Malicious-URL;;Malicious-URL;;;medicalrxquality.su;alert@successbets.com;216.222.194.166;;

13.6.2017 11:13;;Malicious-URL;;Malicious-URL;;;organictabletinc.ru;alert@giftavoice.com;46.101.72.178;;

13.6.2017 11:20;;Malicious-URL;;Malicious-URL;;;yatejiancai.net;info@yatejiancai.net;52.213.100.116;;

13.6.2017 11:24;;Malicious-URL;;Malicious-URL;;;medicalrxreward.ru;pending+7z1eyv30fh3@1934penny.com;103.48.81.8;;

13.6.2017 11:43;;Malicious-URL;;Malicious-URL;;;medicalrxquality.su;alert@balanceandoptions.com;162.144.195.166;;

13.6.2017 12:00;3f80789e58a287b67d0ce4793e3e9061;JS.Downloader.D;Malware;Malware;InvoicePIS3179940.zip;NoReplyMailbox@nautilusmusic.com;115.74.86.90;;

13.6.2017 12:00;69df4c90f05190fa200411f5df699a0f;JS.Downloader.D;Malware;Malware;B2UC5VZ5F.wsf;NoReplyMailbox@nautilusmusic.com;115.74.86.90;;

13.6.2017 12:00;7c71d8a6e76e41249f927154092a5e03;JS.Downloader.D;Malware;Malware;B2UC5VZ5F.wsf;NoReplyMailbox@nautilusmusic.com;115.74.86.90;;

13.6.2017 12:02;526146d4900b3491c8257ce1ed16655b;JS.Downloader.D;Malware;Malware;TFYGNILC.zip;NoReplyMailbox@xn-grnli-kua.se;61.2.8.106;;

13.6.2017 12:02;c4966e1fb25010707e7ccc19566046c7;JS.Downloader.D;Malware;Malware;InvoicePIS0094570.zip;NoReplyMailbox@candlestore.fr;103.50.145.67;;

13.6.2017 12:02;c4966e1fb25010707e7ccc19566046c7;JS.Downloader.D;Malware;Malware;InvoicePIS7845316.zip;NoReplyMailbox@xn-grnli-kua.se;61.2.8.106;;

13.6.2017 12:02;f37ed21521ba91f504e3ac9b5df68705;JS.Downloader.D;Malware;Malware;TFYGNILC.wsf;NoReplyMailbox@xn-grnli-kua.se;61.2.8.106;;

13.6.2017 12:03;5172b22c21aebc7b57a72d5c527af55d;JS.Downloader.D;Malware;Malware;InvoicePIS4073046.zip;NoReplyMailbox@plumhoff.dk;190.117.167.141;;

13.6.2017 12:03;9073c2faa0dfb772f92fd4c9e5496ac;JS.Downloader.D;Malware;Malware;TPBACUCUQ.zip;NoReplyMailbox@plumhoff.dk;190.117.167.141;;

13.6.2017 12:03;ab9fb30797b98280046f9c58b4a0036d;JS.Downloader.D;Malware;Malware;TPBACUCUQ.wsf;NoReplyMailbox@plumhoff.dk;190.117.167.141;;

13.6.2017 12:04;3e975a5ced5918906ee15c83b0b3cb29;JS.Downloader.D;Malware;Malware;InvoicePIS2189699.zip;NoReplyMailbox@louisianafairsandfestivals.com;110.227.104.110;;

13.6.2017 12:04;3e975a5ced5918906ee15c83b0b3cb29;JS.Downloader.D;Malware;Malware;InvoicePIS8511463.zip;NoReplyMailbox@pdcodnet.com;154.72.134.221;;

13.6.2017 12:04;3e975a5ced5918906ee15c83b0b3cb29;JS.Downloader.D;Malware;Malware;InvoicePIS1507687.zip;NoReplyMailbox@printme.org;59.93.94.162;;

13.6.2017 12:04;3e975a5ced5918906ee15c83b0b3cb29;JS.Downloader.D;Malware;Malware;InvoicePIS5274562.zip;NoReplyMailbox@sofaroos.co.uk;117.202.184.4;;

13.6.2017 12:04;3e975a5ced5918906ee15c83b0b3cb29;JS.Downloader.D;Malware;Malware;InvoicePIS4782998.zip;NoReplyMailbox@theroaminggambler.com;103.59.104.75;;

13.6.2017 12:04;5172b22c21aebc7b57a72d5c527af55d;JS.Downloader.D;Malware;Malware;InvoicePIS6131006.zip;NoReplyMailbox@fontedegliangeli.it;117.98.166.181;;

13.6.2017 12:04;5172b22c21aebc7b57a72d5c527af55d;JS.Downloader.D;Malware;Malware;InvoicePIS9363476.zip;NoReplyMailbox@rispoliveiculos.com.br;106.77.161.68;;

13.6.2017 12:04;9a0c08ccafed1843ea30d63d29019a73;JS.Downloader.D;Malware;Malware;FHPD2HVB.wsf;NoReplyMailbox@sofaroos.co.uk;117.202.184.4;;

13.6.2017 12:04;fb2aad75c5e9dc7514690ad12fc05423;JS.Downloader.D;Malware;Malware;FHPD2HVB.zip;NoReplyMailbox@sofaroos.co.uk;117.202.184.4;;

13.6.2017 12:05;223d29567ba935df3779af04fa59880b;JS.Downloader.D;Malware;Malware;InvoicePIS9722662.zip;NoReplyMailbox@christtemplekal.org;39.43.73.173;;

13.6.2017 12:05;3e975a5ced5918906ee15c83b0b3cb29;JS.Downloader.D;Malware;Malware;InvoicePIS9004414.zip;NoReplyMailbox@davis.com.vn;14.230.20.39;;

13.6.2017 12:05;bd8472d1eb31dc820d2e080ed45ee0ea;JS.Downloader.D;Malware;Malware;BSYFBZJDX.wsf;NoReplyMailbox@christtemplekal.org;39.43.73.173;;

13.6.2017 12:05;efde4115a3f47c82a0d4b7312461eae;JS.Downloader.D;Malware;Malware;BSYFBZJDX.zip;NoReplyMailbox@christtemplekal.org;39.43.73.173;;

13.6.2017 12:06;43ed9ab5e44d436c0d3cdd328b085028;JS.Downloader.D;Malware;Malware;IPMCZD1YJ.zip;NoReplyMailbox@nyhusern.com;43.225.167.78;;

13.6.2017 12:06;984adab27189c9c623dace9495e69c302;JS.Downloader.D;Malware;Malware;IPMCZD1YJ.wsf;NoReplyMailbox@nyhusern.com;43.225.167.78;;

13.6.2017 12:06;9f032ddf5fb26721f8048dfb4f27e35f;JS.Downloader.D;Malware;Malware;InvoicePIS8702035.zip;NoReplyMailbox@nyhusern.com;43.225.167.78;;

13.6.2017 12:07;09819034c977e0450872c7c288652a47;JS.Downloader.D;Malware;Malware;JPSSFFO1.zip;NoReplyMailbox@springstco.com;46.41.217.27;;

13.6.2017 12:07;9f032ddf5fb26721f8048dfb4f27e35f;JS.Downloader.D;Malware;Malware;InvoicePIS2356417.zip;NoReplyMailbox@carlb.info;46.143.152.31;;

13.6.2017 12:07;9f032ddf5fb26721f8048dfb4f27e35f;JS.Downloader.D;Malware;Malware;InvoicePIS4633216.zip;NoReplyMailbox@dragmedia.org;116.212.150.38;;

13.6.2017 12:07;ede88d33d78e18ef96a2fb2764cec35c;JS.Downloader.D;Malware;Malware;InvoicePIS3401906.zip;NoReplyMailbox@springstco.com;46.41.217.27;;

13.6.2017 12:07;fedb8842a221eb1b29540f1051890e5e;JS.Downloader.D;Malware;Malware;JPSSFFO1.wsf;NoReplyMailbox@springstco.com;46.41.217.27;;

13.6.2017 12:08;36a74330e6a71e992f378cd4eac7dd84;JS.Downloader.D;Malware;Malware;RHK9AGFQL.wsf;NoReplyMailbox@rewind-theband.com;103.37.80.38;;

13.6.2017 12:08;80142388c9f4de411bf96356bd92d9e6;JS.Downloader.D;Malware;Malware;RHK9AGFQL.zip;NoReplyMailbox@rewind-theband.com;103.37.80.38;;

13.6.2017 12:08;8aacfa6a28804d2298002eb2352aa794;JS.Downloader.D;Malware;Malware;InvoicePIS5321638.zip;NoReplyMailbox@rewind-theband.com;103.37.80.38;;

13.6.2017 12:08;ede88d33d78e18ef96a2fb2764cec35c;JS.Downloader.D;Malware;Malware;InvoicePIS1564740.zip;NoReplyMailbox@biblicalinsights.net;2.180.23.199;;

13.6.2017 12:09;09d4057883a48dde20dfe8b62da57419;JS.Downloader.D;Malware;Malware;PLCUXBVT.wsf;NoReplyMailbox@ptsddiary.com;49.238.44.97;;

13.6.2017 12:09;8aacfa6a28804d2298002eb2352aa794;JS.Downloader.D;Malware;Malware;InvoicePIS5651097.zip;NoReplyMailbox@primeiasi.ro;112.196.73.189;;

13.6.2017 12:09;bd5b660fcc3db79de684c0b66e5afc27;JS.Downloader.D;Malware;Malware;PLCUXBVT.zip;NoReplyMailbox@ptsddiary.com;49.238.44.97;;

13.6.2017 12:09;cb16a4deb2bae3a50e64c5eb4b7ea8bd;JS.Downloader.D;Malware;Malware;InvoicePIS8867820.zip;NoReplyMailbox@ptsddiary.com;49.238.44.97;;

13.6.2017 12:10;223d29567ba935df3779af04fa59880b;JS.Downloader.D;Malware;Malware;InvoicePIS8342713.zip;NoReplyMailbox@metromutt.org;203.189.135.226;;

13.6.2017 12:10;33159e1ba7d06d3d116a4a963447d9c8;JS.Downloader.D;Malware;Malware;XN8TBZBY2.zip;NoReplyMailbox@raytalteyzers.com;106.215.183.211;;

13.6.2017 12:10;7d701ec0d3d0200c686393ccadef2f6;JS.Downloader.D;Malware;;Malware;XN8TBZBY2.wsf;;NoReplyMailbox@raytalleydancers.com;106.215.183.211;;
13.6.2017
12:10;c7ee52c969e5cc7508fa5689411a820b;JS.Downloader.D;Malware;;Malware;InvoicePIS2595232.zip;;NoReplyMailbox@raytalleydancers.com;106.215.183.211;;
13.6.2017
12:10;cb16a4deb2bae3a50e64c5eb4b7ea8bd;JS.Downloader.D;Malware;;Malware;InvoicePIS6400750.zip;;NoReplyMailbox@mundotecnologico.pt;198.0.81.45;;
13.6.2017
12:11;293b51bf87e0eaa93b4bb28f3191d4ae;JS.Downloader.D;Malware;;Malware;HDW5KJXU.zip;;NoReplyMailbox@giovanilorenzen.com.br;180.211.134.122;;
13.6.2017
12:11;84629f2363f31b47f6322ad61601f4fa;JS.Downloader.D;Malware;;Malware;HDW5KJXU.wsf;;NoReplyMailbox@giovanilorenzen.com.br;180.211.134.122;;
13.6.2017
12:11;d4ed15624e925e688e3f51b713bc6a87;JS.Downloader.D;Malware;;Malware;InvoicePIS9178471.zip;;NoReplyMailbox@cheztantelori.com;139.192.30.68;;
13.6.2017 12:11;d4ed15624e925e688e3f51b713bc6a87;JS.Downloader.D;Malware;;Malware;InvoicePIS9404715.zip;;NoReplyMailbox@divtech.info;200.122.205.99;;
13.6.2017
12:11;d4ed15624e925e688e3f51b713bc6a87;JS.Downloader.D;Malware;;Malware;InvoicePIS5661034.zip;;NoReplyMailbox@giovanilorenzen.com.br;180.211.134.122;;
13.6.2017 12:12;6aa8a735eb430dae15ea44ac688ff663;JS.Downloader.D;Malware;;Malware;VZAQEXB94.zip;;NoReplyMailbox@hyperbarictech.com;202.91.79.154;;
13.6.2017 12:12;bb468eaa16aea17ebd9d7b0c938ba74;JS.Downloader.D;Malware;;Malware;InvoicePIS3248027.zip;;NoReplyMailbox@frankaudio.dk;37.111.130.127;;
13.6.2017
12:12;bb468eaa16aea17ebd9d7b0c938ba74;JS.Downloader.D;Malware;;Malware;InvoicePIS6133988.zip;;NoReplyMailbox@hyperbarictech.com;202.91.79.154;;
13.6.2017 12:12;bb468eaa16aea17ebd9d7b0c938ba74;JS.Downloader.D;Malware;;Malware;InvoicePIS1427486.zip;;NoReplyMailbox@vidaki.nl;202.156.240.108;;
13.6.2017 12:12;bfc8b8f8e1660c6d8c4a7a4c72afac81;JS.Downloader.D;Malware;;Malware;VZAQEXB94.wsf;;NoReplyMailbox@hyperbarictech.com;202.91.79.154;;
13.6.2017 12:13;5d439130ecc3dbb571c3883cc77e95e;JS.Downloader.D;Malware;;Malware;JVHQPMPYH.zip;;NoReplyMailbox@powowpress.co.uk;123.200.16.190;;
13.6.2017 12:13;81cf3a21795e3f9f54acc81934241613;JS.Downloader.D;Malware;;Malware;JVHQPMPYH.wsf;;NoReplyMailbox@powowpress.co.uk;123.200.16.190;;
13.6.2017
12:13;f6cb606c2e6c5951e624d3a31d512eeb;JS.Downloader.D;Malware;;Malware;InvoicePIS6622531.zip;;NoReplyMailbox@powowpress.co.uk;123.200.16.190;;
13.6.2017 12:14;512072f1dd120f34d3e8362f74db1a40;JS.Downloader.D;Malware;;Malware;OGFANA687.wsf;;NoReplyMailbox@dxbtours.com;43.229.88.102;;
13.6.2017 12:14;593a16136334533d043698abcce3068;JS.Downloader.D;Malware;;Malware;OGFANA687.zip;;NoReplyMailbox@dxbtours.com;43.229.88.102;;
13.6.2017 12:14;6eb312550af99eae30fa63c8bdc9fb62;JS.Downloader.D;Malware;;Malware;InvoicePIS6274897.zip;;NoReplyMailbox@4cshellfish.com;61.2.106.3;;
13.6.2017 12:14;6eb312550af99eae30fa63c8bdc9fb62;JS.Downloader.D;Malware;;Malware;InvoicePIS0042480.zip;;NoReplyMailbox@dxbtours.com;43.229.88.102;;
13.6.2017 12:14;6eb312550af99eae30fa63c8bdc9fb62;JS.Downloader.D;Malware;;Malware;InvoicePIS9300309.zip;;NoReplyMailbox@qcmarathon.org;59.145.104.174;;
13.6.2017
12:14;6eb312550af99eae30fa63c8bdc9fb62;JS.Downloader.D;Malware;;Malware;InvoicePIS5982033.zip;;NoReplyMailbox@sunstatepartners.com;118.69.53.35;;
13.6.2017 12:14;f6cb606c2e6c5951e624d3a31d512eeb;JS.Downloader.D;Malware;;Malware;InvoicePIS5965517.zip;;NoReplyMailbox@hansalbers.nl;212.33.201.184;;
13.6.2017 12:15;2ad928715cc7bc8e7c06450e618d4a0;JS.Downloader.D;Malware;;Malware;DBLMBZEUY.wsf;;NoReplyMailbox@nikkibeulens.com;137.59.134.211;;
13.6.2017 12:15;5738bba256223495535afb9d1575f66b;JS.Downloader.D;Malware;;Malware;DBLMBZEUY.zip;;NoReplyMailbox@nikkibeulens.com;137.59.134.211;;
13.6.2017 12:15;a2e6ca9d86fad627cf76092638020dfa;JS.Downloader.D;Malware;;Malware;InvoicePIS7921637.zip;;NoReplyMailbox@nikkibeulens.com;137.59.134.211;;
13.6.2017 12:15;a2e6ca9d86fad627cf76092638020dfa;JS.Downloader.D;Malware;;Malware;InvoicePIS7800814.zip;;NoReplyMailbox@perisa.se;186.32.191.194;;
13.6.2017 12:16;1d4864a1f0f24b7e483f459e6b7babc2;JS.Downloader.D;Malware;;Malware;InvoicePIS6376011.zip;;NoReplyMailbox@ets.no;113.160.116.32;;
13.6.2017 12:16;1d4864a1f0f24b7e483f459e6b7babc2;JS.Downloader.D;Malware;;Malware;InvoicePIS7452266.zip;;NoReplyMailbox@lobi-info.rs;1.53.243.105;;
13.6.2017
12:16;1d4864a1f0f24b7e483f459e6b7babc2;JS.Downloader.D;Malware;;Malware;InvoicePIS2459503.zip;;NoReplyMailbox@monarchtrainingolutions.com;59.99.243.156
;;
13.6.2017 12:16;1d4864a1f0f24b7e483f459e6b7babc2;JS.Downloader.D;Malware;;Malware;InvoicePIS5150014.zip;;NoReplyMailbox@ronaldjw.com;221.120.224.145;;
13.6.2017 12:16;1d4864a1f0f24b7e483f459e6b7babc2;JS.Downloader.D;Malware;;Malware;InvoicePIS8750460.zip;;NoReplyMailbox@tochikiraeta.com;113.174.104.91;;
13.6.2017 12:16;2a7ae2fb3ee240086916ffdc11b21d3;JS.Downloader.D;Malware;;Malware;BXTLKK5R.wsf;;NoReplyMailbox@ronaldjw.com;221.120.224.145;;
13.6.2017 12:16;66fbf485bb2836042c42c59ea1421ecb;JS.Downloader.D;Malware;;Malware;0935973187542.zip;;olgame@aflux.fr;46.218.151.111;;
13.6.2017 12:16;77660a6f528157e84bb565dbcc1cbf2;JS.Downloader.D;Malware;;Malware;5793.zip;;olgame@aflux.fr;46.218.151.111;;
13.6.2017 12:16;79ac63623d9565380549e4aa82ad9664;JS.Downloader.D;Malware;;Malware;BXTLKK5R.zip;;NoReplyMailbox@ronaldjw.com;221.120.224.145;;
13.6.2017 12:16;a2e6ca9d86fad627cf76092638020dfa;JS.Downloader.D;Malware;;Malware;InvoicePIS1027146.zip;;NoReplyMailbox@pandmarine.com;183.80.189.198;;
13.6.2017 12:16;a2e6ca9d86fad627cf76092638020dfa;JS.Downloader.D;Malware;;Malware;InvoicePIS2508977.zip;;NoReplyMailbox@tecniofi.net;154.66.122.34;;
13.6.2017 12:17;1d4864a1f0f24b7e483f459e6b7babc2;JS.Downloader.D;Malware;;Malware;InvoicePIS2445912.zip;;NoReplyMailbox@dr-dianne.com;197.232.52.130;;
13.6.2017
12:17;893fc32645577666d43cd12d3fd9bd75;JS.Downloader.D;Malware;;Malware;InvoicePIS9192946.zip;;NoReplyMailbox@flammula.com.br;115.79.104.102;;
13.6.2017
12:17;893fc32645577666d43cd12d3fd9bd75;JS.Downloader.D;Malware;;Malware;InvoicePIS4094689.zip;;NoReplyMailbox@fledgelingmusic.co.uk;91.98.57.102;;
13.6.2017 12:17;893fc32645577666d43cd12d3fd9bd75;JS.Downloader.D;Malware;;Malware;InvoicePIS9606908.zip;;NoReplyMailbox@mikokoepke.com;185.4.18.101;;
13.6.2017
12:17;893fc32645577666d43cd12d3fd9bd75;JS.Downloader.D;Malware;;Malware;InvoicePIS3909330.zip;;NoReplyMailbox@rbyrneproductions.com;94.183.162.241;;
13.6.2017
12:17;b3926c9c186be295982388b746a70bcc;JS.Downloader.D;Malware;;Malware;UQLRRLKT.zip;;NoReplyMailbox@rbyrneproductions.com;94.183.162.241;;
13.6.2017 12:17;ceefdae29e83f337f4f0824258fb9ce;JS.Downloader.D;Malware;;Malware;UQLRRLKT.wsf;;NoReplyMailbox@rbyrneproductions.com;94.183.162.241;;
13.6.2017 12:18;1cc50ccce0f7f39044c19f2173326b5;JS.Downloader.D;Malware;;Malware;InvoicePIS2763476.zip;;NoReplyMailbox@ffices.com;103.236.115.190;;
13.6.2017
12:18;893fc32645577666d43cd12d3fd9bd75;JS.Downloader.D;Malware;;Malware;InvoicePIS1524721.zip;;NoReplyMailbox@amerispec.hrcxmail.com;171.61.66.142;;
13.6.2017
12:18;893fc32645577666d43cd12d3fd9bd75;JS.Downloader.D;Malware;;Malware;InvoicePIS2136893.zip;;NoReplyMailbox@aversaagency.net;117.213.136.113;;
13.6.2017
12:18;893fc32645577666d43cd12d3fd9bd75;JS.Downloader.D;Malware;;Malware;InvoicePIS2206646.zip;;NoReplyMailbox@huserarchitekten.ch;78.39.246.98;;
13.6.2017 12:18;95e39b56c329d061fe2cd2e795c64536;JS.Downloader.D;Malware;;Malware;VGGX81KY.wsf;;NoReplyMailbox@ffices.com;103.236.115.190;;
13.6.2017 12:18;c3a3705f71d0c30bf95a85dd1d8a75b;JS.Downloader.D;Malware;;Malware;VGGX81KY.zip;;NoReplyMailbox@ffices.com;103.236.115.190;;
13.6.2017 12:19;1cc50ccce0f7f39044c19f2173326b5;JS.Downloader.D;Malware;;Malware;InvoicePIS8635822.zip;;NoReplyMailbox@urgent-consult.com;117.0.171.77;;
13.6.2017 12:19;ede88d33d78e18ef96a2fb2764cec35c;JS.Downloader.D;Malware;;Malware;InvoicePIS6623211.zip;;NoReplyMailbox@ipbacbkone.co.uk;91.98.104.41;;
13.6.2017 12:20;223ad29567ba935df3779a0f4fa59880b;JS.Downloader.D;Malware;;Malware;InvoicePIS7515194.zip;;NoReplyMailbox@nsh.m.dk;203.112.217.200;;
13.6.2017 12:20;ede88d33d78e18ef96a2fb2764cec35c;JS.Downloader.D;Malware;;Malware;InvoicePIS6061100.zip;;NoReplyMailbox@famvanrijn.nl;117.200.227.37;;
13.6.2017 12:21;1dda0ecd29f7dfe2052b4c666d2676b5;JS.Downloader.D;Malware;;Malware;W4MEVE8KL.zip;;NoReplyMailbox@phpmysites.us;93.132.33.141;;
13.6.2017 12:21;da026c4f42aba48979e10c67ef830549;JS.Downloader.D;Malware;;Malware;W4MEVE8KL.wsf;;NoReplyMailbox@phpmysites.us;93.132.33.141;;
13.6.2017 12:21;e05027f9aa77b0eb50a23e7c46d9ea2;JS.Downloader.D;Malware;;Malware;InvoicePIS9561344.zip;;NoReplyMailbox@euroasia.kz;103.31.178.114;;
13.6.2017
12:21;e05027f9aa77b0eb50a23e7c46d9ea2;JS.Downloader.D;Malware;;Malware;InvoicePIS2538181.zip;;NoReplyMailbox@onlineopinion.net;122.177.111.141;;
13.6.2017 12:21;e05027f9aa77b0eb50a23e7c46d9ea2;JS.Downloader.D;Malware;;Malware;InvoicePIS7441535.zip;;NoReplyMailbox@phpmysites.us;93.132.33.141;;
13.6.2017 12:22;35380ed3b89195d996e417b7cdcecc27;JS.Downloader.D;Malware;;Malware;InvoicePIS8352643.zip;;NoReplyMailbox@cartazero.it;89.185.196.46;;
13.6.2017
12:22;35380ed3b89195d996e417b7cdcecc27;JS.Downloader.D;Malware;;Malware;InvoicePIS8324733.zip;;NoReplyMailbox@cgm.northwestern.edu;118.71.84.49;;
13.6.2017 12:22;35380ed3b89195d996e417b7cdcecc27;JS.Downloader.D;Malware;;Malware;InvoicePIS5241154.zip;;NoReplyMailbox@west-un-42.de;45.115.65.100;;
13.6.2017
12:22;35380ed3b89195d996e417b7cdcecc27;JS.Downloader.D;Malware;;Malware;InvoicePIS1153590.zip;;NoReplyMailbox@kchealthandhealing.com;41.224.72.240;;
13.6.2017
12:22;35380ed3b89195d996e417b7cdcecc27;JS.Downloader.D;Malware;;Malware;InvoicePIS1507308.zip;;NoReplyMailbox@vecdesign.com.br;113.161.165.121;;
13.6.2017
12:22;35380ed3b89195d996e417b7cdcecc27;JS.Downloader.D;Malware;;Malware;InvoicePIS2356714.zip;;NoReplyMailbox@williamnschapel.org;85.15.42.79;;
13.6.2017 12:22;60b353ec26c3792dd3265eddc9c9aa0;JS.Downloader.D;Malware;;Malware;InvoicePIS5TDIWI.wsf;;NoReplyMailbox@cartazero.it;89.185.196.46;;
13.6.2017 12:22;b5237a56671937d3f3b3f6e564af556;JS.Downloader.D;Malware;;Malware;GJEX5TDIWI.zip;;NoReplyMailbox@cartazero.it;89.185.196.46;;
13.6.2017 12:22;e05027f9aa77b0eb50a23e7c46d9ea2;JS.Downloader.D;Malware;;Malware;InvoicePIS6113129.zip;;NoReplyMailbox@kgkozmetik.com;5.53.161.174;;
13.6.2017 12:23;35380ed3b89195d996e417b7cdcecc27;JS.Downloader.D;Malware;;Malware;InvoicePIS9233463.zip;;NoReplyMailbox@elical.com;203.110.93.26;;
13.6.2017 12:23;c4966e1fb25010707e7ccc19566046c7;JS.Downloader.D;Malware;;Malware;InvoicePIS7968216.zip;;NoReplyMailbox@melorymki.pl;103.70.154.199;;
13.6.2017 12:23;c4966e1fb25010707e7ccc19566046c7;JS.Downloader.D;Malware;;Malware;InvoicePIS5542446.zip;;NoReplyMailbox@moratrucking.net;43.243.38.48;;
13.6.2017
12:23;c4966e1fb25010707e7ccc19566046c7;JS.Downloader.D;Malware;;Malware;InvoicePIS8666754.zip;;NoReplyMailbox@secondstoriysales.com;41.227.133.51;;
13.6.2017 12:24;c4966e1fb25010707e7ccc19566046c7;JS.Downloader.D;Malware;;Malware;InvoicePIS3099911.zip;;NoReplyMailbox@goshowit.com;122.144.8.29;;

