

Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2014

Pekka Koivula & Juho Tuomola

RANSOMWARE- HAITTAOHJELMAT



TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

Kesäkuu 2014 | 88 sivua

Esko Vainikka

Pekka Koivula & Juho Tuomola

RANSOMWARE-HAITTAOHJELMAT

Opinnäytetyön tavoitteena on luoda lukijalle kuva siitä, miten ransomware-haittaohjelmat toimivat, mitkä ovat niiden tekijöiden motiivit ja miten niitä vastaan pystyy suojautumaan. Viimeaikaisten tartuntatapausten perusteella aihe on tällä hetkellä erittäin ajankohtainen ja se koskee sekä yrityksiä että yksityishenkilöitä.

Opinnäytetyön teoriaosuudessa esitellään ransomwaren kehityskaari eri vaiheineen. Osuudessa keskitytään kahteen ransomwaren päätyyppiin eli salaavaan ja ei-salaavaan kiristyshaittaohjelmaan.

Empiirisessä osuudessa käsitellään CryptoLocker-kiristyshaittaohjelman tartuttamista Windows-pohjaiseen järjestelmään. Samalla otetaan selvää kyseisen haittaohjelman toimintatavasta, tartuntakohteista sekä sen mahdollisista kiertämistavoista. Tämän on tarkoitus antaa lukijalle tarkka selvitys CryptoLockerin toimintaperiaatteista.

Lopputuloksena saatiin aikaan työ, jonka tarkoituksena on tarjota ransomwareen liittyvää tietoa sitä tarvitseville.

ASIASANAT:

malware, ransomware, tietoturva

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communication and Information Security

June 2014 | 88 pages

Esko Vainikka

Pekka Koivula & Juho Tuomola

RANSOMWARE MALWARE

The objective of this Bachelor's thesis is to give the reader an overview of the functionality of ransomware, the motives of the authors and the protection against ransomware. The subject is currently very topical because of the recent infection cases and it applies to both companies and individuals.

The theoretical section presents the trajectory of ransomware at its different stages. This section focuses on two main types of ransomware: encrypting and non-encrypting.

The empirical part of the thesis deals with infecting CryptoLocker in a Windows-based system. This part describes the behavior of CryptoLocker, its targets and potential ways to prevent it. This part intends to provide the reader with a detailed explanation of CryptoLocker policies.

As a result, the purpose of this thesis is to increase the awareness of ransomware.

KEYWORDS:

malware, ransomware, information security

SISÄLTÖ

1 JOHDANTO	6
2 RANSOMWARE YLEISESTI	7
2.1 Kehitys	7
2.2 Maksutavat	11
2.3 Suojautuminen	12
2.4 Poistaminen	13
3 LEVINNEISYYS	16
4 TULEVAISUUDENNÄKYMÄT	18
5 RANSOMWAREN TUTKIMINEN SULJETUSSA YMPÄRISTÖSSÄ	20
5.1 Ympäristön käyttöjärjestelmät	21
5.2 Ympäristön ohjelmistot	23
5.3 Kiristyshaittaohjelma – CryptoLocker	25
5.4 Testiympäristön pystyttäminen	26
5.5 CryptoLockerin testaus	33
5.6 CryptoLockerilta suojautuminen	38
6 TYÖN TOTEUTTAMISEN HAASTEET	41
7 POHDINTA	42
LÄHTEET	44

LIITTEET

Liite 1. Wireshark-loki.
Liite 2. Regshot-loki.

KUVAT

Kuva 1. Reveton-poliisiviruksen lunnasvaatimus.	10
---	----

Kuva 2. Käynnistyksen lisäasetukset.	13
Kuva 3. Komentorivi.	14
Kuva 4. Resurssienhallinta.	14
Kuva 5. Julkisen avaimen salaus (Microsoft 2005).	26
Kuva 6. Asennusruutu 1.	27
Kuva 7. Asennusruutu 2.	28
Kuva 8. VMwaren asennus komentoriviltä.	29
Kuva 9. VMwaren kernelin päivitysruutu.	30
Kuva 10. VMware päivittää kernelin moduulia.	30
Kuva 11. Virtuaaliverkkosovittimen valinta.	31
Kuva 12. Virtual Network Editor.	32
Kuva 13. CryptoLockerin kohdetiedostot XP-ympäristössä.	33
Kuva 14. CryptoLockerin luomat tiedostot.	35
Kuva 15. CryptoLockerin saastuttama kone.	36
Kuva 16. CryptoLockerille syötetty keksitty purkukoodi.	37
Kuva 17. Local Security Policy.	38
Kuva 18. Uuden säännön luominen.	39
Kuva 19. Kuvankaappaus osasta Process Monitor -loki.	39
Kuva 20. CryptoLockerin suoritus keskeytyy.	40