13.6.2017 12:24;f6cb606c2e6c5951e624d3a1d512eeb;JS.Downloader.D;Malware;;Malware;InvoicePIS6885381.zip;;NoReplyMailbox@adoracion.es;49.248.0.212;;
13.6.2017 12:25;6c7c73e76447f66c1686a70f23ae3c90;JS.Downloader.D;Malware;;Malware;LXMDWRTT1.wsf;;NoReplyMailbox@maxxicredito.com.br;118.69.133.215;;
13.6.2017 12:25;b4b0484a927da4f90a0d4b902cbad9;JS.Downloader.D;Malware;;Malware;LXMDWRTT1.zip;;NoReplyMailbox@maxxicredito.com.br;118.69.133.215;;
13.6.2017
12:25;e5c1f2b82447838983a93ccb0d9d941d;JS.Downloader.D;Malware;;Malware;InvoicePIS0596203.zip;;NoReplyMailbox@maxxicredito.com.br;118.69.133.215;;
13.6.2017 12:26;e5c1f2b82447838983a93ccb0d9d941d;JS.Downloader.D;Malware;;Malware;InvoicePIS7288527.zip;;NoReplyMailbox@deutsche-bauconsult.de;103.56.181.122;;
13.6.2017 12:27;0ed9e760ba4ccb42261d0da451b3cfd9;JS.Downloader.D;Malware;;Malware;PRHWXRUT.zip;;NoReplyMailbox@benix.in;103.61.255.51;;
13.6.2017 12:27;3561db113ce3ac144c38a198ae548e3;JS.Downloader.D;Malware;;Malware;BIBAADUQJ.wsf;;NoReplyMailbox@clearwatermedia.net;182.75.117.218;;
13.6.2017
12:27;3b78c8715eb70bfac98a51a9f6c0e1f2;JS.Downloader.D;Malware;;Malware;InvoicePIS7919963.zip;;NoReplyMailbox@clearwatermedia.net;182.75.117.218;;
13.6.2017 12:27;4b3db4a2f00628192443d23aa74c6ca8;JS.Downloader.D;Malware;;Malware;BIBAADUQJ.zip;;NoReplyMailbox@clearwatermedia.net;182.75.117.218;;
13.6.2017 12:27;4e130f154f01c2d0afd1d4179302a2b1;JS.Downloader.D;Malware;;Malware;PRHWXRUT.wsf;;NoReplyMailbox@benix.in;103.61.255.51;;
13.6.2017 12:27;ea8d80450c8730797d50f962df369681;JS.Downloader.D;Malware;;Malware;InvoicePIS2822771.zip;;NoReplyMailbox@benix.in;103.61.255.51;;
13.6.2017 12:29;25b4d7e7aa58c6a8da842288ea19ed;JS.Downloader.D;Malware;;Malware;TFEPKSEUB.zip;;NoReplyMailbox@gladrentsinc.com;109.102.48.254;;
13.6.2017
12:29;806e41c3c8d60b2141f11b6563dce36;JS.Downloader.D;Malware;;Malware;InvoicePIS8528106.zip;;NoReplyMailbox@gladrentsinc.com;109.102.48.254;;
13.6.2017 12:29;9e489ecf8b9a30f65fa40fe2358806f;JS.Downloader.D;Malware;;Malware;TFEPKSEUB.wsf;;NoReplyMailbox@gladrentsinc.com;109.102.48.254;;
13.6.2017 12:30;6f08c594cb9daf2f7f7e1db74cd449;JS.Downloader.D;Malware;;Malware;JODUBWOOO.zip;;NoReplyMailbox@surface.pk;182.71.29.1;;
13.6.2017
12:30;806e41c3c8d60b2141f11b6563dce36;JS.Downloader.D;Malware;;Malware;InvoicePIS4613345.zip;;NoReplyMailbox@lamerenville.com;123.17.131.129;;
13.6.2017 12:30;9930466bbcc074acc28c463e1f3e768f1;JS.Downloader.D;Malware;;Malware;InvoicePIS1251923.zip;;NoReplyMailbox@alarmdialer.co.uk;59.90.102.88;;
13.6.2017 12:30;9930466bbcc074acc28c463e1f3e768f1;JS.Downloader.D;Malware;;Malware;InvoicePIS7651367.zip;;NoReplyMailbox@surface.pk;182.71.29.1;;
13.6.2017 12:30;ca086db9670fc1f0fe88f23904bc133f;JS.Downloader.D;Malware;;Malware;JODUBWOOO.wsf;;NoReplyMailbox@surface.pk;182.71.29.1;;
13.6.2017 12:31;162e4c99216025359dba1b50c78076e9;JS.Downloader.D;Malware;;Malware;NIBT6L7OT.wsf;;NoReplyMailbox@nexus-com.net;14.176.1.6;;
13.6.2017 12:31;b2831bf675bf7dcd0c73ff1998a6ee59;JS.Downloader.D;Malware;;Malware;NIBT6L7OT.zip;;NoReplyMailbox@nexus-com.net;14.176.1.6;;
13.6.2017 12:31;e8298ff9732445c9d210423c5abd5a6a;JS.Downloader.D;Malware;;Malware;InvoicePIS8033804.zip;;NoReplyMailbox@nexus-com.net;14.176.1.6;;
13.6.2017 12:33;206f540e7bbd3b8c973eb491b60ce971;JS.Downloader.D;Malware;;Malware;WZ8VBHOMZ.zip;;NoReplyMailbox@ecplagas.com;117.221.172.116;;
13.6.2017 12:33;8869dd9e4aebc708b3e3e71ffb90e065;JS.Downloader.D;Malware;;Malware;InvoicePIS6427784.zip;;NoReplyMailbox@ecplagas.com;117.221.172.116;;
13.6.2017 12:33;c27a624a55e0ea55e6facd73179f601;JS.Downloader.D;Malware;;Malware;WZ8VBHOMZ.wsf;;NoReplyMailbox@ecplagas.com;117.221.172.116;;
13.6.2017 12:34;c7ee52c969e5cc7508fa5689411a820b;JS.Downloader.D;Malware;;Malware;InvoicePIS7024420.zip;;NoReplyMailbox@banger.dk;182.187.141.41;;
13.6.2017
12:34;c7ee52c969e5cc7508fa5689411a820b;JS.Downloader.D;Malware;;Malware;InvoicePIS2525732.zip;;NoReplyMailbox@encontrodasartes.com.br;122.162.165.195;;
13.6.2017 12:35;6f7776303d1689e8a420c229660e803;JS.Downloader.D;Malware;;Malware;IFEPZEUS.wsf;;NoReplyMailbox@rijnschoolvrolings.nl;116.102.153.91;;
13.6.2017
12:35;80f109cdb22b65cacab1fc1516a1a0ff;JS.Downloader.D;Malware;;Malware;InvoicePIS3900494.zip;;NoReplyMailbox@rijnschoolvrolings.nl;116.102.153.91;;
13.6.2017 12:35;d4145ea8c209b71818ed293edf4f7058;JS.Downloader.D;Malware;;Malware;IFEPZEUS.zip;;NoReplyMailbox@rijnschoolvrolings.nl;116.102.153.91;;
13.6.2017
12:36;73f5727896c4e1eda0910fb127a424e6;JS.Downloader.D;Malware;;Malware;InvoicePIS5418604.zip;;NoReplyMailbox@acossolucoes.com.br;182.65.215.81;;
13.6.2017 12:36;73789ebf886e48d493fcd88fcb607eeb;JS.Downloader.D;Malware;;Malware;THLFPKKUM.wsf;;NoReplyMailbox@acossolucoes.com.br;182.65.215.81;;
13.6.2017 12:36;e8608cb54abe5ca211bce300114f7358;JS.Downloader.D;Malware;;Malware;THLFPKKUM.zip;;NoReplyMailbox@acossolucoes.com.br;182.65.215.81;;
13.6.2017
12:42;55d34bfd452ab22bf2b9d1d753ca2801;JS.Downloader.D;Malware;;Malware;InvoicePIS8516149.zip;;NoReplyMailbox@bluestonepartnersllc.com;5.219.234.101;;
13.6.2017
12:42;60241e197b935df8e5d1a4f7cbb84f6d;JS.Downloader.D;Malware;;Malware;OISW3UWNF.zip;;NoReplyMailbox@bluestonepartnersllc.com;5.219.234.101;;
13.6.2017
12:42;6b19899a7096403487a461fae9a3c6ebb;JS.Downloader.D;Malware;;Malware;OISW3UWNF.wsf;;NoReplyMailbox@bluestonepartnersllc.com;5.219.234.101;;
13.6.2017 12:42;ab90d092278c83645d7d8bc80467596f;JS.Downloader.D;Malware;;Malware;RKQGL42MY.wsf;;NoReplyMailbox@reciclatec.com.br;193.242.209.180;;
13.6.2017
12:42;b46c5edf7f8e86b94f747838433b526e;JS.Downloader.D;Malware;;Malware;InvoicePIS1563240.zip;;NoReplyMailbox@reciclatec.com.br;193.242.209.180;;
13.6.2017 12:42;f7f73946b7a94d0c382bab9270ef841f;JS.Downloader.D;Malware;;Malware;RKQGL42MY.zip;;NoReplyMailbox@reciclatec.com.br;193.242.209.180;;
13.6.2017 12:43;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;
13.6.2017 12:44;7707e5723aa76cad3111208e45b09b;JS.Downloader.D;Malware;;Malware;QJPMTBCHP.wsf;;NoReplyMailbox@hicdr.com;122.166.16.76;;
13.6.2017 12:44;a154aaa32237277cfd92fa1b839f;JS.Downloader.D;Malware;;Malware;InvoicePIS726234.zip;;NoReplyMailbox@hicdr.com;122.166.16.76;;
13.6.2017 12:44;ed1eaa319acbbf0d954651f5ce3feb2;JS.Downloader.D;Malware;;Malware;QJPMTBCHP.zip;;NoReplyMailbox@hicdr.com;122.166.16.76;;
13.6.2017 12:44;;Malicious-URL;Malicious-URL;;masterlead.info;;;
13.6.2017 12:46;35380ed3b89195d996e417b7cdcecc27;JS.Downloader.D;Malware;;Malware;InvoicePIS7449870.zip;;NoReplyMailbox@piperpress.com;188.158.63.32;;
13.6.2017 12:46;;Malicious-URL;;info@firetrainingsolution.com;194.88.106.148;;
13.6.2017
12:47;0e2afafb7d8c58fb0ec1f9f8e5f4043;JS.Downloader.D;Malware;;Malware;InvoicePIS7907340.zip;;NoReplyMailbox@baytexpaintsgghana.com;154.118.74.163;;
13.6.2017 12:47;831393f5454410039dcb82473ec04c5;JS.Downloader.D;Malware;;Malware;KTUC21SFX.zip;;NoReplyMailbox@baytexpaintsgghana.com;154.118.74.163;;
13.6.2017 12:47;9dbc15f227ad1776b0c5c31cc35763eb;JS.Downloader.D;Malware;;Malware;KTUC21SFX.wsf;;NoReplyMailbox@baytexpaintsgghana.com;154.118.74.163;;
13.6.2017 12:47;;Malicious-URL;Malicious-URL;;medicemail.com;;;
13.6.2017 12:49;35607aa425a91dc5ecabb72f5fe7e8cf;JS.Downloader.D;Malware;;Malware;InvoicePIS7477563.zip;;NoReplyMailbox@ffm.lvcoxxmail.com;106.67.26.56;;
13.6.2017 12:49;bc4189409ee117b4847d503ca4df8804;JS.Downloader.D;Malware;;Malware;J9FZLERJ.wsf;;NoReplyMailbox@ffm.lvcoxxmail.com;106.67.26.56;;
13.6.2017 12:49;e08d12b043dc21198e34f547ba6bf80f;JS.Downloader.D;Malware;;Malware;J9FZLERJ.zip;;NoReplyMailbox@ffm.lvcoxxmail.com;106.67.26.56;;
13.6.2017 12:55;508ad764a04f0adf4b298a4f874a0ba;JS.Downloader.D;Malware;;Malware;OJV13QP7.zip;;NoReplyMailbox@acusine1.eu;117.216.12.144;;
13.6.2017 12:55;ccc436eb276a9ce12337b7b708edd2e;JS.Downloader.D;Malware;;Malware;OJV13QP7.wsf;;NoReplyMailbox@acusine1.eu;117.216.12.144;;
13.6.2017 12:55;e016a7f8b0a65e44b484f0391deb156;JS.Downloader.D;Malware;;Malware;InvoicePIS8992880.zip;;NoReplyMailbox@acusine1.eu;117.216.12.144;;
13.6.2017
12:58;81459d308f6710852229c9d0d165494d;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc83810972341355406296.zip;;showroomfax@hollytreecottagebath.co.uk;117.211.100.20;;
13.6.2017 12:59;47c58b9dac843081bfbbf9e276e3;NO HIT;Malware;Malware;Malware;HSBC Bank Details.jar;jo_serranilla@rmgmedical.com;173.203.187.110;;
13.6.2017
12:59;ab4dbf20517c38c9bd78c24bf98be7b9;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc71224149682067678931.zip;;showroomfax@350ppm.co.uk;14.177.21.926;;
13.6.2017
12:59;ab4dbf20517c38c9bd78c24bf98be7b9;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc13549551352974570561.zip;;showroomfax@cardeliveries.co.uk;14.16.9.74.64;;
13.6.2017
12:59;ab4dbf20517c38c9bd78c24bf98be7b9;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc87963824856931936769.zip;;showroomfax@collinsconsultants.co.uk;11.94.76.149;;
13.6.2017
12:59;ab4dbf20517c38c9bd78c24bf98be7b9;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc51104721012877468069.zip;;showroomfax@icelandprotravel.co.uk;10.3.255.5.83;;
13.6.2017
12:59;ab4dbf20517c38c9bd78c24bf98be7b9;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc99594642198404868570.zip;;showroomfax@move2music.co.uk;197.1.55.65.150;;
13.6.2017
12:59;ab4dbf20517c38c9bd78c24bf98be7b9;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc69364672751192136004.zip;;showroomfax@pbod.globalnet.co.uk;117.241.236.135;;
13.6.2017
13:00;ab4dbf20517c38c9bd78c24bf98be7b9;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc68807746350645575919.zip;;showroomfax@eyetoons.co.uk;197.148.104.100;;
13.6.2017
13:00;ab4dbf20517c38c9bd78c24bf98be7b9;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc90103451548053908952.zip;;showroomfax@irondukeproductions.com;122.163.61.214;;

13.6.2017
13:00;e694e8d98584eec933ec2372d0b0b57c;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc74462597735840641963.zip;;showroomfax@devilsh.globalnet.co.uk;2
10.212.27.98;;
13.6.2017 13:01;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;;;
13.6.2017
13:06;40d4683ba54e81907ec57f70d3d0a089;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc51724415909132821944.zip;;showroomfax@mjnet.worldonline.co.uk
;14.161.12.180;;
13.6.2017
13:10;bab39d5faff17e303d0efaf1b7cb0dab;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc50845351276086429412.zip;;showroomfax@aanddplumbing.co.uk;183.
87.55.40;;
13.6.2017
13:10;bab39d5faff17e303d0efaf1b7cb0dab;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc95704532516027912083.zip;;showroomfax@ksinteriordesign.co.uk;122.
177.82.128;;
13.6.2017 13:10;;Malicious-URL;Malicious-URL;;organictabletinc.ru;;;
13.6.2017
13:11;bab39d5faff17e303d0efaf1b7cb0dab;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc67289622303139083672.zip;;showroomfax@symbol.globalnet.co.uk;1.2
2.71.249;;
13.6.2017
13:13;9f5accfd9fd21b4c519f71eb55fc7c36;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc68575053734550522083.zip;;showroomfax@charactergroup.co.uk;103.2
17.131.250;;
13.6.2017 13:16;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@SUSTAIN.fr;123.16.244.203;;
13.6.2017 13:18;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;info@PLENIPOTENTIARY.fr;42.119.112.153;;
13.6.2017 13:18;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@RADIOGRAPHY.com;14.181.189.194;;
13.6.2017 13:18;;Malicious-URL;Malicious-URL;;sexy-dates.ru;update+ve8ysrm7n81q@gribbinsfilms.com;159.203.114.105;;
13.6.2017 13:19;0e84e05496ef125d8838a7c2ba1dddb;NO HIT;Malware;Malware;Malware;VBJD9GDBP.wsf;;NoReplyMailbox@ajwad.com;139.192.98.110;;
13.6.2017 13:19;7fac821bead47c15100f4fc87bbc0f7;Trojan.Gen.7;Malware;Malware;Malware;InvoicePIS5983294.zip;;NoReplyMailbox@ajwad.com;139.192.98.110;;
13.6.2017 13:19;cb571e4f57dc1b7fe89c33a14974e813;Trojan-
Downloader;JS/Locky;Malware;Malware;Malware;VBJD9GDBP.zip;;NoReplyMailbox@ajwad.com;139.192.98.110;;
13.6.2017 13:20;399179ea6fec3b6025634ca3c9a9a1d9;Trojan-
Downloader;JS/Locky;Malware;Malware;Malware;C9KUM3Z5Y.zip;;NoReplyMailbox@vanberkeladvies.nl;113.189.100.33;;
13.6.2017
13:20;736f0b395ba8096fa05e63eb72d6e925;JS.Downloader.D;Malware;Malware;Malware;C9KUM3Z5Y.wsf;;NoReplyMailbox@vanberkeladvies.nl;113.189.100.33;;
13.6.2017
13:21;bab39d5faff17e303d0efaf1b7cb0dab;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc74871470061476879507.zip;;showroomfax@butler2.worldonline.co.uk
;112.133.236.29;;
13.6.2017
13:21;bab39d5faff17e303d0efaf1b7cb0dab;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc72418492306891394016.zip;;showroomfax@switchtoewood.co.uk;110.9
3.205.228;;
13.6.2017
13:22;30a14d1e9273addf4ff8602168e47d2e;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc2211232972263373070.zip;;showroomfax@kerrynet.co.uk;117.211.1
3.6;;
13.6.2017
13:24;0d7ced64bd438442336dee5d5e695b3d;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc41553723103128116663.zip;;showroomfax@elbico.co.uk;115.79.212
.143;;
13.6.2017 13:25;;JS.Downloader.D;Malware;Malicious-URL;;InvoicePIS4810347.zip;;info@TROT.br NoReplyMailbox@yellowbike.gr;14.228.143.73;;
13.6.2017 13:25;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@PITY.co.uk;113.22.18.49;;
13.6.2017 13:26;12dec9704ee655948ff4d4e5c3e0758;JS.Downloader.D;Malware;Malware;Malware;HJBYP3OM.wsf;;NoReplyMailbox@planj.be;202.153.47.11;;
13.6.2017
13:26;1d4864a1f0f24b7e483f459e6b7babc2;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2736602.zip;;NoReplyMailbox@philipagee.com;191.103.77.54;;
13.6.2017
13:26;1d4864a1f0f24b7e483f459e6b7babc2;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4810347.zip;;NoReplyMailbox@yellowbike.gr;111.94.18.13;;
13.6.2017 13:26;35e5816964c14000ca63ae695348d5c1;JS.Downloader.D;Malware;Malware;Malware;HJBYP3OM.zip;;NoReplyMailbox@planj.be;202.153.47.11;;
13.6.2017 13:26;8259047757f8223956512cf65bc67d0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS7739156.zip;;NoReplyMailbox@planj.be;202.153.47.11;;
13.6.2017
13:27;1d4864a1f0f24b7e483f459e6b7babc2;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1210453.zip;;NoReplyMailbox@paranoticias.com;103.41.212.34;;
13.6.2017
13:27;573f99e725469f4a3a5f11574330cb20;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9557502.zip;;NoReplyMailbox@shiftingshadow.net;202.124.179.26;;
;
13.6.2017
13:27;72b0c9c6e6344facdf5504611e899f17;JS.Downloader.D;Malware;Malware;Malware;CIUWIKUMU.zip;;NoReplyMailbox@shiftingshadow.net;202.124.179.26;;
13.6.2017
13:27;8f2aa19236b274ecf950237700637a2d;JS.Downloader.D;Malware;Malware;Malware;CIUWIKUMU.wsf;;NoReplyMailbox@shiftingshadow.net;202.124.179.26;;
13.6.2017 13:27;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@catchsafaris.com;82.165.137.91;;
13.6.2017 13:27;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@EDUCABLE.pl;14.164.241.49;;
13.6.2017 13:28;c7ee52c969e5cc7508fa5689411a820b;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8388401.zip;;NoReplyMailbox@a-
tipiko.it;122.162.108.208;;
13.6.2017
13:29;c4966e1fb25010707e7cc19566046c7;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9064382.zip;;NoReplyMailbox@araservi.es;117.248.141.199;;
13.6.2017
13:30;b46c5edf7f8e86b94f747838433b526e;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4320386.zip;;NoReplyMailbox@javanan56.com;42.112.55.247;;
13.6.2017
13:30;f5082e000fc1e3bc4a20d28e912edbf2;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc73028054170301542320.zip;;showroomfax@yourmemories.co.uk;197.
3.5.69;;
13.6.2017 13:30;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;notification+d866jb2g6601@ermietaddeo.com;112.175.245.9;;
13.6.2017
13:31;210c9e58d42347b728a07ce4041ead91;JS.Downloader.D;Malware;Malware;Malware;AKSUOE6V.wsf;;NoReplyMailbox@isminikaydet.com;41.228.212.59;;
13.6.2017
13:31;3055a7d2593b2e73d53e6ebc37a2cd20;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc37973930472131838748.zip;;showroomfax@lukebozios.com;122.165
.146.210;;
13.6.2017
13:31;51e4c67da35209722ba90724af27c27c;JS.Downloader.D;Malware;Malware;Malware;AKSUOE6V.zip;;NoReplyMailbox@isminikaydet.com;41.228.212.59;;
13.6.2017
13:31;906bf571289229686dc5fde822b1f0a0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8815860.zip;;NoReplyMailbox@isminikaydet.com;41.228.212.59;;
13.6.2017
13:31;906bf571289229686dc5fde822b1f0a0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3741799.zip;;NoReplyMailbox@performancwebmarketing.com;14.
191.244.71;;
13.6.2017
13:32;6d9548baca165321d649ea879dbc558c;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1889645.zip;;NoReplyMailbox@fourandnine.co.uk;117.211.126.13;;
;
13.6.2017
13:32;6d9548baca165321d649ea879dbc558c;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8260906.zip;;NoReplyMailbox@mмосc.com;117.211.126.13;;
13.6.2017
13:32;980c90ad0ac0e6ab4f0de196c1c2c514;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc38902431906039324297.zip;;showroomfax@abbeycliffrenovations.co
.uk;103.81.211.15;;
13.6.2017
13:32;bc5f5753b558afd1e168c29688e11479;JS.Downloader.D;Malware;Malware;Malware;DXR9MIFMU.zip;;NoReplyMailbox@fourandnine.co.uk;117.211.126.13;;
13.6.2017
13:32;fe04999248f4295bfd79ccdf0f165c4;JS.Downloader.D;Malware;Malware;Malware;DXR9MIFMU.wsf;;NoReplyMailbox@fourandnine.co.uk;117.211.126.13;;

13.6.2017
13:33;63264c36607debe6cb23f3e328e109aa;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc04465030417245429151.zip;;showroomfax@appleguru.co.uk;42.112.67.61;;
13.6.2017
13:33;63264c36607debe6cb23f3e328e109aa;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc73670297967823358527.zip;;showroomfax@borin_globalnet.co.uk;59.177.146.107;;
13.6.2017
13:33;6d9548baca165321d649ea879dbc558c;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4150898.zip;;NoReplyMailbox@amberspage.com;210.2.148.70;;
13.6.2017
13:34;191a2ee39508fa6be4cff62450acef94;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc04697173101097468670.zip;;showroomfax@pixelparrot.co.uk;49.238.62.3;;
13.6.2017
13:34;63264c36607debe6cb23f3e328e109aa;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc63922773771748136516.zip;;showroomfax@lukeawaynow.com;117.221.201.200;;
13.6.2017
13:35;249ec38c0f3b604407373a5d8261d269;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc73512140541633637523.zip;;showroomfax@doorways2power.co.uk;117.240.210.50;;
13.6.2017
13:36;66531df14dd8ae2c9ce56da8ebdd8c29;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc46354611262109778467.zip;;showroomfax@irrigationuk.com;59.145.200.210;;
13.6.2017
13:38;9398d4aafab1a34ce589b045e8559175;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc01462437361346033785.zip;;showroomfax@spanishpropertyclub.org.uk;202.91.81.251;;
13.6.2017
13:39;9398d4aafab1a34ce589b045e8559175;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc44769705104725279391.zip;;showroomfax@ensindraughting.co.uk;17.211.69.188;;
13.6.2017
13:39;9398d4aafab1a34ce589b045e8559175;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc34419302877407774616.zip;;showroomfax@fingerpostfarm.co.uk;109.104.128.54;;
13.6.2017
13:40;15ad0740a13e4aad75aee095501dd0a6;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc56191835675381827718.zip;;showroomfax@monsterlime.co.uk;27.97.172.19;;
13.6.2017
13:40;93c152fba33ede4748f1d126b2cb0661;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc67060729195198498981.zip;;showroomfax@cupis.co.uk;103.239.232.192;;
13.6.2017
13:41;21fee80f788ac800a98692556e56a14;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc29272683899620826806.zip;;showroomfax@axim.co.uk;14.162.132.145;;
13.6.2017 13:41;3ac014e2883b43e08b89a7c04c0296fd;JS.Downloader.D;Malware;Malware;Malware;P1I84RYKF.wsf;;NoReplyMailbox@midocaz.com;103.11.80.22;;
13.6.2017 13:41;55cd299c23b913f21fbcceb7ec2042a6;W2KM_DLOADR.LRN;Malware;Malware;Malware;P1I84RYKF.zip;;NoReplyMailbox@midocaz.com;103.11.80.22;;
13.6.2017
13:41;72f9bdd50fee1d6fea9f085e60ac4a7a;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9128019.zip;;NoReplyMailbox@midocaz.com;103.11.80.22;;
13.6.2017 13:43;087d4b35423bf48988b7a2e24d1efe0d;JS.Downloader.D;Malware;Malware;Malware;BNQJ3RF2J.zip;;NoReplyMailbox@frydenlund.net;73.201.243.150;;
13.6.2017
13:43;2c300ffaceb725650e2d83bad999729c;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc44198274411462246356.zip;;showroomfax@jlllogistics.co.uk;177.36.60.245;;
13.6.2017 13:43;9dea789be596e602f7f076916491930;JS.Downloader.D;Malware;Malware;Malware;BNQJ3RF2J.wsf;;NoReplyMailbox@frydenlund.net;73.201.243.150;;
13.6.2017
13:43;c2624faabd66d00f8b322d48bdabb1d;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3052353.zip;;NoReplyMailbox@frydenlund.net;73.201.243.150;;
13.6.2017
13:44;9d5b50be8d2f147f6a87e2b9a5a5c7e;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc25576115644026313301.zip;;showroomfax@palslegal.co.uk;103.230.222.94;;
13.6.2017
13:45;3055a7d2593b2e73d536eebc37a2cd20;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc70925459246069095272.zip;;showroomfax@lcano.co.uk;202.179.84.218;;
13.6.2017
13:45;3a9d4a80290eaf7da6255cb57b0d310a;JS.Downloader.D;Malware;Malware;Malware;VTIX6OV4W.zip;;NoReplyMailbox@topsyturvytiaras.com;117.241.96.221;;
13.6.2017
13:45;6ca0ac4c4232e37ef5d0aaa66f99cf2d;JS.Downloader.D;Malware;Malware;Malware;VTIX6OV4W.wsf;;NoReplyMailbox@topsyturvytiaras.com;117.241.96.221;;
13.6.2017
13:45;9d5b50be8d2f147f6a87e2b9a5a5c7e;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc73820858153857455941.zip;;showroomfax@q2serves.co.uk;175.107.27.15;;
13.6.2017
13:45;ceddf8634c4b94b560a9cf94c4875eb8;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS5352373.zip;;NoReplyMailbox@propagstudio.sk;103.69.241.193;;
13.6.2017
13:45;ceddf8634c4b94b560a9cf94c4875eb8;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1309532.zip;;NoReplyMailbox@topsyturvytiaras.com;117.241.96.221;;
13.6.2017 13:46;8db85405502241730a1e84fc861408d0;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc52349424471672738762.zip;;showroomfax@c-gstarkey.co.uk;122.161.34.142;;
13.6.2017 13:46;8db85405502241730a1e84fc861408d0;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc48740953242324694283.zip;;showroomfax@elements-chartreuse.co.uk;116.110.174.198;;
13.6.2017
13:48;a2e6ca9d86fad627cf76092638020dfa;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4398753.zip;;NoReplyMailbox@lohnloh.com;41.220.31.34;;
13.6.2017 13:48;a2e6ca9d86fad627cf76092638020dfa;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0099861.zip;;NoReplyMailbox@termik.be;41.220.31.34;;
13.6.2017
13:48;bcd32eee03d1c473868c62c6a0989769;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc79755115676979955456.zip;;showroomfax@iakuhoy.org;191.189.11.160;;
13.6.2017
13:49;90599243c441ffcfb85d077c6b8c5259;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc83560483840240355850.zip;;showroomfax@whatiwantwhenidie.co.uk;39.43.56.92;;
13.6.2017
13:51;93c152fba33ede4748f1d126b2cb0661;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc69620575703551486174.zip;;showroomfax@mdlit.co.uk;171.50.130.109;;
13.6.2017 13:51;9baf7bc8fb721a433646bdd31e743b14;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc81675342086102082071.zip;;showroomfax@liverpool-offices.co.uk;139.0.7.26;;
13.6.2017
13:53;03b126a8bfcf6471c15aa4b5dbbc0c84;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc75228619890661429254.zip;;showroomfax@frothycoffeeman.co.uk;27.34.245.218;;
13.6.2017
13:54;03b126a8bfcf6471c15aa4b5dbbc0c84;W2KM_DLOADR.LRN;Malware;Malware;Malware;doc21023568271907110324.zip;;showroomfax@muddybootsphotography.co.uk;111.93.187.98;;
13.6.2017
14:01;43dc722a14e4e5fb834f45828bb286e1;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;long.bellorhamilton002@sempreeventos.com.br;114.143.90.75;;
13.6.2017 14:01;7c4d863d2f558c49a6265e5a85bb71e0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1813308.zip;;NoReplyMailbox@jazz.hr;14.98.88.62;;
13.6.2017
14:01;7c4d863d2f558c49a6265e5a85bb71e0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS5700794.zip;;NoReplyMailbox@mp3god.screaming.net;14.98.88.62;;
;

13.6.2017
14:01;7c4d863d2f558c49a6265e5a85bb71e0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2545788.zip;;NoReplyMailbox@prnigeria.net;182.75.99.98;;
13.6.2017
14:01;7c4d863d2f558c49a6265e5a85bb71e0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS7104190.zip;;NoReplyMailbox@publiselios.com;116.72.211.189;;
13.6.2017
14:01;7c4d863d2f558c49a6265e5a85bb71e0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1366861.zip;;NoReplyMailbox@skatboet.se;210.212.249.98;;
13.6.2017
14:01;7c4d863d2f558c49a6265e5a85bb71e0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1457766.zip;;NoReplyMailbox@thedesigncompany.org;46.225.56.40;;
13.6.2017 14:01;8ae5fc4e681f7e161056c7a05cbd5abf;JS.Downloader.D;Malware;Malware;Malware;MVOJ8IHOK.zip;;NoReplyMailbox@skatboet.se;210.212.249.98;;
13.6.2017 14:01;d0efb098a42a9e1f646790bd598f574f;JS.Downloader.D;Malware;Malware;Malware;MVOJ8IHOK.wsf;;NoReplyMailbox@skatboet.se;210.212.249.98;;
13.6.2017 14:10;0bc2f300fa4b5af701a42d2845ef034;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;april.supier25401@erts.lu;220.231.127.13;;
13.6.2017 14:10;d957059e7bbd5c4a08fb0aeaa53d37ee;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;lauren.startin00@vzaugg.com;122.165.235.247;;
13.6.2017
14:11;291380c1a818214498ce12284449ee5b;JS.Downloader.D;Malware;Malware;Malware;G3TGDV4D.wsf;;NoReplyMailbox@facialdevelopment.com;87.107.210.253;;
13.6.2017
14:11;37e556964da5d5c093cca6c54c2af301;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9484289.zip;;NoReplyMailbox@facialdevelopment.com;87.107.210.253;;
13.6.2017
14:11;409931d44a97665840c3dac21e0c163;JS.Downloader.D;Malware;Malware;Malware;G3TGDV4D.zip;;NoReplyMailbox@facialdevelopment.com;87.107.210.253;;
13.6.2017 14:11;d957059e7bbd5c4a08fb0aeaa53d37ee;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;sofia.bramwell4521@dedalos-ambiental.com;103.84.186.2;;
13.6.2017 14:12;564bdcead4ac2f36984a05dacfed231a;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;emilia.nicolson249@asatte.ca;122.176.45.228;;
13.6.2017
14:12;564bdcead4ac2f36984a05dacfed231a;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;kathleen.woods409@dolcevitagallery.com;220.227.61.73;;
13.6.2017
14:12;564bdcead4ac2f36984a05dacfed231a;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;rosalie.priestley3691@inventtheworld.com.au;110.224.200.50;;
13.6.2017
14:15;da463e735c031b5bf1dbb459bddaf504;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;clark.macdonald318@2metalloprokat.ru;171.78.247.16;;
13.6.2017 14:16;c8d83d4f228e440c588d41c66d55b0a0;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;jillian.brand924@resral.com;1.23.119.39;;
13.6.2017
14:16;c8d83d4f228e440c588d41c66d55b0a0;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;mauro.hogarth2715@cityplacedental.ca;14.102.40.209;;
13.6.2017 14:19;;;Malicious-URL;;joeatbv@richardahallpc.us;49.140.98.169;;
13.6.2017 14:20;;;Malicious-URL;;organictabletinc.ru;pending+sce68k30medt@xinyu34.com;91.212.89.54;;
13.6.2017 14:21;1c6b7a950890cd19cd1a16e8ac103b4b;JS.Downloader.D;Malware;Malware;Malware;UPEWTHZC.zip;;NoReplyMailbox@commercy.fr;210.18.148.87;;
13.6.2017
14:21;6a3e79450b53caa355e69833e0c5d1a6;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4194583.zip;;NoReplyMailbox@commercy.fr;210.18.148.87;;
13.6.2017
14:21;6a3e79450b53caa355e69833e0c5d1a6;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0409147.zip;;NoReplyMailbox@luxetrade.com.br;37.139.119.8;;
13.6.2017 14:21;7a4d19bc2ef9639885bbb935b5b27c67;JS.Downloader.D;Malware;Malware;Malware;UPEWTHZC.wsf;;NoReplyMailbox@commercy.fr;210.18.148.87;;
13.6.2017 14:22;04c172bfbac82af21fed30fe4fac5bb;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;araceli.wayles97@infoshade.com;103.24.85.135;;
13.6.2017 14:23;f5082e000fc1e3bc4a20d28e912edbf2;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;alden.maberley29@chatri.com.au;109.66.130.135;;
13.6.2017 14:23;f5082e000fc1e3bc4a20d28e912edbf2;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;helena.dyneley624@marlatenn.ca;109.66.130.135;;
13.6.2017 14:24;633aff60408fd82be6e7e57498262618;JS.Downloader.D;Malware;Malware;Malware;QEYT4WAH.wsf;;NoReplyMailbox@knulle.me;116.74.28.79;;
13.6.2017 14:24;6ff23a9d1d8c87bea411fa8ba23cb85d;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0100713.zip;;NoReplyMailbox@knulle.me;116.74.28.79;;
13.6.2017 14:24;cabceea7b0dca01653baf3dba57cdf;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;ebony.morse324@boulderdj.com;103.211.60.211;;
13.6.2017 14:24;e3d2978c445328c57c6443d2624b4cd7;JS.Downloader.D;Malware;Malware;Malware;QEYT4WAH.zip;;NoReplyMailbox@knulle.me;116.74.28.79;;
13.6.2017 14:26;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS7659805.zip;;NoReplyMailbox@at-network.net;154.103.186.242;;
13.6.2017
14:26;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS5117817.zip;;NoReplyMailbox@dominicdesbiens.com;171.50.142.209
;;
13.6.2017
14:26;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2272860.zip;;NoReplyMailbox@mqsu.org;220.158.152.159;;
13.6.2017 14:26;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4201962.zip;;NoReplyMailbox@promid.hr;43.239.55.12;;
13.6.2017 14:26;aeb05ae24cd38d17e542a552d2d90516;JS.Downloader.D;Malware;Malware;Malware;HDOBYKDTN.wsf;;NoReplyMailbox@at-network.net;154.103.186.242;;
13.6.2017 14:26;b50dd608f79907800ad7d74aaaf51b1b;JS.Downloader.D;Malware;Malware;Malware;HDOBYKDTN.zip;;NoReplyMailbox@at-network.net;154.103.186.242;;
13.6.2017 14:26;;;Malicious-URL;;medicalrxreward.ru;notification+qwcqhdoinnav@aggiemathtutor.com;104.131.44.207;;
13.6.2017 14:27;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2531768.zip;;NoReplyMailbox@espace-danse.ch;41.72.195.174;;
13.6.2017 14:27;;;Malicious-URL;;seosboat.org;;
13.6.2017 14:28;09dab227d2903f83492bd245fbd1d1af;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;minerva.prince65@ssi.ir;45.119.31.145;;
13.6.2017
14:28;23551ea1f235961ed349ee402f877133;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8968808.zip;;NoReplyMailbox@propertyservices.co.nz;95.107.172.88;;
13.6.2017
14:28;23551ea1f235961ed349ee402f877133;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1482966.zip;;NoReplyMailbox@rockypointland4sale.com;89.34.72.30;;
13.6.2017
14:28;23551ea1f235961ed349ee402f877133;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3130040.zip;;NoReplyMailbox@swiftandnine.com;212.156.246.174;
;;
13.6.2017
14:28;5f12666968fd7785aad604c8f3dc85d;JS.Downloader.D;Malware;Malware;Malware;XO3AX3TVI.wsf;;NoReplyMailbox@swiftandnine.com;212.156.246.174;;
13.6.2017
14:28;d6fef5d59f29326acc1c50937c2c9a2a;JS.Downloader.D;Malware;Malware;Malware;XO3AX3TVI.zip;;NoReplyMailbox@swiftandnine.com;212.156.246.174;;
13.6.2017
14:29;23551ea1f235961ed349ee402f877133;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS7974066.zip;;NoReplyMailbox@cartis.hu;59.153.232.171;;
13.6.2017
14:29;23551ea1f235961ed349ee402f877133;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2329210.zip;;NoReplyMailbox@cleanwell.com.br;113.190.166.199;;
13.6.2017
14:29;23551ea1f235961ed349ee402f877133;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0047302.zip;;NoReplyMailbox@cranberrycat.com;59.98.231.77;;
13.6.2017
14:29;23551ea1f235961ed349ee402f877133;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4350565.zip;;NoReplyMailbox@evrostrans.gr;31.50.138.67;;
13.6.2017
14:29;72f9bdd50fee1d6fea9f085e60ac4a7a;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1354119.zip;;NoReplyMailbox@ghouserroofing.co.uk;106.51.110.190;
;;
13.6.2017
14:29;72f9bdd50fee1d6fea9f085e60ac4a7a;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1837342.zip;;NoReplyMailbox@visionbapatia.com;113.161.224.4;;
13.6.2017 14:29;;;Malicious-URL;;Medicalrxreward.ru;alert@utahrealestatgirl.com;94.102.220.126;;
13.6.2017 14:29;;;Malicious-URL;;Medicalrxreward.ru;notification+ec2q7ayqze5n@canoncm.com;192.254.175.47;;
13.6.2017
14:30;5cc983086eb5f2a42e5a204706bbc7ab;JS.Downloader.D;Malware;Malware;Malware;P7BXFHZE.zip;;NoReplyMailbox@newhomestore.com.au;58.65.241.74;;
13.6.2017
14:30;72f9bdd50fee1d6fea9f085e60ac4a7a;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9081836.zip;;NoReplyMailbox@christmasdramas.net;212.156.145.14
;;