KUVIOT

Kuvio 1. Ransomwareen levinneisyys (McAfee Labs 2013b, 19).	17
Kuvio 2. Suunnitelma toteutettavasta testausympäristöstä.	21
Kuvio 3. Windows-käyttöjärjestelmäversioiden markkinaosuus helmikuussa 2014 (NetMarketShare 2014).	22

1 JOHDANTO

Tietoyhteiskunnan kasvu maailmanlaajuisesti yhä suuremmaksi viime vuosina on samalla mahdollistanut haittaohjelmien räjähdysmäisen kasvun. Maailmanlaajuisessa tietoverkossa liikkuu tälläkin hetkellä lukemattomia erilaisia haittaohjelmia, jotka yrittävät löytää potentiaalista kohdetta, johon iskeä.

Viime vuosina ransomware eli kiristyshaittaohjelmat, yksi haittaohjelmien alalajeista, ovat nostaneet itsensä otsikoihin yhä uudestaan. Tällä hetkellä tietoturvasiantuntijat ennustavat tämän olevan vasta alkua jollekin suuremmalle.

Työn teoriaosuudessa selvitetään lukijalle, mikä on ransomware ja minkälaisia muutoksia se tekee kohteeksi joutuneelle tietokoneelle. Tekstissä käsitellään myös lyhyesti ransomwaren historiaa ja levinneisyyttä maailmalla.

Empiriaosuudessa käsitellään CryptoLocker-nimisen kiristyshaittaohjelman toimintaa Windows-pohjaisessa ympäristössä. Haittaohjelmana CryptoLocker on mielenkiintoinen vaihtoehto, koska se on tällä hetkellä yksi yleisimmistä maailmalla liikkuvista salaavista kiristyshaittaohjelmista.

Testauksessa otetaan selvää miten helposti kyseinen haittaohjelma tarttuu tietokoneeseen, mitä muutoksia se tekee tietokoneen tiedostoihin ja onko sen luoma tiedostojen salaus mahdollista kiertää. Tätä varten toteutetaan suljettu testiympäristö, johon tartutetaan tarkoituksella CryptoLocker-haittaohjelma ja samalla seurataan sen tekemiä muutoksia.

Työn lopussa analysoidaan testiympäristöstä saatuja tietoja ja käsitellään opinnäytetyön etenemiseen liittyviä ongelmia.

Opinnäytteen työnjako jaettiin siten, että Juho Tuomola panosti teoriaosuuden kirjoittamiseen, kun taas Pekka Koivula otti enemmän vastuuta empiriaosuuden kirjoittamisesta. Työnjaosta huolimatta molemmat osallistuivat kaikkiin osaluoihin ja CryptoLockerin suljetun ympäristön tutkimus tehtiin yhdessä.

2 RANSOMWARE YLEISESTI

2.1 Kehitys

Ransomware eli kiristyshaittaohjelma on haittaohjelmien alatyyppejä, jonka tarkoitus on estää saastuttamansa tietokoneen käyttö joko kokonaan tai osittain. Nimensä mukaisesti kiristyshaittaohjelma luo lukituksen kohdetietokoneeseen tai vaihtoehtoisesti salaa käyttäjän tärkeitä henkilökohtaisia tiedostoja. Tämän jälkeen haittaohjelma vaatii tietokoneen käyttäjää maksamaan lunnasrahat lukituksen avaamiseksi tai salauksen purkamiseksi.

Suurin osa kiristyshaittaohjelmista on suunniteltu toimimaan Windows-pohjaisissa käyttöjärjestelmissä. On kuitenkin tavattu joitakin varhaisia variaatioita, jotka on suunniteltu esimerkiksi Android-käyttöjärjestelmille.

Kiristyshaittaohjelmien historia ulottuu vuoteen 1989. Silloin ilmestyi PC Cyborg-niminen troijalainen, joka tunnetaan myös nimellä AIDS. Se toimi ainoastaan DOS-käyttöjärjestelmässä. Koska Internet oli tuolloin vielä harvojen käytössä, levitettiin PC Cyborgia kirjeitse. Kirje sisälsi levykkeen, joka oli naamioitu sisältämään AIDS-tietoutta. (Kassner 2010.)

Kun levykkeen sisältämän ohjelman käynnisti, muokkasi se käyttöjärjestelmän käynnistystiedostoja siten, että troijalainen aktivoitui tietokoneen 90 uudelleenkäynnistyskerran jälkeen. Aktivoituessaan troijalainen piilotti kaikki hakemistot ja salasi tiedostojen nimet. Maksamalla satojen dollarien summan troijalaisen kehittäjälle sai koodin, jolla salauksen sai purettua. (Kassner 2010.)

Alkeellisuudestaan huolimatta tätä haittaohjelmaa voidaan pitää ensimmäisenä ransomwarena, vaikkei kyseistä termiä silloin vielä tunnettukaan. PC Cyborg käytti symmetristä kryptografiaa, joten sen salaus oli verrattain helppo purkaa ilman lunnaiden maksamista. (Kassner 2010.)

Kiristyshaittaohjelmat voidaan jakaa karkeasti kahteen eri kategoriaan, joiden yhteinen tekijä on rahan kiristäminen haittaohjelman uhrilta pitämällä tietokonet-

ta tai osaa sen tiedostoista panttivankina. Muilta osilta nämä kaksi erilaista tyyppiä eroavat hyvin paljon toisistaan. Ensimmäinen ransomware PC Cyborg kuuluu ensimmäiseksi esiteltävään kategoriaan eli salaaviin kiristyshaittaohjelmiin. Ensimmäisen suuremman ransomware-aallon haittaohjelmat kuten ns. poliisivirukset kuuluvat toiseksi esiteltävään kategoriaan eli ei-salaaviin kiristyshaittaohjelmiin.

Salaava kiristyshaittaohjelma

Vuonna 1996 julkaistiin tutkielma, jossa esitellään kryptografian käyttöä tehokkaan haittaohjelman luomista varten. Tätä kuvataan tutkielmassa termillä kryptovirologia. Tutkielmassa luotiin ohjelmaprototyyppi, joka käyttää julkisen avaimen kryptografiaa. Tällä tekniikalla luodaan nykyään uusimmat ja hankalimmat salaavat kiristyshaittaohjelmat. (Kassner 2010.)

Salaavan kiristyshaittaohjelman saastuttaessa tietokoneen se salaa käyttäjän henkilökohtaiset tiedostot ja jättää jälkeensä lunnasvaatimuksen, jonka maksamalla käyttäjä saa itsellensä vaihdossa tiedostojen salauksen purkuun tarvittavan salausavaimen. (F-Secure Labs 2013.)

Salaavan kiristyshaittaohjelman pääkohteet ovat erityisesti yritysten heikosti salatut Windows-pohjaiset palvelimet. Tällaisissa tapauksissa sen levittämiseen hyökkääjät käyttävät pääsääntöisesti RDP-protokollaan perustuvaa etätyöpöytäyhteyttä kohteen palvelimeen. Helpon salasanan murtuessa yritys ja erehdys-metodilla hyökkääjä suorittaa haittaohjelman manuaalisesti yrityksen palvelimella, jonka seurauksena kaikki yrityksen sisäverkkoon liitetyt laitteet joutuvat salauksen kohteeksi. (F-Secure Labs 2013.)

Haittaohjelman tarkoituksena on käydä läpi kaikki käyttöjärjestelmän sisältämät tiedostot ja salata haittaohjelmaan määritellyt tiedostotyytit. Kohteiksi päätyvät yleensä esimerkiksi erilaiset tekstit, kuvat, videot tai vaikka tietokantatiedostot. Ideana on kuitenkin, että salattaviksi joutuvat käyttäjälle mahdollisesti korvaamattomat tiedostot. Sen sijaan käyttöjärjestelmän sisältämät järjestelmätiedostot jäävät kokonaan koskematta, koska hyökkääjä haluaa varmistaa yrityksen

tietokoneiden käynnistymisen käyttöjärjestelmään, jotta lunnasvaatimus voidaan esittää. (F-Secure Labs 2013.)

Ottamalla kohteeksi suuria yrityksiä tavallisten kotikäyttäjien sijaan hyökkääjä varmistaa aiheuttaneensa mahdollisimman paljon haittaa kohteelleen. Yrityksen tehdessä huomattavaa taloudellista tappiota ilman pääsyä tarvittaviin asiakirjoihin tai palvelimilla sijaitseviin tietokantoihin, on se huomattavasti potentiaalisempi lunnaiden maksaja kuin yksittäinen henkilö. (F-Secure Labs 2013.)

Ensimmäisiä vaarallisia salaavia kiristyshaittaohjelmia on vuoden 2004 loppupuolella havaittu Gpcode. Sitä levitettiin sähköpostin liitetiedostona ja se oli alun perin kohdistettu venäläisille käyttäjille. Gpcode salaa käyttäjälle tärkeitä tiedostoja ja pyytää lähettämään lunnaita vastineeksi salauksenpurkuohjelmasta, jolla tiedostojen salauksen saa purettua. Tietoturvayhtiö Kaspersky onnistui purkamaan jopa 660 bitin avaimella salatut tiedostot. (Emelyanova & Nazarov 2006.) Uusimmat variantit käyttävät jopa 1024 bitin salausavainta, jolloin salauksen purku on vaikeaa tai lähes mahdotonta (Kaspersky Lab 2008).