13.6.2017
14:30;ad6081dfe138adf32ad1fd58d22d576;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0580162.zip;;NoReplyMailbox@newhomestore.com.au;58.65.241.74;;
13.6.2017
14:30;c34962c46579f1a2f12835bf30df2beb;JS.Downloader.D;Malware;Malware;Malware;P7BFXHZE.wsf;;NoReplyMailbox@newhomestore.com.au;58.65.241.74;;
13.6.2017 14:31;ad6081dfe138adf32ad1fd58d22d576;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9450218.zip;;NoReplyMailbox@agro-magazin.com;103.7.52.254;;
13.6.2017
14:33;05c9427d2790bc8a1edb48e627ac4a62;JS.Downloader.D;Malware;Malware;Malware;C8DTJJCH.wsf;;NoReplyMailbox@hamamotodds.com;62.149.99.133;;
13.6.2017
14:33;8283bb5278c5cbb5aa699fcb31cb3d6d;JS.Downloader.D;Malware;Malware;Malware;C8DTJJCH.zip;;NoReplyMailbox@hamamotodds.com;62.149.99.133;;
13.6.2017
14:33;9f23ac2196aa71baa4e21b03c680fc1;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8212316.zip;;NoReplyMailbox@hamamotodds.com;62.149.99.133;;
13.6.2017 14:36;663d84c35044d1ebdba0e6d4ccb30cec;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;angie.bardesley09@animart.com.il;103.208.152.11;;
13.6.2017 14:43;4a15f97fcdcf1b06c8ce3a9c8e399906;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;melva.danson251@javelin-studio.com;117.218.235.82;;
13.6.2017 14:43;4a15f97fcdcf1b06c8ce3a9c8e399906;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;shad.torre1153@funkyparrot.com;171.49.169.140;;
13.6.2017
14:43;5d8a8b3b47305e2efc57887c63f5e006;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;consuelo.macansh95@philsgiftsandmore.com;103.81.153.130;;
13.6.2017 14:43;5d8a8b3b47305e2efc57887c63f5e006;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;isreal.hindmach1752@royalrich.com;59.95.145.153;;
13.6.2017 14:43;5d8a8b3b47305e2efc57887c63f5e006;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;lauren.kennett2891@lindsaywebb.com;196.1.211.26;;
13.6.2017 14:43;5d8a8b3b47305e2efc57887c63f5e006;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;rogielo.sanford66@rjball.com;87.116.181.69;;
13.6.2017
14:44;5d8a8b3b47305e2efc57887c63f5e006;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;abdul.r392@customactionsports.com;113.190.153.172;;
13.6.2017
14:44;5d8a8b3b47305e2efc57887c63f5e006;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;lavanone.breaker249@mishramusic.com;180.211.170.78;;
13.6.2017
14:44;5d8a8b3b47305e2efc57887c63f5e006;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;raleigh.depledge20@howard6.worldonline.co.uk;14.102.56.62;;
13.6.2017
14:45;3055a7d2593b2e73d536eebc37a2cd20;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;audra.bartlett84@upratovianietepovanie.sk;182.65.78.42;;
13.6.2017 14:50;5d8a8b3b47305e2efc57887c63f5e006;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;marcy.erin15@elwesa.ch;182.65.76.195;;
13.6.2017 14:55;4d0f3d7b436c6864960984195dc92140;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;alana.cafferty5256@inharmony.sk;110.225.193.89;;
13.6.2017 14:55;4d0f3d7b436c6864960984195dc92140;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;inez.whiley04@mcmetalsfe.com;122.172.95.236;;
13.6.2017
14:56;4d0f3d7b436c6864960984195dc92140;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;angelina.priestman0182@flightsafaris.com;117.242.60.70;;
13.6.2017 14:56;4d0f3d7b436c6864960984195dc92140;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;burton.dechair2022@lobbyplanet.eu;122.174.16.241;;
13.6.2017
14:56;66531df14dd8ae2c9ce56da8ebdd8c29;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;ester.brokenbrow564@giftsplus.co.uk;171.49.206.203;;
13.6.2017 14:56;66531df14dd8ae2c9ce56da8ebdd8c29;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;fletcher.verner69@theyovcercadio.com;14.167.96.101;;
13.6.2017
15:05;c8d83d4f228e440c588d41c66d55b0a0;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;palmer.manning5814@mulhollandprep.com;182.72.71.34;;
13.6.2017 15:06;ab91313525f86b2d1aa5d4e0aef09f9;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;casey.kennedy4834@profi-car.com.tw;116.96.10.168;;
13.6.2017 15:06;ab91313525f86b2d1aa5d4e0aef09f9;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;concepcion.nessen90@mitchelhll.com;178.135.82.3;;
13.6.2017 15:06;ab91313525f86b2d1aa5d4e0aef09f9;W2KM_DLOADR.LRN;Malware;Malware;Malware;nm.zip;;josephine.watt09@depatton.com.br;203.160.60.114;;
13.6.2017
15:07;2f9951ed2aec0691a8bd5ec9bf066d56;JS.Downloader.D;Malware;Malware;Malware;TYBREMBWZ.wsf;;NoReplyMailbox@ciofocusgroups.org;2.180.0.240;;
13.6.2017 15:07;ac1bf3b18025cb1eba9bcff48af744cc;JS.Downloader.D;Malware;Malware;Malware;TYBREMBWZ.zip;;NoReplyMailbox@ciofocusgroups.org;2.180.0.240;;
13.6.2017
15:07;e482d1b09b3d53019471700cacc9f2a;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1591518.zip;;NoReplyMailbox@ciofocusgroups.org;2.180.0.240;;
13.6.2017
15:08;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS5907322.zip;;NoReplyMailbox@bbshuochi.com;27.74.240.52;;
13.6.2017
15:08;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8916561.zip;;NoReplyMailbox@eorsl.com;183.81.110.106;;
13.6.2017
15:08;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS322422.zip;;NoReplyMailbox@faisdodomontresor.com;113.184.6.254;;
13.6.2017
15:08;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS6492330.zip;;NoReplyMailbox@spiertzfoto.nl;116.110.52.57;;
13.6.2017
15:08;229e7a340ee0877afcf20afef7de2aa9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9365634.zip;;NoReplyMailbox@triess.screaming.net;112.196.40.45;;
13.6.2017
15:09;29d32f82d0b3a9925e29e796c57dba53;JS.Downloader.D;Malware;Malware;Malware;TBD2OWG6.zip;;NoReplyMailbox@chekkosgroup.com;62.201.253.32;;
13.6.2017
15:09;40c4a338bce54f60658d56b4a888b96;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3770349.zip;;NoReplyMailbox@chekkosgroup.com;62.201.253.32;;
13.6.2017 15:09;40c4a338bce54f60658d56b4a888b96;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS5307835.zip;;NoReplyMailbox@idee-harting.de;5.200.78.110;;
13.6.2017 15:09;40c4a338bce54f60658d56b4a888b96;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0013137.zip;;NoReplyMailbox@pda-bs.com;117.206.6.49;;
13.6.2017
15:09;40c4a338bce54f60658d56b4a888b96;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1153198.zip;;NoReplyMailbox@poosaintpoos.com.au;45.127.229.86;;
13.6.2017
15:09;40c4a338bce54f60658d56b4a888b96;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1267521.zip;;NoReplyMailbox@scutifer.com;14.174.40.209;;
13.6.2017
15:10;40c4a338bce54f60658d56b4a888b96;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4889261.zip;;NoReplyMailbox@trestique.com;223.186.174.4;;
13.6.2017
15:12;598c8c6daed0fceb8e9af3a5ef08de6;JS.Downloader.D;Malware;Malware;Malware;D7UNHE8C.wsf;;NoReplyMailbox@kingsleyaccommodationlongford.com.au;17.176.113.139;;
13.6.2017
15:12;ac9ebed621028c84cd107103a29b7fb4;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2028525.zip;;NoReplyMailbox@kingsleyaccommodationlongford.com.au;171.76.113.139;;
13.6.2017
15:12;b3df6f5e0ff9dc4b05488f45a6c0f8;JS.Downloader.D;Malware;Malware;Malware;D7UNHE8C.zip;;NoReplyMailbox@kingsleyaccommodationlongford.com.au;171.76.113.139;;
13.6.2017
15:15;3695dfcad25b4991e168ce62ae6910c9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2059338.zip;;NoReplyMailbox@forrestdmd.com;197.237.225.55;;
13.6.2017
15:15;3695dfcad25b4991e168ce62ae6910c9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4912894.zip;;NoReplyMailbox@ozvardarli.com;190.186.174.118;;
13.6.2017
15:15;3ddcc06fdff7b8a5e39fe7051bc0de;JS.Downloader.D;Malware;Malware;Malware;GSQX8YX2H.zip;;NoReplyMailbox@forrestdmd.com;197.237.225.55;;
13.6.2017
15:15;cf678344191ec6a5329fd11fdc62ef1;JS.Downloader.D;Malware;Malware;Malware;GSQX8YX2H.wsf;;NoReplyMailbox@forrestdmd.com;197.237.225.55;;
13.6.2017 15:16;04734fe0df46bb7e3982e2274cc9a125;JS.Downloader.D;Malware;Malware;Malware;nm.zip;;charlene.carnaghan84@lot-dot.com;175.107.37.184;;
13.6.2017
15:16;893fc32645577666d43cd12d3fd9bd75;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0779730.zip;;NoReplyMailbox@joaquin.es;103.66.79.180;;
13.6.2017
15:16;893fc32645577666d43cd12d3fd9bd75;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS7639084.zip;;NoReplyMailbox@outersurfaces.com;103.66.79.180;;

13.6.2017
15:16;893fc3264557766d43cd12d3fd9bd75;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3456476.zip;;NoReplyMailbox@tennesseetrading.co.uk;103.198.30.106;;
13.6.2017 15:17;04734fe0df46bb7e3982e2274cc9a125;JS.Downloader.D;Malware;Malware;Malware;nm.zip;;erin.lanthis630@laportadellavallee.com;1.54.214.70;;
13.6.2017 15:17;893fc3264557766d43cd12d3fd9bd75;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS876263.zip;;NoReplyMailbox@quality-media.com;154.118.137.14;;
13.6.2017
15:18;8f21e2d49ead1e0a533c962351ca8d95;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8686522.zip;;NoReplyMailbox@visureitalia.com;66.255.45.242;;
13.6.2017 15:18;d3f1838f1f225e94318f54f03fb7703a;JS.Downloader.D;Malware;Malware;Malware;Y1XG17LK8.zip;;NoReplyMailbox@visureitalia.com;66.255.45.242;;
13.6.2017 15:21;9f032ddf5fb26721f8048dfb4f27e35f;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0936554.zip;;NoReplyMailbox@blz.nl;41.72.105.114;;
13.6.2017
15:21;9f032ddf5fb26721f8048dfb4f27e35f;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1687438.zip;;NoReplyMailbox@studiodentisticofazzari.it;197.2.220.80
;;
13.6.2017 15:22;2bc702e552990c90ecd3a1f2f8d399e1;JS.Downloader.D;Malware;Malware;Malware;ORIPSM5D.zip;;NoReplyMailbox@vjdrewwdown.com;187.50.25.154;;
13.6.2017
15:22;f1ebdf4790e24e49d9d42eb239f1756;JS.Downloader.D;Malware;Malware;Malware;ORIPSM5D.wsf;;NoReplyMailbox@vjdrewwdown.com;187.50.25.154;;
13.6.2017
15:22;f2d2a7043b8738bb40756723c432a4c;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9298544.zip;;NoReplyMailbox@spquicksifters.com;77.242.21.133;
;
13.6.2017
15:22;f2d2a7043b8738bb40756723c432a4c;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS7093799.zip;;NoReplyMailbox@vjdrewwdown.com;187.50.25.154;;
13.6.2017 15:23;;Malicious-URL;Malicious-URL;;;xurl.es;m.yarilen2017@yandex.ru;112.82.136.196;;
13.6.2017
15:25;272e3b9382b2e5c9f800a4595235853e;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0569750.zip;;NoReplyMailbox@fit4all.dk;115.117.169.42;;
13.6.2017
15:25;272e3b9382b2e5c9f800a4595235853e;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2924743.zip;;NoReplyMailbox@weblogskin.com;113.184.16.73;;
13.6.2017
15:26;64efb45941286a88c1cc1781220169e9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3392600.zip;;NoReplyMailbox@andriajenningslscw.com;182.68.160.126;;
13.6.2017
15:26;64efb45941286a88c1cc1781220169e9;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3020323.zip;;NoReplyMailbox@decorjardin.fr;58.187.68.117;;
13.6.2017
15:26;a0078ce44e16e34b767b17e28cb20d43;JS.Downloader.D;Malware;Malware;Malware;ALNAL74Z.wsf;;NoReplyMailbox@andriajenningslscw.com;182.68.160.126;;
13.6.2017
15:26;a3e4b2c32a6b0c8fb737476ab048db;JS.Downloader.D;Malware;Malware;Malware;ALNAL74Z.zip;;NoReplyMailbox@andriajenningslscw.com;182.68.160.126;;
13.6.2017
15:27;5c891973b0274edfcb99e17ed17e8b51;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1602691.zip;;NoReplyMailbox@lareauassur.com;182.71.126.254;;
13.6.2017
15:27;5c891973b0274edfcb99e17ed17e8b51;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2329348.zip;;NoReplyMailbox@savagebrands.com;124.6.175.230;;
13.6.2017 15:27;5c891973b0274edfcb99e17ed17e8b51;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2841120.zip;;NoReplyMailbox@stefany.ca;95.76.3.152;;
13.6.2017 15:27;9ecc9cf18092964e1241bba94a3fe4cd;JS.Downloader.D;Malware;Malware;Malware;PT1ADNV2.zip;;NoReplyMailbox@stefany.ca;95.76.3.152;;
13.6.2017 15:27;dcdc532ff549c5c10c11430cbf6767cdf;JS.Downloader.D;Malware;Malware;Malware;PT1ADNV2.wsf;;NoReplyMailbox@stefany.ca;95.76.3.152;;
13.6.2017
15:28;5c891973b0274edfcb99e17ed17e8b51;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8414456.zip;;NoReplyMailbox@englishplusonline.com;39.43.242.12
3;;
13.6.2017 15:28;;Malicious-URL;Malicious-URL;;;ynlanta.cn;fcprzovhseir@safco.us;71.93.119.214;;
13.6.2017 15:28;;Malicious-URL;Malicious-URL;;;ynlanta.cn;svimf@pecan-grove.us;71.93.119.214;;
13.6.2017 15:29;;Malicious-URL;Malicious-URL;;;InvoicePIS0409185.zip;organictabletinc.ru;alert@weknowwhatswhat.com;NoReplyMailbox@wclscs.com;5.35.252.189;;
13.6.2017 15:30;50b78aa0919375659c8c0ee10e062453;JS.Downloader.D;Malware;Malware;Malware;OEOWNGE.zip;;NoReplyMailbox@wclscs.com;103.79.248.121;;
13.6.2017 15:30;73675b8db1d3d44b54abb508e3018d47;JS.Downloader.D;Malware;Malware;Malware;OEOWNGE.wsf;;NoReplyMailbox@wclscs.com;103.79.248.121;;
13.6.2017
15:30;a2e6ca9d86fad627cf76092638020dfa;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0643236.zip;;NoReplyMailbox@mollygreacen.com;117.253.148.46;;
13.6.2017
15:30;c68fab7f75c520bd5ab475ea8ced2669;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0409185.zip;;NoReplyMailbox@wclscs.com;103.79.248.121;;
13.6.2017 15:32;;Malicious-URL;Malicious-URL;;;ynlanta.cn;gieghbaehxbswe@cucpus.k12.va.us;49.128.62.220;;
13.6.2017 15:32;;Malicious-URL;Malicious-URL;;;ynlanta.cn;xfcnbjvd@kentasmith.us;49.128.62.220;;
13.6.2017 15:33;a1e68fea7f09b973d4d272363b1c0d7f;JS.Downloader.D;Malware;Malware;Malware;FTOZTYGDZ.wsf;;NoReplyMailbox@ircdette.com;103.83.136.2;;
13.6.2017
15:33;c09440d3b4dc70a4edf35cfb2c88b05b;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4865205.zip;;NoReplyMailbox@danninc.com;122.161.41.194;;
13.6.2017
15:33;c09440d3b4dc70a4edf35cfb2c88b05b;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1122825.zip;;NoReplyMailbox@dishinoutbeauty.com;115.79.53.225;
;;
13.6.2017
15:33;c09440d3b4dc70a4edf35cfb2c88b05b;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8664716.zip;;NoReplyMailbox@ircdette.com;103.83.136.2;;
13.6.2017
15:33;c09440d3b4dc70a4edf35cfb2c88b05b;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS6261415.zip;;NoReplyMailbox@limohirefirm.co.uk;103.194.249.18;;
13.6.2017 15:33;e3368c8660cc0a7dc54eaea5f4d0c3f5;JS.Downloader.D;Malware;Malware;Malware;FTOZTYGDZ.zip;;NoReplyMailbox@ircdette.com;103.83.136.2;;
13.6.2017 15:33;;Malicious-URL;;;stamptoy.com;;;
13.6.2017
15:39;c09440d3b4dc70a4edf35cfb2c88b05b;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS6339180.zip;;NoReplyMailbox@triggerthecode.com;197.242.114.83;
;;
13.6.2017
15:39;c09440d3b4dc70a4edf35cfb2c88b05b;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS2458280.zip;;NoReplyMailbox@jenniferhaven.com;113.163.156.176;;
13.6.2017 15:42;;Malicious-URL;Malicious-URL;;;medicalexquality.su;notification+bn0wm5rqgvmc@taylormadeforage.com;195.170.168.40;;
13.6.2017 15:50;506e945149d6dc46e0c08472f6e633c2;JS.Downloader.D;Malware;Malware;Malware;XLCR7AAD.wsf;;NoReplyMailbox@sep-as.eu;182.69.166.135;;
13.6.2017 15:50;7ebd2107ee57adb080c99e427a952a7d;JS.Downloader.D;Malware;Malware;Malware;XLCR7AAD.zip;;NoReplyMailbox@sep-as.eu;182.69.166.135;;
13.6.2017 15:50;9895519ea08f59f1264479767d9620e2;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS5022953.zip;;NoReplyMailbox@sep-as.eu;182.69.166.135;;
13.6.2017
15:50;9895519ea08f59f1264479767d9620e2;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS6799299.zip;;NoReplyMailbox@thesportszone.hrcxmail.com;122.1
67.139.145;;
13.6.2017
15:52;1a90715ce3b554c4f2449ef14dd6773;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1540064.zip;;NoReplyMailbox@beano.worldonline.co.uk;5.22.127.1
92;;
13.6.2017
15:52;9ae772c8d48e34625885ffe3f6a7e3a1;JS.Downloader.D;Malware;Malware;Malware;XE65AKHGN.wsf;;NoReplyMailbox@beano.worldonline.co.uk;5.22.127.192;;
13.6.2017
15:52;f43453915bb87148b3026dd1364960ee;JS.Downloader.D;Malware;Malware;Malware;XE65AKHGN.zip;;NoReplyMailbox@beano.worldonline.co.uk;5.22.127.192;;
13.6.2017
15:53;1a90715ce3b554c4f2449ef14dd6773;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS6732179.zip;;NoReplyMailbox@redbankflavour.com;5.22.127.192;;
13.6.2017 15:54;;Malicious-URL;Malicious-URL;;;organictabletinc.ru;alert@sailboatsclassified.com;38.96.175.221;;
13.6.2017
15:56;547c90755df7a589dbeb1380055c9a7;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0556385.zip;;NoReplyMailbox@educacaoambiental.com.br;91.250.
233.129;;
13.6.2017 15:56;562e50795bc3ea7e2dc02cec74b7547c;JS.Downloader.D;Malware;Malware;Malware;IBBGQFVBT.zip;;NoReplyMailbox@opascraft.com;115.78.10.208;;
13.6.2017
15:56;7a5a5c4734584ae87beacef16a7bbb8c;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1520747.zip;;NoReplyMailbox@opascraft.com;115.78.10.208;;
13.6.2017 15:56;a839e0ded87f19ee5d9848c9cee81ea;JS.Downloader.D;Malware;Malware;Malware;IBBGQFVBT.wsf;;NoReplyMailbox@opascraft.com;115.78.10.208;;

13.6.2017
15:56;d83b5847217bd049cfd93ca4069cf;JS.Downloader.D;Malware;Malware;Malware;CDT4B6DU.zip;;NoReplyMailbox@educacaoambiental.com.br;91.250.233.129;
;;
13.6.2017
15:56;ed1d9f3a76c79c51cc0c0697ccdc5050;JS.Downloader.D;Malware;Malware;Malware;CDT4B6DU.wsf;;NoReplyMailbox@educacaoambiental.com.br;91.250.233.129;
;
13.6.2017
15:59;879fd25518cb5a472a75a8c66bd3e9cb;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1916987.zip;;NoReplyMailbox@thejprgroup.com;125.19.204.82;;
13.6.2017
15:59;8c48a996f0b5622349553796b6f9b6ee;JS.Downloader.D;Malware;Malware;Malware;QPS2LWEDV.zip;;NoReplyMailbox@thejprgroup.com;125.19.204.82;;
13.6.2017
15:59;b68492abb290ab39063eeb3f072a507f;JS.Downloader.D;Malware;Malware;Malware;QPS2LWEDV.wsf;;NoReplyMailbox@thejprgroup.com;125.19.204.82;;
13.6.2017
16:02;8869dd9e4aebc708b3e3e71ffb90e065;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4473716.zip;;NoReplyMailbox@globalpbc.com;112.197.0.92;;
13.6.2017 16:02;8869dd9e4aebc708b3e3e71ffb90e065;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS4250701.zip;;NoReplyMailbox@omoe-net.dk;43.224.130.135;;
13.6.2017
16:03;cb16a4deb2bae3a50e64c5eb4b7ea8bd;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3724222.zip;;NoReplyMailbox@thundershop.ro;178.135.39.92;;
13.6.2017 16:03;;Malicious-URL;;ynlanta.cn;dbypaxzdnore@lu.lousd.k12.ca.us;201.53.1.48;;
13.6.2017 16:03;;Malicious-URL;;ynlanta.cn;obfrsatxpayu@hubba.boogers.sf.ca.us;201.53.1.48;;
13.6.2017 16:04;268ba158f6f5473030b44f769120b80c;W2KM_DLOADR.LRN;Malware;Malware;Malware;646541.zip;;Dallas@incofer.com.br;223.190.69.99;;
13.6.2017
16:08;b3ad1e2d94b42b6ad16daf8fde74a262;JS.Downloader.D;Malware;Malware;Malware;TZ8MYYVKB.zip;;NoReplyMailbox@freshersplane.com;103.72.63.38;;
13.6.2017
16:08;d81bb32caccab7c9158b331ae6da4918;JS.Downloader.D;Malware;Malware;Malware;TZ8MYYVKB.wsf;;NoReplyMailbox@freshersplane.com;103.72.63.38;;
13.6.2017
16:08;f74c83148daf9c625237ee26404be078;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3586840.zip;;NoReplyMailbox@freshersplane.com;103.72.63.38;;
13.6.2017
16:09;6cdfaa2aeac6f6138df5c2a5fe477db;JS.Downloader.D;Malware;Malware;Malware;OOJVFMYO2.zip;;NoReplyMailbox@appshopperapp.com;103.48.57.224;;
13.6.2017
16:09;90b334a69b31d18b473dab7cfa44dc6f;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3793287.zip;;NoReplyMailbox@appshopperapp.com;103.48.57.224;
;;
13.6.2017
16:09;d1c5c4341b0323e6701789fa951205d;JS.Downloader.D;Malware;Malware;Malware;OOJVFMYO2.wsf;;NoReplyMailbox@appshopperapp.com;103.48.57.224;;
13.6.2017
16:09;f74c83148daf9c625237ee26404be078;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3363516.zip;;NoReplyMailbox@octopussparklingwines.eu;42.119.142.43;;
13.6.2017
16:10;90b334a69b31d18b473dab7cfa44dc6f;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9349417.zip;;NoReplyMailbox@viralinnature.com;182.75.246.110;;
13.6.2017
16:11;2d0858a652ec18f6bf1b47d8a41c273f;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS6286754.zip;;NoReplyMailbox@ewv.com.br;140.0.10.117;;
13.6.2017 16:11;62151d038b98828d705c01b893b848e;JS.Downloader.D;Malware;Malware;Malware;MCRO7LQ2.wsf;;NoReplyMailbox@ewv.com.br;140.0.10.117;;
13.6.2017 16:11;84d3d8b0147d4eb3bc3cf3b7eae6e7e;JS.Downloader.D;Malware;Malware;Malware;MCRO7LQ2.zip;;NoReplyMailbox@ewv.com.br;140.0.10.117;;
13.6.2017 16:11;9806b33ff347c42880e886c5b971316;JS.Downloader.D;Malware;Malware;Malware;WWHMHTN.zip;;NoReplyMailbox@pioneer-magazine.com.tw;117.220.155.54;;
13.6.2017 16:11;9b07e10aff94428ae06b6b7d8b3ed1bd;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8388128.zip;;NoReplyMailbox@pioneer-magazine.com.tw;117.220.155.54;;
13.6.2017 16:11;f0a812769b8b0e08880fbabeb5bca0c4;JS.Downloader.D;Malware;Malware;Malware;WWHMHTN.wsf;;NoReplyMailbox@pioneer-magazine.com.tw;117.220.155.54;;
13.6.2017 16:15;;Malicious-URL;;extraordines.com;;;
13.6.2017 16:15;;Malicious-URL;;answeresingenesi.com;;;
13.6.2017
16:18;17521c6d57e1c9984059e0013f1ab554;JS.Downloader.D;Malware;Malware;Malware;I3PYNET9.wsf;;NoReplyMailbox@cathywalker.com;14.175.168.133;;
13.6.2017
16:18;881e7f9d3c9cabdfbc921beacfc2aa;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS9146133.zip;;NoReplyMailbox@cathywalker.com;14.175.168.133;;
13.6.2017 16:18;c3ef882575c85621b7d1051081a6585c;JS.Downloader.D;Malware;Malware;Malware;I3PYNET9.zip;;NoReplyMailbox@cathywalker.com;14.175.168.133;;
13.6.2017
16:20;825904775f8223956512cf65bc67d0;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0368977.zip;;NoReplyMailbox@myhome.occxmail.com;42.117.243.32;;
13.6.2017 16:22;;Malicious-URL;;ynlanta.cn;vznetbucoqq@hmsinet.ca;217.61.123.233;;
13.6.2017
16:23;9f23ac2196aa714baa4e21b03c680fc1;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0835335.zip;;NoReplyMailbox@bookaprize.com;150.129.51.46;;
13.6.2017
16:23;9f23ac2196aa714baa4e21b03c680fc1;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0005747.zip;;NoReplyMailbox@mulhollanndprep.com;150.129.51.46;;
;
13.6.2017
16:24;012fd7b27730fac430d414ef7c56acd3;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS6052560.zip;;NoReplyMailbox@ovosjb.com.br;125.99.109.78;;
13.6.2017 16:24;6ce6a87438bef27761ceb89709d0c33;JS.Downloader.D;Malware;Malware;Malware;AHMUMJFE.wsf;;NoReplyMailbox@ovosjb.com.br;125.99.109.78;;
13.6.2017 16:24;a720b206dba750a5df010f8b5c2b9821;JS.Downloader.D;Malware;Malware;Malware;AHMUMJFE.zip;;NoReplyMailbox@ovosjb.com.br;125.99.109.78;;
13.6.2017 16:25;;Malicious-URL;;ynlanta.cn;uajxdoutkqp@hna.honda.com;110.153.16.148;;
13.6.2017 16:26;35d94267a19ed5cd1932c1201418e6ee;JS.Downloader.D;Malware;Malware;Malware;ONXGCEVPV.zip;;NoReplyMailbox@zrl.co.nz;128.65.180.23;;
13.6.2017 16:26;cb0d25cc4514ef94227c8532309a2ff1;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS7439850.zip;;NoReplyMailbox@zrl.co.nz;128.65.180.23;;
13.6.2017 16:26;d25f019673c9b6626c59a09eadd798e;JS.Downloader.D;Malware;Malware;Malware;ONXGCEVPV.wsf;;NoReplyMailbox@zrl.co.nz;128.65.180.23;;
13.6.2017 16:26;;Malicious-URL;;basedbusinesstraffic.com;voraisai2@gmail.com;116.213.38.138;;
13.6.2017 16:27;63e7872444bfab7cd61f8c1edbbba3442;JS.Downloader.D;Malware;Malware;Malware;XGKLAQFT.wsf;;NoReplyMailbox@ffsolutions.com;31.206.239.177;;
13.6.2017 16:27;78e41b717f9c60223063b84833ec3249;JS.Downloader.D;Malware;Malware;Malware;XGKLAQFT.zip;;NoReplyMailbox@ffsolutions.com;31.206.239.177;;
13.6.2017
16:27;c1dd874eb8ba7d3b5bc9830a0e879470;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS0152639.zip;;NoReplyMailbox@ffsolutions.com;31.206.239.177;;
13.6.2017
16:28;c1dd874eb8ba7d3b5bc9830a0e879470;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS7209918.zip;;NoReplyMailbox@allinsportsbar.com;181.124.114.150;;
13.6.2017
16:31;79c66c7da948948819885a0e0eb26455;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1696594.zip;;NoReplyMailbox@glemstaler.com;122.164.182.204;;
13.6.2017
16:31;90dd1450022a08d643261d2a3c1b57f1;JS.Downloader.D;Malware;Malware;Malware;LBHQZGYR.wsf;;NoReplyMailbox@glemstaler.com;122.164.182.204;;
13.6.2017 16:31;db1cedf9b5181e2ce4bd70c4b7f8cef7;JS.Downloader.D;Malware;Malware;Malware;LBHQZGYR.zip;;NoReplyMailbox@glemstaler.com;122.164.182.204;;
13.6.2017 16:31;;Malicious-URL;;stamptoy.com;;;
13.6.2017 16:35;;Malicious-URL;;dolkupo.com;;;
13.6.2017
16:36;6c46d687a4a3289716fe7c0e2283c52c;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS8548067.zip;;NoReplyMailbox@jnconstrucciones.com.pe;185.106.28.98;;
13.6.2017
16:36;6f0a5de7cc3544b173e094995ffaf6bb;JS.Downloader.D;Malware;Malware;Malware;OVUXG7FL.wsf;;NoReplyMailbox@jnconstrucciones.com.pe;185.106.28.98;;
13.6.2017
16:36;76c53f35e29e51145d47c0fd142ffa35;JS.Downloader.D;Malware;Malware;Malware;OVUXG7FL.zip;;NoReplyMailbox@jnconstrucciones.com.pe;185.106.28.98;;
13.6.2017 16:36;;Malicious-URL;;ynlanta.cn;imwln@hmshost.com;88.85.240.60;;
13.6.2017 16:37;;Malicious-URL;;medicemail.com;martinreplyto@mail.com;185.127.18.205;;
13.6.2017 16:54;;Malicious-URL;;medicalrxquality.su;alert@georgianapartments.com;128.199.81.38;;

13.6.2017 16:57;4db2e3e8cd9cf3e08b3e4b0cc5b9a22;W2KM_DLOADR.LRN;Malware;Malware;Malware;710931.zip;;Tricia@hemphammock.net;182.48.78.81;;

13.6.2017 16:57;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@wilnavarro.com;101.79.5.90;;

13.6.2017 16:58;32b0321b6d46051c871bd78f5354d848;W2KM_DLOADR.LRN;Malware;Malware;Malware;2803441.zip;;Daron@agavesweetinc.com;14.186.79.214;;

13.6.2017
17:00;ab90d092278c83645d7d8bc80467596f;JS.Downloader.D;Malware;Malware;Malware;RKQGL24MY.wsf;;NoReplyMailbox@peakenvironmental.net;113.165.166.81;;

13.6.2017
17:00;b46c5edf7f8e86b94f747838433b526e;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS1549997.zip;;NoReplyMailbox@peakenvironmental.net;113.165.166.81;;

13.6.2017
17:00;f7f3946b7a94d0c382bab9270ef841f;JS.Downloader.D;Malware;Malware;Malware;RKQGL24MY.zip;;NoReplyMailbox@peakenvironmental.net;113.165.166.81;;

13.6.2017 17:03;32b0321b6d46051c871bd78f5354d848;W2KM_DLOADR.LRN;Malware;Malware;Malware;419343.zip;;Marguerite@aceservices.info;50.251.57.49;;

13.6.2017 17:04;43dc722a14e4e5fb834f45828bb286e1;W2KM_DLOADR.LRN;Malware;Malware;Malware;865269.zip;;Edmond@davidjacksonp.com;122.172.119.55;;

13.6.2017 17:10;;Malicious-URL;Malicious-URL;;ynlanta.cn;xrnlcogweu@call911.us;24.144.12.233;;

13.6.2017 17:12;;Malicious-URL;Malicious-URL;;ynlanta.cn;tofiqtveggxq@rbli.reno.nv.us;189.62.85.35;;

13.6.2017
17:13;20b80750aac3180611615feeba92b1d;JS.Downloader.D;Malware;Malware;Malware;LGTBUSEF.zip;;NoReplyMailbox@dstaticllc.com;14.231.96.149;;

13.6.2017
17:13;4a3690b180719477f723bedad865a43;JS.Downloader.D;Malware;Malware;Malware;LGTBUSEF.wsf;;NoReplyMailbox@dstaticllc.com;14.231.96.149;;

13.6.2017
17:13;6d952a5c89c0b0ce8d3687fd15f12de;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS3198915.zip;;NoReplyMailbox@dstaticllc.com;14.231.96.149;;

13.6.2017 17:18;9191d73e21029fbc2db4b720aa2451ca;W2KM_DLOADR.LRN;Malware;Malware;Malware;607838.zip;;Joyce@lethalforex.com;113.163.98.134;;

13.6.2017 17:18;;Malicious-URL;;dolkupo.com;;;

13.6.2017 17:18;;Malicious-URL;;stamptoy.com;;;

13.6.2017 17:18;;Malicious-URL;;stamptoy.com;;;

13.6.2017 17:22;beaac74011f1f2d2e18c269add820bd3;W2KM_DLOADR.LRN;Malware;Malware;Malware;266680191.zip;;Eileen@tnprod.com;190.85.70.74;;

13.6.2017 17:22;beaac74011f1f2d2e18c269add820bd3;W2KM_DLOADR.LRN;Malware;Malware;Malware;876061821.zip;;Fermin@elenalnglois.com;50.254.136.30;;

13.6.2017 17:22;beaac74011f1f2d2e18c269add820bd3;W2KM_DLOADR.LRN;Malware;Malware;Malware;75842.zip;;Kristofer@fireskills.co.uk;79.60.230.241;;

13.6.2017 17:22;beaac74011f1f2d2e18c269add820bd3;W2KM_DLOADR.LRN;Malware;Malware;Malware;6576509.zip;;Lacy@firstgear.ca;2.190.206.25;;

13.6.2017 17:29;608c594cb9d9af2f7f7e1db74cd449;JS.Downloader.D;Malware;Malware;Malware;JODUBWOOW.zip;;NoReplyMailbox@newborns.nl;95.0.185.19;;

13.6.2017
17:29;9930466bbc074ac28c463e1f3e768f1;JS.Downloader.D;Malware;Malware;Malware;InvoicePIS7736215.zip;;NoReplyMailbox@newborns.nl;95.0.185.19;;

13.6.2017 17:29;cd8d60b760fc1f0fe88f23904bc133f;JS.Downloader.D;Malware;Malware;Malware;JODUBWOOW.wsf;;NoReplyMailbox@newborns.nl;95.0.185.19;;

13.6.2017 17:39;6e0d5724c614763361efdd0537d8a429;W2KM_DLOADR.LRN;Malware;Malware;Malware;385896984.zip;;Robin@soundaccount.de;103.225.231.42;;

13.6.2017 17:39;8f21e2d49ead1e0a533c962351ca8d95;JS.Downloader.D;;Malware;InvoicePIS4166737.zip;;NoReplyMailbox@pcdr.nl;202.158.125.242;;

13.6.2017 17:40;8957a31dc7e49005cf51e5ff4de80e45;W2KM_DLOADR.LRN;Malware;Malware;Malware;871599418.zip;;Bertram@dzw.com.ve;41.251.101.136;;

13.6.2017 17:45;;Malicious-URL;Malicious-URL;;ynlanta.cn;oukgkud@wayland.ma.us;177.142.172.74;;

13.6.2017 17:46;;Malicious-URL;Malicious-URL;;yotmail.net;team@fullcontactmail.com;168.245.54.5;;

13.6.2017 17:53;0976a49ef2078497ba2a8b172b4b2ff3;W2KM_DLOADR.LRN;Malware;Malware;Malware;09170102.zip;;Phil@futuremax.eu;223.186.247.242;;

13.6.2017 17:55;22ac99f30b8d0bfae0b1590ce271f1cf;W2KM_DLOADR.LRN;Malware;Malware;Malware;779150398.zip;;Ophelia@profpaintsupply.com;113.22.97.91;;

13.6.2017 18:16;;Malicious-URL;Malicious-URL;;organicaretrade.ru;ueyrqi@02138mag.com;119.4.172.243;;

13.6.2017 18:19;;Malicious-URL;Malicious-URL;;organicaretrade.ru;ilvsjpa@021fy.com;39.84.164.9;;

13.6.2017
18:34;c1dd874eb8ba7d3b5bc9830a0e879470;JS.Downloader.D;Malware;;Malware;InvoicePIS6774383.zip;;NoReplyMailbox@brigadebrigade.com;2.191.115.57;;

13.6.2017 18:47;;Malicious-URL;;brandtsdusky.com;;;

13.6.2017 19:01;;Malicious-URL;;mercedez@intelisell.com;147.135.204.185;;

13.6.2017 19:20;;Malicious-URL;Malicious-URL;;ynlanta.cn;emvhtjp@maxtrans.us;71.80.161.95;;

13.6.2017 19:21;;Malicious-URL;Malicious-URL;;ynlanta.cn;awuzuzax@crivitz.k12.wi.us;71.80.161.95;;

13.6.2017 19:40;;Malicious-URL;Malicious-URL;;marrytags.de;;;

13.6.2017 19:55;;Malicious-URL;;dolkupo.com;;;

13.6.2017 19:58;;Malicious-URL;Malicious-URL;;ynlanta.cn;qnyvbejrezeqm@edgy.us;201.37.51.249;;

13.6.2017 20:07;;Malicious-URL;Malicious-URL;;ynlanta.cn;Abramson_Harry@globescope.us;177.182.144.133;;

13.6.2017 20:07;;Malicious-URL;Malicious-URL;;ynlanta.cn;vefnzwcw@park6.k12.wy.us;177.182.144.133;;

13.6.2017 20:25;;Malicious-URL;;cierra@homeeii.com;147.135.184.142;;

13.6.2017 20:26;;Malicious-URL;;cierra@homeeii.com;147.135.184.142;;

13.6.2017 20:33;;Malicious-URL;Malicious-URL;;ynlanta.cn;ardymj@espl.lib.va.us;179.218.190.181;;

13.6.2017 20:34;;Malicious-URL;Malicious-URL;;ynlanta.cn;smjibbzwsb@woe.us;179.218.190.181;;

13.6.2017 21:00;2f1b8f1ae112f3382cda66e7624d1b50;JS_NEMU.B2B35B1C;Malware;Malicious-URL;Malware;62861.zip, 14148.zip;;larion.zitsbank@cygate.fi;171.35.168.15;;

13.6.2017 21:03;;Malicious-URL;Malicious-URL;;medicalrxquality.su;alert@axsignpro.com;5.35.246.85;;

13.6.2017 21:06;;Malicious-URL;Malicious-URL;;ynlanta.cn;zuwpgs@hmsheridan.co.uk;217.61.123.233;;

13.6.2017 21:07;;Malicious-URL;;brandtsdusky.com;;;

13.6.2017 21:10;;Malicious-URL;;martinreplyto@mail.com;185.127.18.205;;

13.6.2017 21:15;;Malicious-URL;Malicious-URL;;ynlanta.cn;gutmxx@asd.k12.pa.us;187.106.97.17;;

13.6.2017 21:21;;Malicious-URL;Malicious-URL;;organictabletinc.ru;notification+jcw3b73cero3@allmentoseuoven.com;153.122.50.188;;

13.6.2017 21:24;;Malicious-URL;Malicious-URL;;ynlanta.cn;uknmjxohjh@hms.ru;80.249.187.178;;

13.6.2017 21:33;;Malicious-URL;Malicious-URL;;medicalrxquality.su;notification+00zwnbsqbt@thewoodlandprocession.com;101.78.134.142;;

13.6.2017 21:36;;Malicious-URL;Malicious-URL;;medicalrxquality.su;pending+zves8q7xv7jo@highwayministriesinternational.com;92.39.247.251;;

13.6.2017 21:41;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;alert@rajutgrosir.com;178.20.155.246;;

13.6.2017 21:41;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@sanfordbpicou.com;219.99.166.55;;

13.6.2017 21:43;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;update+ccxmdenyg5dr@backtothefuturenaturally.com;91.221.71.204;;

13.6.2017 21:49;;Malicious-URL;Malicious-URL;;shipcorporation.org;info@aarambh.org;103.71.155.17;;

13.6.2017 21:55;;Malicious-URL;Malicious-URL;;medicalrxreward.ru;update+xeimb04enpbo@laserskinspecialist.com;223.223.216.35;;

13.6.2017 21:55;;Malicious-URL;Malicious-URL;;marrytags.de;;;

13.6.2017 22:00;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@virologo.com;108.175.9.78;;

13.6.2017 22:09;;Malicious-URL;Malicious-URL;;ynlanta.cn;cpfhgmckhtw@fcsinc.us;46.29.197.6;;

13.6.2017 22:09;;Malicious-URL;Malicious-URL;;ynlanta.cn;mtycw@edapt.us;46.29.197.6;;

13.6.2017 22:14;;Malicious-URL;Malicious-URL;;ynlanta.cn;cwuaejgch@hmsnt.com;42.81.36.152;;

13.6.2017 22:23;;Malicious-URL;Malicious-URL;;ynlanta.cn;Kennett_Casey@cardamom.us;189.122.128.62;;

13.6.2017 22:30;;Malicious-URL;Malicious-URL;;organictabletinc.ru;alert@averagebrand.com;208.86.184.80;;

13.6.2017 22:53;;Malicious-URL;Malicious-URL;;ynlanta.cn;Lamberts_Elliot@ftcollinsco.us;179.232.135.227;;

13.6.2017 22:54;;Malicious-URL;Malicious-URL;;ynlanta.cn;wmeadvibettoa@concertchoir.us;179.232.135.227;;

13.6.2017 23:08;;Malicious-URL;Malicious-URL;;homesmartreward.ru;noreplay@butterflyemirates.org;74.208.184.52;;

13.6.2017 23:09;;Malicious-URL;Malicious-URL;;onlinesmartale.com;nflbjw@hmsoldies.org.uk;151.253.17.60;;

13.6.2017 23:10;;Malicious-URL;Malicious-URL;;marrytags.de;;;

13.6.2017 23:15;;Malicious-URL;Malicious-URL;;ynlanta.cn;302303262477810.HR13117@ivk.hmf-ft.de;177.220.252.30;;

13.6.2017 23:18;;Malicious-URL;Malicious-URL;;ynlanta.cn;vjijiq@dacum.us;177.142.72.98;;

13.6.2017 23:23;;Malicious-URL;Malicious-URL;;ynlanta.cn;dredrydgh@althani.us;94.158.70.11;;

13.6.2017 23:33;;Malicious-URL;Malicious-URL;;marrytags.de;;;

13.6.2017 23:37;;Malicious-URL;Malicious-URL;;marrytags.de;;;

13.6.2017 23:46;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@yeniegitimplatformu.org;212.204.251.1;;

14.6.2017 0:14;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@muhezahospicecare.org;47.90.90.103;;

14.6.2017 0:17;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@pennstatenation.org;141.138.137.115;;

14.6.2017 0:29;;Malicious-URL;Malicious-URL;;marrytags.de;;;

14.6.2017 0:36;;Malicious-URL;Malicious-URL;;ynlanta.cn;zteziitc@dress-queen.us;71.86.91.221;;

14.6.2017 0:54;;Malicious-URL;Malicious-URL;;marrytags.de;;;

14.6.2017 0:57;03b4b61fd541908ce06d6bf8a0db7d85;JS_NEMU.B2B35B1C;Malware;;Malware;395276701.zip, 27683.zip;;petri.kahkonen@cygate.fi;117.255.236.30;;

14.6.2017 1:02;;Malicious-URL;Malicious-URL;;homesmartreward.ru;noreplay@nowknow.org;85.25.210.227;;

14.6.2017 1:04;;Malicious-URL;Malicious-URL;;ynlanta.cn;fhzknxlvwtj@monet.k12.ca.us;186.220.166.185;;

14.6.2017 1:04;;Malicious-URL;Malicious-URL;;;ynlanta.cn;xqbfqsr@clpccd.cc.ca.us;186.220.166.185;;
 14.6.2017 1:05;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@bulldogsandfriendsfoundation.org;194.88.246.107;;
 14.6.2017 1:08;;Malicious-URL;Malicious-URL;;;marrytags.de;;;
 14.6.2017 1:17;;Malicious-URL;Malicious-URL;;;marrytags.de;;;
 14.6.2017 1:34;;Malicious-URL;Malicious-URL;;;serp-booster.com;hennjohn6@gmail.com;222.97.39.119;;
 14.6.2017 1:40;;Malicious-URL;Malicious-URL;;;ynlanta.cn;mzbmywweyof@holidayshores.us;201.53.21.45;;
 14.6.2017 1:41;;Malicious-URL;Malicious-URL;;;ynlanta.cn;agsdvlrhkccf@mail.liberty.k12.mo.us;201.53.21.45;;
 14.6.2017 1:42;;Malicious-URL;Malicious-URL;;;ynlanta.cn;ayiwjmr@desperado.us;75.82.169.169;;
 14.6.2017 1:59;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@weloveaustralian.org;194.58.88.57;;
 14.6.2017 2:01;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@cardboardcreatures.org;212.67.205.154;;
 14.6.2017 2:03;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@simonacarini.org;5.9.156.20;;
 14.6.2017 2:03;;Malicious-URL;Malicious-URL;;;homesmartreward.ru;noreplay@ukrainianbiodiesel.org;103.254.12.53;;
 14.6.2017 2:03;;Malicious-URL;;;mtgros.net;;;
 14.6.2017 2:06;;Malicious-URL;Malicious-URL;;;ynlanta.cn;uhgug@hmshost.com.au;42.81.36.152;;
 14.6.2017 2:31;;Malicious-URL;Malicious-URL;;;marrytags.de;;;
 14.6.2017 2:34;;Malicious-URL;Malicious-URL;;;marrytags.de;;;
 14.6.2017 3:40;;Malicious-URL;Malicious-URL;;;marrytags.de;;;
 14.6.2017 3:45;;Malicious-URL;Malicious-URL;;;marrytags.de;;;
 14.6.2017 3:57;;Malicious-URL;Malicious-URL;;;marrytags.de;;;
 14.6.2017 4:05;;Malicious-URL;;;date-best.ru;;;
 14.6.2017 4:06;;Malicious-URL;Malicious-URL;;;ynlanta.cn;idxctadp@fbusd.us;92.240.248.118;;
 14.6.2017 4:28;;Malicious-URL;;;supports@patriciamjewels.com;177.237.165.217;;
 14.6.2017 4:43;;Malicious-URL;;;hxxp://kotelnaja.tepp.ru/administrator/components/com_content/views/featured/tmp/sitemap.html;supports@patriciamjewels.com;31.47.38.194;;
 14.6.2017 4:56;;Malicious-URL;Malicious-URL;;;ynlanta.cn;Mercer_Grover@villas-direct.us;37.46.168.3;;
 14.6.2017 5:30;;Malicious-URL;Malicious-URL;;;ynlanta.cn;wppagjaghvoyz@moviezone.us;118.150.24.227;;
 14.6.2017 5:53;;Malicious-URL;Malicious-URL;;;rbkyi.com;;;
 14.6.2017 6:05;;Malicious-URL;Malicious-URL;;;ynlanta.cn;gfhdtzappdtgxt@ci.aberdeen.ms.us;82.192.229.63;;
 14.6.2017 6:05;;Malicious-URL;Malicious-URL;;;ynlanta.cn;vdnieszwersc@pams.us;82.192.229.63;;
 14.6.2017 6:14;;Malicious-URL;Malicious-URL;;;rbkyi.com;;;
 14.6.2017 6:19;;Malicious-URL;Malicious-URL;;;rbkyi.com;;;
 14.6.2017 6:20;;Malicious-URL;Malicious-URL;;;rbkyi.com;;;
 14.6.2017 6:21;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;178.32.60.137;;
 14.6.2017 6:38;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;51.254.238.130;;
 14.6.2017 6:40;;Malicious-URL;;;lovelvbag.com;;;
 14.6.2017 6:43;;Malicious-URL;Malicious-URL;;;rbkyi.com;raybanerx@iujer.top;123.207.246.203;;
 14.6.2017 6:43;;Malicious-URL;;;nordiskhandelsplads.dk;;;
 14.6.2017 6:59;;Malicious-URL;Malicious-URL;;;rbkyi.com;raybanerx@iujer.top;123.207.97.150;;
 14.6.2017 7:02;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;51.255.15.239;;
 14.6.2017 7:04;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@worldrealestatecouncil.org;175.107.196.94;;
 14.6.2017 7:06;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@beautifulnationproject.org;221.132.35.150;;
 14.6.2017 7:15;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@cellbraries.org;213.192.5.26;;
 14.6.2017 7:21;;Malicious-URL;Malicious-URL;;;ynlanta.cn;;;
 14.6.2017 7:22;;Malicious-URL;Malicious-URL;;;dealydo.com;aspeplbcpij@apnr.us;96.30.234.137;;
 14.6.2017 7:22;;Malicious-URL;Malicious-URL;;;ynlanta.cn;Dutton_Alex@ovsd.us;96.30.234.137;;
 14.6.2017 7:27;;Malicious-URL;Malicious-URL;;;rbkyi.com;raybanerx@iujer.top;123.207.237.22;;
 14.6.2017 8:00;;Malicious-URL;Malicious-URL;;;rbkyi.com;raybanerx@iujer.top;118.89.43.38;;
 14.6.2017 8:00;;Malicious-URL;Malicious-URL;;;rbkyi.com;raybanerx@iujer.top;123.207.227.133;;
 14.6.2017 8:07;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;178.32.51.218;;
 14.6.2017 8:12;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@myoo.org;74.122.152.222;;
 14.6.2017 8:19;;Malicious-URL;;;bcontactscc.com;;;
 14.6.2017 8:34;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;51.254.238.130;;
 14.6.2017 8:47;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;51.255.15.239;;
 14.6.2017 9:01;;Malicious-URL;Malicious-URL;;;express-catalogs.com;;;
 14.6.2017 9:03;;Malicious-URL;;;bcontactscc.com;;;
 14.6.2017 9:10;;Malicious-URL;Malicious-URL;;;ynlanta.cn;heupdibpcv@hmshost.com.au;47.90.4.23;;
 14.6.2017 9:38;;Malicious-URL;Malicious-URL;;;ynlanta.cn;417172072306876.XE45772@peus.hmsinet.ca;189.2.65.120;;
 14.6.2017 9:39;;Malicious-URL;Malicious-URL;;;ynlanta.cn;440382366047064.CS85885@mwbs.hmsinet.ca;91.134.12.89;;
 14.6.2017 9:39;;Malicious-URL;Malicious-URL;;;familierabatnordic.dk;;;
 14.6.2017 9:39;;Malicious-URL;Malicious-URL;;;ynlanta.cn;546802802688674.TJ48055@bwu.hmsmakina.com.tr;91.134.12.89;;
 14.6.2017 9:40;;Malicious-URL;Malicious-URL;;;organiccacetrade.ru;yrxigkyjod@007mundo.com;195.140.195.194;;
 14.6.2017 9:42;;Malicious-URL;Malicious-URL;;;masterlead.info;;;
 14.6.2017 9:43;;Malicious-URL;Malicious-URL;;;ynlanta.cn;pgbjusbpy@hmsh Sheridan.co.uk;178.32.41.88;;
 14.6.2017 9:55;;Malicious-URL;;;contact@thegapinthemiddle.com;185.99.122.29;;
 14.6.2017 9:57;;Malicious-URL;;;bcontactscc.com;;;
 14.6.2017 10:01;;Malicious-URL;;;bcontactscc.com;;;
 14.6.2017 10:05;;Malicious-URL;;;contact@thegapinthemiddle.com;212.16.98.57;;
 14.6.2017 10:07;;Malicious-URL;Malicious-URL;;;xurl.es;4643F5A6AD795675A9ACE55A0E4D6E33@yandex.ru;217.61.123.233;;
 14.6.2017 10:12;;Malicious-URL;Malicious-URL;;;homesmartreward.ru;noreplay@saddleshop.org;95.110.198.220;;
 14.6.2017 10:13;;Malicious-URL;;;fermin@homeeii.com;212.16.98.57;;
 14.6.2017 10:19;;Malicious-URL;Malicious-URL;;;ynlanta.cn;134266085881436.HP25424@siw.hmshost.com.a;49.140.212.37;;
 14.6.2017 10:20;;Malicious-URL;;;petrus.palola@tvtools.fi;194.136.189.84;;
 14.6.2017 10:40;;Malicious-URL;Malicious-URL;;;express-catalogs.com;luke.gripenberg@tvtools.fi;194.136.189.84;;
 14.6.2017 10:45;;Malicious-URL;;;bcontactscc.com;;;
 14.6.2017 10:51;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@medprogenerics.org;62.122.247.86;;
 14.6.2017 10:52;;Malicious-URL;;;bcontactscc.com;;;
 14.6.2017 10:55;;Malicious-URL;;;contact@thegapinthemiddle.com;185.99.122.29;;
 14.6.2017 11:01;;Malicious-URL;Malicious-URL;;;express-catalogs.com;s.mertanen@gerdmans.com;198.2.131.113;;
 14.6.2017 11:05;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;178.32.58.252;;
 14.6.2017 11:06;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;
 14.6.2017 11:16;;Malicious-URL;;;bcontactscc.com;;;
 14.6.2017 11:20;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@michasociety.org;91.121.183.59;;
 14.6.2017 11:22;;Malicious-URL;;;erot@srv.hotadultdate.com;207.154.249.66;;
 14.6.2017 11:24;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@museudaescultura.org;89.253.222.60;;
 14.6.2017 11:28;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@verkehrspsychologie.org;208.67.200.192;;
 14.6.2017 11:41;;Malicious-URL;Malicious-URL;;;homesmartreward.ru;noreplay@inherplace.org;188.112.30.2;;
 14.6.2017 11:41;;Malicious-URL;Malicious-URL;;;scandigogo.com;;;
 14.6.2017 11:47;;Malicious-URL;Malicious-URL;;;homesmartreward.ru;noreplay@bellacitta.org;162.218.115.210;;
 14.6.2017 11:51;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;178.32.58.252;;
 14.6.2017 11:57;;Malicious-URL;Malicious-URL;;;homesmartreward.ru;noreplay@smeandassociates.org;37.153.108.163;;
 14.6.2017 12:02;;Malicious-URL;Malicious-URL;;;express-catalogs.com;;;
 14.6.2017 12:08;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;51.254.238.130;;
 14.6.2017 12:08;;Malicious-URL;Malicious-URL;;;ynlanta.cn;Bawerman_Janet@generalsports.us;177.34.224.202;;
 14.6.2017 12:12;;Malicious-URL;;;bcontactscc.com;;;
 14.6.2017 12:16;;Malicious-URL;Malicious-URL;;;homesmartreward.ru;;;
 14.6.2017 12:16;;Malicious-URL;;;noreplay@haboob.org;35.154.227.205;;
 14.6.2017
 12:22;a8bdf4d947bfc08862a0603dd2791f8e3;Trojan.Pidief;Malware;Malware;Malware;576625422.PDF;ilene.pinnion@brewingvessels.co.uk;117.218.235.247;;

14.6.2017 12:25;6338bd2ac02006a98076cab1783606f8;Trojan.Pidief;Malware;Malware;Malware;757717383.PDF;;Clarice.pole@bothwell-pri.s-lanark.sch.uk;178.153.3.222;;
14.6.2017
12:25;6338bd2ac02006a98076cab1783606f8;Trojan.Pidief;Malware;Malware;Malware;794483104.PDF;;Claudia.meador@stevensonline.org.uk;186.208.147.52;;
14.6.2017 12:25;6338bd2ac02006a98076cab1783606f8;Trojan.Pidief;Malware;Malware;Malware;21370583.PDF;;Debra.nunn@kimsim.me.uk;27.64.127.40;;
14.6.2017 12:25;6338bd2ac02006a98076cab1783606f8;Trojan.Pidief;Malware;Malware;Malware;148945700.PDF;;Ursula.moon@firmusheating.co.uk;106.219.61.71;;
14.6.2017
12:26;567fb5f7f8677fd95314be3c4e49c853;Trojan.Pidief;Malware;Malware;Malware;658353248.PDF;;Douglas.wilson@nostalgiccarhire.co.uk;169.255.161.101;;
14.6.2017
12:26;6338bd2ac02006a98076cab1783606f8;Trojan.Pidief;Malware;Malware;Malware;68146923.PDF;;Arnoldo.z@changethruhypnotherapy.co.uk;113.193.178.19;;
14.6.2017
12:27;567fb5f7f8677fd95314be3c4e49c853;Trojan.Pidief;Malware;Malware;Malware;838662612.PDF;;Matilda.jolly@marksschoolofmotoring.co.uk;79.61.89.109;;
14.6.2017
12:27;567fb5f7f8677fd95314be3c4e49c853;Trojan.Pidief;Malware;Malware;Malware;25585246.PDF;;Myrtle.rawlings@daikaju.globalnet.co.uk;122.174.37.181;;
14.6.2017
12:27;6338bd2ac02006a98076cab1783606f8;Trojan.Pidief;Malware;Malware;Malware;431622733.PDF;;Leticia.ogram@frankwoodcarver.me.uk;117.206.10.137;;
14.6.2017 12:27;934302484d33508e78ff9def4f080b1e;Trojan.Pidief;Malware;Malware;Malware;86083257.PDF;;Ina.winning@liz03.globalnet.co.uk;115.77.116.212;;
14.6.2017 12:28;;Malicious-URL;Malicious-URL;;marrytags.de;admin@marrytags.de;178.32.51.218;;
14.6.2017 12:35;;Malicious-URL;;bcontactscc.com;;;
14.6.2017 12:38;;Malicious-URL;;msqym.com;;;
14.6.2017 12:41;;Malicious-URL;Malicious-URL;;medicemail.com;;;
14.6.2017 12:45;;Malicious-URL;Malicious-URL;;homesmartreward.ru;noreplay@thegamesite.org;103.215.136.16;;
14.6.2017 12:54;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@centroagroalimentaredelcampidano.org;45.64.1.80;;
14.6.2017 12:55;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
14.6.2017 13:02;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@conservationskills.org;95.59.26.63;;
14.6.2017 13:07;;Malicious-URL;Malicious-URL;;marrytags.de;admin@marrytags.de;178.32.51.218;;
14.6.2017
13:11;b61154ed588f7570fc8723e25407cf40;Trojan.Pidief;Malware;Malware;Malware;75696446.PDF;;Doyle.loveless@poetknight.worldonline.co.uk;61.14.230.142;;
14.6.2017 13:11;;Malicious-URL;Malicious-URL;;marrytags.de;admin@marrytags.de;51.255.15.239;;
14.6.2017 13:12;b47365439f6752829199a2eb02c55114;Trojan.Pidief;Malware;Malware;Malware;693218235.PDF;;Audra.morgan@sygmacare.co.uk;14.186.195.63;;
14.6.2017 13:12;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@theliteracycampaign.org;91.221.71.204;;
14.6.2017 13:13;84078ca75de4fbb9d9ed0913b5a038f;Trojan.Pidief;Malware;Malware;Malware;309111517.PDF;;Savannah.hancock@pmltd.co.uk;100.101.9.122;;
14.6.2017 13:14;b61154ed588f7570fc8723e25407cf40;Trojan.Pidief;Malware;Malware;Malware;785684412.PDF;;Maryellen.blauvelt@cozo.co.uk;37.63.191.100;;
14.6.2017 13:15;6dd62179306c0a248a68198375952326;Trojan.Pidief;Malware;Malware;Malware;92153027.PDF;;Vivian.howard@ami.co.uk;114.69.251.82;;
14.6.2017 13:15;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@positivaexperienciaprofessional.org;178.77.103.62;;
14.6.2017 13:20;;Malicious-URL;Malicious-URL;;whssx.cn;admin@boosen.com;218.240.43.184;;
14.6.2017 13:24;;Malicious-URL;;seostead.org;;;
14.6.2017 13:26;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;
14.6.2017 13:33;;Malicious-URL;Malicious-URL;;ynlanta.cn;kbzrpq@nonprofitnet.us;179.210.196.217;;
14.6.2017 13:33;;Malicious-URL;Malicious-URL;;ynlanta.cn;lpgpip@ctu.lib.il.us;179.210.196.217;;
14.6.2017 13:40;;Malicious-URL;;gexinmeng@shanghaizhida.com;222.73.105.170;;
14.6.2017 13:43;;Malicious-URL;Malicious-URL;;ynlanta.cn;npsjnf@hmshtost.com.au;212.52.44.51;;
14.6.2017 13:46;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
14.6.2017 13:47;;Malicious-URL;Malicious-URL;;xurl.es;_____esa.kuusisto@cygate.fi;185.51.215.229;;
14.6.2017 13:51;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
14.6.2017 14:05;;Malicious-URL;Malicious-URL;;homesmartreward.ru;noreplay@ciasvalencia.org;207.38.117.244;;
14.6.2017 14:12;;Malicious-URL;Malicious-URL;;homesmartreward.ru;noreplay@nctraina.org;107.170.175.226;;
14.6.2017 14:13;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@eglenerekesfediyoruz.org;213.165.95.67;;
14.6.2017 14:16;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
14.6.2017 14:17;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@STRAY.com;117.195.239.141;;
14.6.2017 14:19;;Malicious-URL;Malicious-URL;;scandigogo.com;;;
14.6.2017 14:21;;Malicious-URL;Malicious-URL;;ynlanta.cn;kwmlnzuaiwo@hmt.hitachi-metals.com;49.140.172.69;;
14.6.2017 14:21;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
14.6.2017 14:28;;Malicious-URL;Malicious-URL;;ynlanta.cn;fgqhyko@hmtel.com;5.135.114.133;;
14.6.2017 14:31;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
14.6.2017 14:31;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
14.6.2017 14:31;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;
14.6.2017 14:33;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_9427.ZIP, IMG_4892.exe;Otto@hope1032.com.au;103.55.89.125;;
14.6.2017 14:35;d202bd9ac670e0da6dd9857873f41e37;JS.Downloader.D;Malware;Malware;Malware;939295568.ZIP, DOC_4943.zip, untitled.wsf;;Janice.copland@savanoriauk.it;27.7.167.162;;
14.6.2017 14:37;cf410a6beca16fce4fdc7157b5d0cbf4;JS.Downloader.D;Malware;Malware;Malware;51990426.ZIP, DOC_7257.zip, untitled.wsf;;Luis.flannagan@onurozkaya.co.uk;212.126.103.208;;
14.6.2017 14:38;6e8eac5fab99343bbcfead1179c86572;JS.Downloader.D;Malware;Malware;Malware;07086607.ZIP, DOC_6063.zip, untitled.wsf;;Ora.atkinson@crosscountrytrain.co.uk;182.69.59.226;;
14.6.2017 14:38;cf410a6beca16fce4fdc7157b5d0cbf4;JS.Downloader.D;Malware;Malware;Malware;215153358.ZIP;;Leigh.roskellej@gjscales.co.uk;14.162.242.234;;
14.6.2017 14:38;;Malicious-URL;Malicious-URL;;marrytags.de;admin@marrytags.de;178.32.58.252;;
14.6.2017
14:39;6e8eac5fab99343bbcfead1179c86572;JS.Downloader.D;Malware;Malware;Malware;175337654.ZIP;;Dennis.breedlove@rattlejagmorris.org.uk;14.186.138.50;;
14.6.2017 14:39;6e8eac5fab99343bbcfead1179c86572;JS.Downloader.D;Malware;Malware;Malware;11560171.ZIP;;Toni.wade@ticktockfilms.co.uk;203.171.245.214;;
14.6.2017 14:39;92ef18d88c7b24fc663c98eb0d754286;JS.Downloader.D;Malware;Malware;Malware;28104494.ZIP;;Candy.seabroke@interent.co.uk;122.160.37.195;;
14.6.2017 14:39;92ef18d88c7b24fc663c98eb0d754286;JS.Downloader.D;Malware;Malware;Malware;233453178.ZIP, DOC_7176.zip, untitled.wsf;;Norris.thulburn@brandmotor.co.uk;14.140.221.69;;
14.6.2017 14:40;04df5d886c06af38d9883db8e6107a20;JS.Downloader.D;Malware;Malware;Malware;817175254.ZIP, DOC_1320.zip, untitled.wsf;;Josefina.mills@silverarchery.co.uk;103.194.145.46;;
14.6.2017 14:40;92ef18d88c7b24fc663c98eb0d754286;JS.Downloader.D;Malware;Malware;Malware;49892331.ZIP;;Clare.sawers@timesofselah.co.uk;188.124.9.123;;
14.6.2017 14:40;92ef18d88c7b24fc663c98eb0d754286;JS.Downloader.D;Malware;Malware;Malware;930181021.ZIP;;Clayton.haddock@littleafred.co.uk;201.41.69.181;;
14.6.2017 14:40;92ef18d88c7b24fc663c98eb0d754286;JS.Downloader.D;Malware;Malware;Malware;074680856.ZIP;;Dalton.willans@camad.co.uk;123.25.239.60;;
14.6.2017 14:40;92ef18d88c7b24fc663c98eb0d754286;JS.Downloader.D;Malware;Malware;Malware;44536335.ZIP;;Rosa.ratcliff@frametheshot.co.uk;101.61.135.236;;
14.6.2017
14:41;04df5d886c06af38d9883db8e6107a20;JS.Downloader.D;Malware;Malware;Malware;181840180.ZIP;;Margaret.horsburgh@ticktick.co.uk;189.33.205.216;;
14.6.2017 14:41;6980db11dba45834b81c5fd9e6678c95;JS.Downloader.D;Malware;Malware;Malware;09837524.ZIP, DOC_8959.zip, untitled.wsf;;Susan.unicomb@dg-elliott.co.uk;36.255.6.3;;
14.6.2017 14:42;b91897db7bdaf6a100ce1c864dc2c478;JS.Downloader.D;Malware;Malware;Malware;562117768.ZIP;;Henrietta.athy@hindmoor.co.uk;113.184.158.181;;
14.6.2017 14:42;b91897db7bdaf6a100ce1c864dc2c478;JS.Downloader.D;Malware;Malware;Malware;60293510.ZIP, DOC_3633.zip, untitled.wsf;;Ronda.birley@dscleaningsvs.co.uk;103.239.147.129;;
14.6.2017 14:43;51e26587e67ecb0a60ddab27405d2885;JS.Downloader.D;Malware;Malware;Malware;43874515.ZIP, DOC_7844.zip, untitled.wsf;;Althea.perkin@greengrowth.org.uk;182.48.246.24;;
14.6.2017 14:43;;Malicious-URL;;hxxp://app.emailbackend.com/display.php?M=102468514&C=c0e047aba3bf548c87f315dc3d0a95b&S=16338&L=12762&N=6981;bounce@emailbackend.com;185.133.137.34;;
14.6.2017 14:43;;Malicious-URL;;hxxp://app.emailbackend.com/link.php?M=102468514&N=16338&L=10066&F=H;bounce@emailbackend.com;185.133.137.34;;
14.6.2017 14:43;;Malicious-URL;;hxxp://app.emailbackend.com/link.php?M=102468514&N=16338&L=10068&F=H;bounce@emailbackend.com;185.133.137.34;;
14.6.2017 14:43;;Malicious-URL;;hxxp://app.emailbackend.com/link.php?M=102468514&N=16338&L=10069&F=H;bounce@emailbackend.com;185.133.137.34;;
14.6.2017 14:43;;Malicious-URL;;hxxp://app.emailbackend.com/link.php?M=102468514&N=16338&L=10073&F=H;bounce@emailbackend.com;185.133.137.34;;
14.6.2017 14:44;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_5064.ZIP;;Cyrus@baitu3d.com;43.225.249.37;;
14.6.2017 14:44;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_0754.ZIP;;Jame@sorrellhill.com;182.77.72.181;;

14.6.2017 14:44;51e26587e67ecb0a60ddab27405d2885;JS.Downloader.D;Malware;Malware;Malware;74009723.ZIP;;Joann.baillie-hamilton@3am.uk.net;113.179.235.25;;;

14.6.2017
14:44;51e26587e67ecb0a60ddab27405d2885;JS.Downloader.D;Malware;Malware;Malware;62703162.ZIP;;Mohamed.lind@transportdatacollection.co.uk;120.56.198.199
;;;

14.6.2017 14:44;8ef1e0909fa3273ff52915a76d774727;JS.Downloader.D;Malware;Malware;Malware;326310722.ZIP, DOC_6557.zip, untitled.wsf;;Effie.france@in-harrow.co.uk;177.42.41.240;;;

14.6.2017 14:44;;;Malicious-URL;Malicious-URL;;;hotcuringbargain.ru;noreplay@swifttechnologysolutions.org;178.255.99.133;;;

14.6.2017 14:45;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_3147.ZIP;;Silvia@orderbydesign.nl;84.120.2.145;;;

14.6.2017 14:45;8ef1e0909fa3273ff52915a76d774727;JS.Downloader.D;Malware;Malware;Malware;44676870.ZIP;;Ines.womersley@legal-protect-uk.com;14.231.227.101;;;

14.6.2017
14:45;8ef1e0909fa3273ff52915a76d774727;JS.Downloader.D;Malware;Malware;Malware;005559058.ZIP;;Melinda.socket@cambridgecakeboutique.co.uk;212.156.88.25
4;;;

14.6.2017
14:46;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_9577.ZIP;;Gwendolyn@stocktonmarina.com;116.96.87.162;;;

14.6.2017
14:46;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_3144.ZIP;;Imelda@virtuallitigationassistance.com;59.160.209.202;;;

14.6.2017 14:46;da4e848a2f327510d2a41f4e957dfc40;Trojan.Gen.7;Malware;Malware;Malware;421272631.ZIP;;Denis.dumaresq@esbar.co.uk;14.174.50.199;;;

14.6.2017 14:46;da4e848a2f327510d2a41f4e957dfc40;Trojan.Gen.7;Malware;Malware;Malware;686280563.ZIP, DOC_8190.zip, untitled.wsf;;Randell.grieg@countrywaste.co.uk;92.55.80.108;;;

14.6.2017 14:46;f2429e5e80c18be2dceb3bab5ec0b5;JS.Downloader.D;Malware;Malware;Malware;749203978.ZIP, DOC_6537.zip, untitled.wsf;;Blanche.shelor@dotuk.org.uk;177.0.48.239;;;

14.6.2017 14:46;f2429e5e80c18be2dceb3bab5ec0b5;JS.Downloader.D;Malware;Malware;Malware;02264711.ZIP;;Lea.horey@oneproperties.co.uk;177.44.128.115;;;

14.6.2017
14:46;f2429e5e80c18be2dceb3bab5ec0b5;JS.Downloader.D;Malware;Malware;Malware;448162537.ZIP;;Shauna.jackman@eelectronics.co.uk;1.53.53.218;;;

14.6.2017 14:47;f2429e5e80c18be2dceb3bab5ec0b5;JS.Downloader.D;Malware;Malware;Malware;02311322.ZIP;;Chet.fitzhugh@driving-instructor-training.co.uk;179.189.245.98;;;

14.6.2017
14:47;f2429e5e80c18be2dceb3bab5ec0b5;JS.Downloader.D;Malware;Malware;Malware;108667987.ZIP;;Robert.oxley@phoenixstamps.co.uk;46.224.87.178;;;

14.6.2017
14:48;64a8dd221125aef13092d5bec64c4e1;JS.Downloader.D;Malware;Malware;Malware;DOC_6829.zip;;Rowena.stelzriede@ajservicesukltd.co.uk;182.70.144.163;;;

14.6.2017
14:48;78a48b8d86a30c4299a74f11427c6f01;JS.Downloader.D;Malware;Malware;Malware;42317115.ZIP;;Rowena.stelzriede@ajservicesukltd.co.uk;182.70.144.163;;;

14.6.2017
14:48;b8449deec24736fa2b089428084766d5;JS.Downloader.D;Malware;Malware;Malware;untitled.wsf;;Rowena.stelzriede@ajservicesukltd.co.uk;182.70.144.163;;;

14.6.2017 14:48;ca3b307abb3f152a14d09028d49dc63e;JS.Downloader.D;Malware;Malware;Malware;49551509.ZIP, DOC_8359.zip, untitled.wsf;;Darla.d@hsaward.me.uk;187.163.121.90;;;

14.6.2017
14:49;ca3b307abb3f152a14d09028d49dc63e;JS.Downloader.D;Malware;Malware;Malware;03358778.ZIP;;Evangelina.montgomery@permonth.co.uk;116.68.105.54;;;

14.6.2017
14:49;ca3b307abb3f152a14d09028d49dc63e;JS.Downloader.D;Malware;Malware;Malware;85202262.ZIP;;June.northing@andrewrothwell.co.uk;39.45.171.179;;;

14.6.2017 14:49;ca3b307abb3f152a14d09028d49dc63e;JS.Downloader.D;Malware;Malware;Malware;221692430.ZIP;;Tara.browne@smallmercies.co.uk;103.66.179.10;;;

14.6.2017 14:49;;;Malicious-URL;Malicious-URL;;;marrytags.de;admin@marrytags.de;178.32.60.137;;;

14.6.2017 14:49;;;Malicious-URL;Malicious-URL;;;organicaretrade.ru;buypwkt@01com.com;221.201.250.161;;;

14.6.2017 14:50;b367000076debd25cbf3b2cce590c29b;JS.Downloader.D;Malware;Malware;Malware;282023644.ZIP, DOC_5726.zip, untitled.wsf;;Dena.loveridge@arenicola.co.uk;200.116.6.84;;;

14.6.2017 14:50;b367000076debd25cbf3b2cce590c29b;JS.Downloader.D;Malware;Malware;Malware;231011952.ZIP;;Gabrielle.vaux@estasia.co.uk;103.255.4.5;;;

14.6.2017
14:50;b367000076debd25cbf3b2cce590c29b;JS.Downloader.D;Malware;Malware;Malware;914800944.ZIP;;Milagros.athy@babyshowerstore.co.uk;115.160.246.186;;;

14.6.2017 14:50;fc0110e47f131366c4a4e011131fe55b;JS.Downloader.D;Malware;Malware;Malware;535114715.ZIP, DOC_5779.zip, untitled.wsf;;Karyn.bryden@wingmangroup.co.uk;37.111.129.112;;;

14.6.2017 14:50;;;Malicious-URL;Malicious-URL;;;organicaretrade.ru;ftbxqupuoz@01930.com;112.193.130.116;;;

14.6.2017 14:51;582c421fddb96d030fb7fb646f3f4cce;JS.Downloader.D;Malware;Malware;Malware;99256348.ZIP, DOC_8531.zip, untitled.wsf;;Shane.wills@prinswillem-alexander.surrey.sch.uk;113.20.116.34;;;

14.6.2017
14:51;b367000076debd25cbf3b2cce590c29b;JS.Downloader.D;Malware;Malware;Malware;95888565.ZIP;;Asa.russell@therevitalizesanctuary.co.uk;117.223.54.28;;;

14.6.2017
14:51;b367000076debd25cbf3b2cce590c29b;JS.Downloader.D;Malware;Malware;Malware;864066365.ZIP;;Ezra.rutherford@yorkgolfshop.co.uk;42.112.156.235;;;

14.6.2017 14:51;b367000076debd25cbf3b2cce590c29b;JS.Downloader.D;Malware;Malware;Malware;36428623.ZIP;;Regina.rawlyns@gasfm.co.uk;123.18.55.195;;;

14.6.2017 14:51;;;Malicious-URL;Malicious-URL;;;organicaretrade.ru;hbiiolyh@0161.com;182.91.28.93;;;

14.6.2017 14:52;582c421fddb96d030fb7fb646f3f4cce;JS.Downloader.D;Malware;Malware;Malware;52520254.ZIP;;Felecia.janes@carnaubawaxshop.co.uk;2.34.176.39;;;

14.6.2017
14:52;582c421fddb96d030fb7fb646f3f4cce;JS.Downloader.D;Malware;Malware;Malware;081746124.ZIP;;Michel.johnson@paintexpress.co.uk;117.248.199.128;;;

14.6.2017 14:52;582c421fddb96d030fb7fb646f3f4cce;JS.Downloader.D;Malware;Malware;Malware;591310862.ZIP;;Patricia.marquis@hdlaw.co.uk;59.95.84.69;;;

14.6.2017 14:52;582c421fddb96d030fb7fb646f3f4cce;JS.Downloader.D;Malware;Malware;Malware;766525699.ZIP;;Roslyn.ross@tessadoc.org.uk;203.210.197.203;;;

14.6.2017 14:52;582c421fddb96d030fb7fb646f3f4cce;JS.Downloader.D;Malware;Malware;Malware;85972531.ZIP;;Selena.bookter@alexanderart.co.uk;95.38.223.241;;;

14.6.2017 14:53;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_7598.ZIP;;Adalberto@mspiveyonline.com;200.87.18.74;;;

14.6.2017 14:53;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_7417.ZIP;;Emilia@bbe-online.net;14.165.51.27;;;

14.6.2017 14:53;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_7964.ZIP;;Phillip@barlowfwm.co.uk;79.127.116.61;;;

14.6.2017 14:53;c421ebd53f00317a7f70090ea21c1600;JS.Downloader.D;Malware;Malware;Malware;880396157.ZIP, DOC_7710.zip, untitled.wsf;;Zack.wittick@blacksmiths1753.co.uk;109.245.219.62;;;

14.6.2017
14:53;f2429e5e80c18be2dceb3bab5ec0b5;JS.Downloader.D;Malware;Malware;Malware;433293822.ZIP;;Dewitt.culham@twyford.globalnet.co.uk;220.227.71.226;;;

14.6.2017
14:53;f2429e5e80c18be2dceb3bab5ec0b5;JS.Downloader.D;Malware;Malware;Malware;719224070.ZIP;;Velma.snoddy@roadsafetysurveys.co.uk;59.93.162.96;;;

14.6.2017 14:53;f2429e5e80c18be2dceb3bab5ec0b5;JS.Downloader.D;Malware;Malware;Malware;546134083.ZIP;;Wendy.fenn@unmundo.co.uk;59.99.235.101;;;

14.6.2017 14:54;03b385175d3ca9291791672b99665c95;JS.Downloader.D;Malware;Malware;Malware;289894136.ZIP, DOC_8525.zip, untitled.wsf;;Estelle.wilcock@e-catumk.com;110.227.85.13;;;

14.6.2017
14:54;03b385175d3ca9291791672b99665c95;JS.Downloader.D;Malware;Malware;Malware;06118516.ZIP;;Zane.burwin@fuzzyproduction.co.uk;202.142.158.155;;;

14.6.2017 14:54;c421ebd53f00317a7f70090ea21c1600;JS.Downloader.D;Malware;Malware;Malware;08574385.ZIP;;Adrian.snively@such.co.uk;14.187.195.39;;;

14.6.2017 14:55;03b385175d3ca9291791672b99665c95;JS.Downloader.D;Malware;Malware;Malware;60858237.ZIP;;Ali.skeen@tessystem.co.uk;213.186.90.148;;;

14.6.2017
14:55;03b385175d3ca9291791672b99665c95;JS.Downloader.D;Malware;Malware;Malware;376467894.ZIP;;Liliana.eshelby@zeedometriccleaning.co.uk;103.255.6.76;;;

14.6.2017 14:56;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_5199.ZIP;;Dewey@icgsac.com;190.103.30.142;;;

14.6.2017 14:56;2fa489afb950f5df14eb77471b29ab35;JS.Downloader.D;Malware;Malware;Malware;untitled.wsf, DOC_7309.zip;;Laurie.scholey@wholesalesportswear.co.uk;123.16.54.168;;;

14.6.2017 14:56;f7ee71c0d8c61edc3258c6ca69a72fc1;JS.Downloader.D;Malware;Malware;Malware;51943368.ZIP;;Jane.roebuck@acousticprint.co.uk;117.212.170.68;;;

14.6.2017 14:56;f7ee71c0d8c61edc3258c6ca69a72fc1;JS.Downloader.D;Malware;Malware;Malware;405652125.ZIP;;Jimmie.torrance@grabhire.uk.com;36.37.174.204;;;

14.6.2017 14:56;f7ee71c0d8c61edc3258c6ca69a72fc1;JS.Downloader.D;Malware;Malware;Malware;996489894.ZIP;;Juanita.orton@blazingswords.co.uk;103.251.48.90;;;

14.6.2017 14:56;f7ee71c0d8c61edc3258c6ca69a72fc1;JS.Downloader.D;Malware;Malware;Malware;48117559.ZIP;;Karyn.calkin@paulokane.co.uk;116.109.225.166;;;

14.6.2017
14:56;f7ee71c0d8c61edc3258c6ca69a72fc1;JS.Downloader.D;Malware;Malware;Malware;243690080.ZIP;;Laurie.scholey@wholesalesportswear.co.uk;123.16.54.168;;;

14.6.2017
14:56;f7ee71c0d8c61edc3258c6ca69a72fc1;JS.Downloader.D;Malware;Malware;Malware;08649028.ZIP;;Louella.heyne@kainuunurheilusukeltajat.fi;41.60.233.250;;;

14.6.2017 14:56;;;Malicious-URL;Malicious-URL;;;express-catalogs.com;;;

14.6.2017 14:57;0164ebfe7df812174ce16117f88e4def;JS.Downloader.D;Malware;Malware;Malware;19790604.ZIP, DOC_4519.zip, untitled.wsf;;Elmo.bunger@wilbrahamboilerservices.co.uk;117.241.97.82;;

14.6.2017 14:57;eea2dad208df20568feeffed6fab9e1;JS.Downloader.D;Malware;Malware;Malware;23841148.ZIP, DOC_4664.zip, untitled.wsf;;Brianna.pritchard@donnabrush.co.uk;59.99.16.7;;

14.6.2017

14:57;eea2dad208df20568feeffed6fab9e1;JS.Downloader.D;Malware;Malware;Malware;568704455.ZIP;;Ken.fairbairn@magnolia.globalnet.co.uk;117.200.12.192;;

14.6.2017 14:58;0164ebfe7df812174ce16117f88e4def;JS.Downloader.D;Malware;Malware;Malware;756257607.ZIP, 45869200.zip, untitled.wsf;;Weldon.pearse@thecoachhouse-norfolk.co.uk;45.124.147.81;;

14.6.2017 14:58;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_4198.ZIP;;Milo@kreativdesign-zug.ch;118.71.59.165;;

14.6.2017

14:59;3716944b627a312207d6966f7bb80c4a;JS.Downloader.D;Malware;Malware;Malware;36382491.ZIP;;Ken.gentorgrant@abcchemicals.co.uk;103.203.95.11;;

14.6.2017 14:59;eba655aa38bde5d422f67a60613674a;JS.Downloader.D;Malware;Malware;Malware;DOC_3698.zip;;Jan.norton@relayance.co.uk;41.212.110.117;;

14.6.2017 15:00;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;

14.6.2017 15:03;7def7e1ee509106f8743cd0efd4a1719;JS.Downloader.D;Malware;Malware;Malware;915844397.ZIP, DOC_9558.zip, untitled.wsf;;Pam.gascoigne@bellgrove.co.uk;117.215.226.75;;

14.6.2017 15:03;85d6de0e2e40a7bd38e2234c3eb09d85;JS.Downloader.D;Malware;Malware;Malware;753815803.ZIP, DOC_4362.zip, untitled.wsf;;Lena.chiasson@kinnairdcrosscountry.co.uk;1.22.60.67;;

14.6.2017

15:03;85d6de0e2e40a7bd38e2234c3eb09d85;JS.Downloader.D;Malware;Malware;Malware;693266184.ZIP;;Lorraine.booth@mgurbanism.co.uk;43.227.226.178;;

14.6.2017

15:04;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_4033.ZIP;;Rosalyn@newtelecomunicacoes.com.br;103.44.96.13;;

14.6.2017 15:04;7def7e1ee509106f8743cd0efd4a1719;JS.Downloader.D;Malware;Malware;Malware;341963378.ZIP;;Otha.flight@raphaelplaits.co.uk;117.200.176.135;;

14.6.2017 15:04;7def7e1ee509106f8743cd0efd4a1719;JS.Downloader.D;Malware;Malware;Malware;24650572.ZIP;;Tammy.travis@tomosjones.uk;106.210.222.225;;

14.6.2017 15:05;21a9de0af7c1cab452817c35f8862990;JS.Downloader.D;Malware;Malware;Malware;DOC_3764.zip;;Irma.welsby@themaiks.com;60.243.82.47;;

14.6.2017

15:05;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_0610.ZIP;;Jermaine@innovationaffinity.com;196.214.58.162;;

14.6.2017 15:05;6f9064aa9901a135508e7566e52fc420;JS.Downloader.D;Malware;Malware;Malware;89527364, untitled.wsf;;Irma.welsby@themaiks.com;60.243.82.47;;

14.6.2017 15:05;78a48b8d86a30c4299a74f11427c6f01;JS.Downloader.D;Malware;Malware;Malware;615404903.ZIP;;Jacklyn.moser@dmspm.co.uk;2.177.234.54;;

14.6.2017 15:05;;Malicious-URL;Malicious-URL;;ynlanta.cn;sxcrkxlllmoe@ffguerins.us;65.104.194.251;;

14.6.2017 15:05;;Malicious-URL;Malicious-URL;;ynlanta.cn;wgtiu@markspencer.us;65.104.194.251;;

14.6.2017 15:06;6adf10dbb08540bd784d2aa3cbd01320;JS.Downloader.D;Malware;Malware;Malware;95143140.ZIP, DOC_7678.zip, untitled.wsf;;Benjamin.severs@catchthematch.co.uk;150.107.214.110;;

14.6.2017 15:06;78a48b8d86a30c4299a74f11427c6f01;JS.Downloader.D;Malware;Malware;Malware;71561677.ZIP;;Valentine.beakman@petehickman.co.uk;61.1.70.132;;

14.6.2017 15:07;1854dba1a3a58746bca84f392d257379;JS.Downloader.D;Malware;Malware;Malware;626397239.ZIP;;Geraldo.olds@salmanhukuk.com;154.72.168.0;;

14.6.2017 15:07;1854dba1a3a58746bca84f392d257379;JS.Downloader.D;Malware;Malware;Malware;08702706.ZIP, DOC_4481.zip, untitled.wsf;;Tammie.triplett@stmarybourne.org.uk;46.41.212.191;;

14.6.2017

15:08;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_9573.ZIP;;Jocelyn@undercovermuslimah.com;103.215.194.0;;

14.6.2017 15:08;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_4569.ZIP;;Roxanne@greengrafix.com;103.215.194.0;;

14.6.2017

15:08;f420cf18259a97d67ebd09489d06d1d8;JS.Downloader.D;Malware;Malware;Malware;642856646.ZIP;;Darlene.soothill@showpieceflooring.co.uk;2.177.246.32;;

14.6.2017 15:08;f420cf18259a97d67ebd09489d06d1d8;JS.Downloader.D;Malware;Malware;Malware;652424006.ZIP, DOC_5607.zip, untitled.wsf;;Rochelle.moir@cgltd.co.uk;117.196.160.214;;

14.6.2017 15:09;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_0918.ZIP;;Adela@brookintennis.com.br;105.168.40.191;;

14.6.2017

15:10;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_8300.ZIP;;Jaime@victorybakingservices.com;45.64.221.96;;

14.6.2017 15:10;445bf769ce3f2e452d3222e14f3df857;JS.Downloader.D;Malware;Malware;Malware;99687853.ZIP, DOC_7407.zip, untitled.wsf;;Jesus.adkins@bratzgirlzreallyrock.co.uk;103.249.7.5;;

14.6.2017

15:11;445bf769ce3f2e452d3222e14f3df857;JS.Downloader.D;Malware;Malware;Malware;074497011.ZIP;;Jarrett.thirnbeck@ponyrider.co.uk;113.189.226.199;;

14.6.2017 15:11;;Malicious-URL;Malicious-URL;;amino-disqus.club;;;

14.6.2017 15:12;62cf57b19b0246940005f45434b68104;JS.Downloader.D;Malware;Malware;Malware;813785080.ZIP, DOC_1877.zip, untitled.wsf;;Joy.hensman@johnsonnb.co.uk;195.181.67.0;;

14.6.2017

15:12;62cf57b19b0246940005f45434b68104;JS.Downloader.D;Malware;Malware;Malware;25771582.ZIP;;Kennith.hamblin@northwesthydro.co.uk;181.48.42.234;;

14.6.2017 15:13;78a48b8d86a30c4299a74f11427c6f01;JS.Downloader.D;Malware;Malware;Malware;763978563.ZIP;;King.winner@whsa.co.uk;117.96.0.45;;

14.6.2017

15:13;78a48b8d86a30c4299a74f11427c6f01;JS.Downloader.D;Malware;Malware;Malware;141104918.ZIP;;Marianne.borthwick@client876b.globalnet.co.uk;46.40.40.68;;

;

14.6.2017 15:14;78a48b8d86a30c4299a74f11427c6f01;JS.Downloader.D;Malware;Malware;Malware;447598073.ZIP;;Wayne.prentice@otol.co.uk;89.114.237.172;;

14.6.2017

15:14;78a48b8d86a30c4299a74f11427c6f01;JS.Downloader.D;Malware;Malware;Malware;478363007.ZIP;;Mariana.mcminn@wiltshireclassics.co.uk;116.202.38.65;;

14.6.2017 15:15;1c92ee08c1f68f3f879b7d7d2d138e;JS.Downloader.D;Malware;Malware;Malware;351695357.ZIP, DOC_5234.zip, untitled.wsf;;Yolanda.ellison@theweddingcars.co.uk;118.69.54.89;;

14.6.2017 15:16;82c5e7dd5c54287d9f6f46ce58ce0a5d;JS.Downloader.D;Malware;Malware;Malware;769402968.ZIP, DOC_1137.zip, untitled.wsf;;Beatrice.marksbury@hcmr.co.uk;117.211.40.27;;

14.6.2017 15:17;09423c3f9653a5aafa1fd3d60eb5b7f1;JS.Downloader.D;Malware;Malware;Malware;458601415.ZIP, DOC_3546.zip, untitled.wsf;;Jenny.pearson?@wychwood-treesurgeons.co.uk;154.72.148.34;;

14.6.2017 15:17;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_7333.ZIP;;Julianne@roadsendstudio.com;121.121.84.84;;

14.6.2017 15:17;4e89bf2c0b20fce2c160beddeaccb24;JS.Downloader.D;Malware;Malware;Malware;50153550.ZIP, DOC_2634.zip, untitled.wsf;;Mona.spillane@artofsound.co.uk;113.161.76.186;;

14.6.2017 15:36;;Malicious-URL;Malicious-URL;;ynlanta.cn;524083251154275.RU22255@bjpv.hmt-electric.com;49.140.65.25;;

14.6.2017 15:37;;Malicious-URL;Malicious-URL;;ynlanta.cn;nupqjh@hmt-ffb.de;49.140.65.25;;

14.6.2017 15:38;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_4699.ZIP;;Nelson@airlearn.net;45.65.48.14;;

14.6.2017 15:40;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;

14.6.2017 15:50;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;

14.6.2017 15:51;;Malicious-URL;;bcontactscc.com;;;

14.6.2017 15:52;;Malicious-URL;Malicious-URL;;homesmartreward.ru;noreplay@globalstorming.org;178.62.151.18;;

14.6.2017 15:55;;Malicious-URL;Malicious-URL;;familierabatnordic.dk;;;

14.6.2017 16:06;;Malicious-URL;Malicious-URL;;ynlanta.cn;nainodlm@hmsy.com;59.72.109.47;;

14.6.2017 16:15;;Malicious-URL;Malicious-URL;;composetop.com;bounce-matti.hartikka@cygate.fi@composetop.com;185.176.26.119;;

14.6.2017 16:23;;Malicious-URL;Malicious-URL;;ynlanta.cn;672264516560076.MQ76756@kjl.hmt-electric.com;125.209.91.101;;

14.6.2017 16:29;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@havertownstucco.org;212.26.132.124;;

14.6.2017 16:31;;Malicious-URL;Malicious-URL;;homesmartreward.ru;noreplay@pelivre.org;89.42.193.230;;

14.6.2017 16:35;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_9414.ZIP;;Blair@seamedintl.com;202.164.36.12;;

14.6.2017

16:35;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_6740.ZIP;;Randolph@madeinsanfrancisco.org;171.49.192.250;;

14.6.2017 16:36;;Malicious-URL;Malicious-URL;;medicemail.com;;;

14.6.2017 16:40;;Malicious-URL;;bcontactscc.com;;;

14.6.2017 16:41;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;;Malware;IMG_2487.ZIP;;Darla@lockershield.net;124.124.211.237;;

14.6.2017 16:41;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@memorycaresandiego.org;91.121.21.86;;

14.6.2017 16:43;;Malicious-URL;Malicious-URL;;marrtags.de;admin@marrtags.de;178.32.60.137;;

14.6.2017 16:43;;Malicious-URL;Malicious-URL;;express-catalogs.com;info@versionsnip.com;185.176.27.191;;

14.6.2017 16:51;;Malicious-URL;;info@ds.emailsent2u.com;185.79.21.29;;

14.6.2017 16:54;;Malicious-URL;Malicious-URL;;express-catalogs.com;;;

14.6.2017 16:56;;Malicious-URL;Malicious-URL;;ceubags.com;no-reply@no-reply.vvwns.cc;194.88.107.57;;

14.6.2017 16:59;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_9206.ZIP;;Daphne@spelc22.org;183.81.67.180;;

14.6.2017
17:02;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_6135.ZIP;;Lucas@nigelhopephotography.co.uk;113.160.147.137;;
14.6.2017 17:02;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_6795.ZIP;;Scotty@cyrk.kscocmail.com;132.255.95.21;;
14.6.2017
17:03;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_0537.ZIP;;Sherman@khanglobalacquisitions.com;14.191.119.181;;
14.6.2017 17:03;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_5980.ZIP;;Tanisha@musica.sk;117.247.84.135;;
14.6.2017 17:03;;Malicious-URL;;information@nations-direct.com;217.182.255.160;;
14.6.2017 17:17;;Malicious-URL;Malicious-URL;;composetop.com;info@composetop.com;185.176.26.65;;
14.6.2017 17:17;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;
14.6.2017 17:22;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_1289.ZIP;;jill@cedesma.com;123.28.185.128;;
14.6.2017 17:22;24413d0395fdeb5ea7e9148eed776e73;TROJ_IN.5BD4624C;Malware;Malware;Malware;IMG_6623.ZIP;;Suzanne@knits-n-knacks.com;190.102.81.181;;
14.6.2017 17:25;;Malicious-URL;;sportsavcs.ci;;;
14.6.2017 17:32;;Malicious-URL;Malicious-URL;;sportsavcs.ci;hargroves@jokon.com;113.166.143.83;;
14.6.2017 17:37;;Malicious-URL;Malicious-URL;;medicemail.com;;;
14.6.2017 17:42;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@sydneyhousecleaning.org;185.4.29.216;;
14.6.2017 17:42;;Malicious-URL;;hxxp://malgorzatajablonska.pl/administrator/components/com_joomgallery/temp/update/media/sitemap.html;supports@patrykwalczak.com;37.104.50.224;;
14.6.2017 17:45;;Malicious-URL;Malicious-URL;;hotcuringbargain.ru;noreplay@dontbet.org;212.159.100.201;;
14.6.2017 17:49;;Malicious-URL;;mignonetyyup.com;;;
14.6.2017 17:52;;Malicious-URL;Malicious-URL;;hxxp://sosh8.uoteuch.ru/administrator/components/com_media/views/medialist/tmpl/sitemap.html;supports@patrykwalczak.com;200.48.77.89;;
14.6.2017 17:52;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;
14.6.2017 17:55;;Malicious-URL;Malicious-URL;hxxp://www.neerubajwa.in/wp-content/plugins/879848c0442.html;bufca@ramesystavel.co.uk;14.161.215.121;;
14.6.2017 17:58;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;
14.6.2017 18:02;;Malicious-URL;hxxp://equaldayequalpay.net/file.php?document=cGF1bGUCGFra2FuZW5AY3lnYXRlMmZp;adp@lexalp.com;96.87.245.217;;
14.6.2017 18:05;;Malicious-URL;hxxp://LBCMARKETING.COM/file.php?document=amFya55iYWFybWVhbnVzZmF0Zm5maQ==;adp@lexalp.com;166.171.123.59;;
14.6.2017 18:06;;Malicious-URL;;cricketbasics.com;;;
14.6.2017 18:09;;Malicious-URL;hxxp://www.efstathopouloslaw.gr/wp-includes/js/tinymce/themes/advanced/skins/wp_theme/img/57596d321ed.html;postmaster@mail.reliable-mail.com;72.52.210.40;;
14.6.2017 18:10;;Malicious-URL;Malicious-URL;;marrytags.de;admin@marrytags.de;178.32.58.252;;
14.6.2017 18:10;;Malicious-URL;hxxp://equaldayequalpay.com/file.php?document=YXJpLmhhbG9wYWVlZW5AY3lnYXRlMmZp;adp@lexalp.com;172.76.10.138;;
14.6.2017 18:13;;Malicious-URL;hxxp://LBCMARKETING.COM/file.php?document=YXJ0b3Y5aXVra29uZW5AY3lnYXRlMmZp;adp@lexalp.com;96.92.154.218;;
14.6.2017 18:27;;Malicious-URL;hxxp://DELANEYBAYFUND.ORG/file.php?document=cmVhbnVzZmF0Zm5maQ==;adp@lexalp.com;213.165.187.242;;
14.6.2017 18:28;;Malicious-URL;hxxp://RISINGSTARSTHERAPY.COM/file.php?document=bWlrYWVwLmhhbnVzZmF0Zm5maQ==;adp@lexalp.com;123.209.69.108;;
14.6.2017 18:35;;Malicious-URL;;thedollwarehouse.com;;;
14.6.2017 18:43;;Malicious-URL;Malicious-URL;;marrytags.de;admin@marrytags.de;51.255.15.239;;
14.6.2017 18:44;;Malicious-URL;hxxp://RISINGSTARSTHERAPY.COM/file.php?document=bWF0dGkua2FoaWxhQGN5Z2F0Zm5maQ==;adp@lexalp.com;75.108.63.248;;
14.6.2017 18:44;;Malicious-URL;hxxp://RISINGSTARSTHERAPY.COM/file.php?document=ZWV2Y55aWh2b2hQGN5Z2F0Zm5maQ==;adp@lexalp.com;70.119.253.232;;
14.6.2017 18:48;;Malicious-URL;;neighborhoodhackers.com;;;
14.6.2017 18:56;;Malicious-URL;;thedollwarehouse.com;;;
14.6.2017 18:58;;Malicious-URL;hxxp://LBCMARKETING.COM/file.php?document=bWlrYWVwLmhhbnVzZmF0Zm5maQ==;adp@lexalp.com;73.151.96.48;;
14.6.2017 18:59;;Malicious-URL;Malicious-URL;;sexy-dates.ru;info@WORKBENCH.br;1.54.215.181;;
14.6.2017 19:05;;Malicious-URL;;mignonetyyup.com;;;
14.6.2017 19:06;;Malicious-URL;Malicious-URL;;marrytags.de;admin@marrytags.de;178.32.58.252;;
14.6.2017 19:22;;Malicious-URL;Malicious-URL;;ynlanta.cn;624221455375685.PQ61680@zais.hmsc.harvard.edu;31.168.230.194;;
14.6.2017 19:22;;Malicious-URL;hxxp://uberattitude.com/file.php?document=YXJpLmhhbG9wYWVlZW5AY3lnYXRlMmZp;adp@lexalp.com;174.79.188.175;;
14.6.2017 19:24;;Malicious-URL;;mignonetyyup.com;;;
14.6.2017 19:25;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;
14.6.2017 19:27;;Malicious-URL;hxxp://tequilacapaz.com/file.php?document=am9ha2lLnVzZmF0Zm5maQ==;adp@lexalp.com;96.68.79.181;;
14.6.2017 19:30;;Malicious-URL;hxxp://www.rrrwellness.com/wp-content/themes/retro-fitted/3317cd41f4f.html;postmaster@ah105.wadax.ne.jp;211.1.224.155;;
14.6.2017 19:36;;Malicious-URL;Malicious-URL;;ynlanta.cn;833436580815066.EA70236@xgmv.hmsost.com;195.46.167.164;;
14.6.2017 19:47;;Malicious-URL;Malicious-URL;;ynlanta.cn;mkobpusxib@hmsheridan.co.uk;94.23.173.62;;
14.6.2017 19:53;;Malicious-URL;hxxp://TEQUILACLUBUS.ORG/file.php?document=dmlsbGUuZWVzZmF0Zm5maQ==;adp@lexalp.com;96.89.85.109;;
14.6.2017 20:00;;Malicious-URL;Malicious-URL;hxxp://TEQUILACLUBUS.ORG/file.php?document=bWlrYWVwLmhhbnVzZmF0Zm5maQ==;adp@lexalp.com;75.145.204.62;;
14.6.2017 20:01;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;
14.6.2017 20:10;;Malicious-URL;Malicious-URL;;multi-service.ma;a8b24ccb@avants.net;130.117.169.158;;
14.6.2017 20:16;;Malicious-URL;Malicious-URL;;trumpdpe.com;info@trumpers.com;185.99.122.53;;
14.6.2017 20:23;f7bc2660856d9c3caf7c09d45edde845;Trojan.Maljava;Malware;Malware;Malware;Quotation.jar;;carlo@geshacoffeeco.com;203.113.243.213;;
14.6.2017 20:27;;Malicious-URL;Malicious-URL;hxxp://lyftreviewer.com/file.php?document=YW50dGkua2FubmluZW5AY3lnYXRlMmZp;adp@lexalp.com;64.238.123.54;;
14.6.2017 20:29;;Malicious-URL;Malicious-URL;hxxp://lyftreviewer.com/file.php?document=ZW5zdGkua2VudGFsYUJjeWdhdGUuZmZp;adp@lexalp.com;173.14.192.2;;
14.6.2017 20:30;;Malicious-URL;Malicious-URL;;homesmartreward.ru;noreplay@penmarketing.org;85.236.207.83;;
14.6.2017 20:31;;Malicious-URL;Malicious-URL;hxxp://capaztequila.com/file.php?document=cHVyY2hhc2VAY3lnYXRlMmZp;adp@lexalp.com;70.120.231.127;;
14.6.2017 20:33;;Malicious-URL;Malicious-URL;hxxp://tequilacapaz.com/file.php?document=YW5kZXIzLnRrb2d2dGVyQGN5Z2F0Zm5maQ==;adp@lexalp.com;50.194.165.153;;
14.6.2017 20:35;;Malicious-URL;Malicious-URL;Malicious-URL;amino-disqus.club;;;
14.6.2017 20:35;;Malicious-URL;;tequilaclubus.org;;;
14.6.2017 20:42;;Malicious-URL;Malicious-URL;hxxp://capaztequila.com/file.php?document=c2FtdS52aXJ0YV91vQGN5Z2F0Zm5maQ==;adp@lexalp.com;67.63.231.266;;
14.6.2017 20:54;;Malicious-URL;Malicious-URL;;marrytags.de;admin@marrytags.de;51.254.238.130;;
14.6.2017 20:56;;Malicious-URL;hxxp://lyftreviewer.com/file.php?document=amFybW8uc2lsbGFucGhQGN5Z2F0Zm5maQ==;adp@lexalp.com;174.127.18.90;;