Nimekkäin tällä hetkellä liikkuvista salauksen suorittavista kiristyshaittaohjelmista on CryptoLocker. Se on hyvin samankaltainen kuin Gpcode, mutta CryptoLockerissa ei ole tällä hetkellä mitään muuta keinoa pelastaa salattuja tiedostoja kuin maksaa lunnaat. CryptoLocker havaittiin ensimmäisen kerran syyskuussa 2013. Sen jälkeen siitä on ilmestynyt useita eri variantteja hieman erilaisella ulkonäöllä ja toiminnalla. (Abrams 2013.)

Ei-salaava kiristyshaittaohjelma

Nimensä mukaisesti ei-salaava kiristyshaittaohjelma ei suorita salausta saastuneen kohdekoneen tiedostoille vaan sen tarkoituksena on estää koko käyttöjärjestelmän käyttäminen näyttämällä lukitusnäyttöä tietokoneella. Lukitusnäyttö käynnistyy automaattisesti seuraavalla saastumisen jälkeisellä tietokoneen uudelleenkäynnistyskerralla ja valtaa koko työpöydän lunnasvaatimuksellaan. Tässä vaiheessa tietokonetta ei pysty enää käyttämään mihinkään muuhun

toimenpiteeseen, koska ilmoitus on vallannut koko näytön ja sen sulkeminen tavallisin keinoin on mahdotonta. (F-Secure Labs 2013.)

Tällaiset kiristyshaittaohjelmat naamioivat itsensä usein väittämällä olevansa paikallinen poliisiviranomainen. Yleisin näistä on Suomessakin esiintynyt Reveton-niminen kiristyshaittaohjelma, joka on paremmin tunnettu nimellä poliisivirus. Ensimmäiset variantit tästä havaittiin vuonna 2012. (F-Secure Labs 2013.) Reveton-tyyppisiä ransomwareja suosittumaksi on nousemassa Urausy, joka on hyvin samankaltainen kuin Reveton (Ortega 2013).

Haittaohjelman esittämää vaatimusta on lokalisoitu usealle kielelle, myös suomeksi. Viestissä esiintyy viranomaisten käyttämiä logoja. Näillä toimenpiteillä vaatimuksesta on saatu mahdollisimman aidon oloinen. Lunnasvaatimus on naamioitu sakoksi, joka on seurausta tietokoneella tapahtuneista laittomista toimista, kuten tekijänoikeusrikkomuksista tai lapsipornon hallussapidosta (Kuva 1). (F-Secure Labs 2013.)

POLIISI
TIETOVERKKORIKOSTEN TUTKINNAN YKSIKKÖ

HUOMIO!

IP:
Paikkakunta: **Finland , Helsinki**
ISP:

Teidän tietokoneenne on lukittu pois yhden tai muutaman syiden vuoksi. Ne syyt ovat seuraavia.

Te olette riikkoneet Tekijänoikeus- ja lähioikeuslain (Video, Musiikki, Ohjelmisto) ja olette käyttäneet laittomasti ja/tai olette levittäneet tekijänoikeuksilla suojattua sisältöä (Content), sillä olette riikkoneet Suomen Rikoslain kohdan 128.

Rikoslainkohdan 128 mukaan edellyttään sakkoo **2-500** minimipalkkojan määrässä tai vapaunrangastusta **2 vuodesta - 8 vuoteen.**

Te olette katsoneet tai levittäneet kiellettyä pornografista sisältöä (Content) (Child Porno / Zoofilia ja jne). Sillä olette riikkoneet Suomen Rikoslain kohdan 202.

Rikoslainkohdan 202 mukaan edellyttään vapaunrangastusta **4 vuodesta - 12 vuoteen.**

Teidän tietokoneestänne on tehnyt laittoman pääsyn tietokoneen tietoihin (Datan) tai Te olette

Rikoslainkohdan 208 mukaan edellyttään sakkoo jopa **100.000** Euroa määrässä ja/tai vapaunrangastusta **4 vuodesta - 9 vuoteen.**

Teidän tietokoneestänne on tehnyt laittoman pääsyn ilman käyttäjän tietoa. On mahdollista että teidän tietokoneenne on tarttunut haittaohjelmia, sillä Te rikotte Parjamentietokonekäytön lain.

Rikoslainkohdan 210 mukaan edellyttään sakkoo **2000** Eurosta **8000** Euroon määrässä.

Teidän tietokoneestänne tehtiin roskapostin - lähettäminen (Spam - lähettäminen) tai muun laittoman mainonnan toiminta tekemisen liikevoiton tarkoituksella, tai tietämättänne. On mahdollista että teidän tietokoneenne on tarttunut haittaohjelmia.

Rikoslainkohdan 212 mukaan edellyttään sakkoo jopa **250.000 Euroa** määrässä ja vapaunrangastusta **6 vuoteen.** Jos edellä mainittu toiminta suoritettiin ilman Teidän tietoa, Te kuulutte edellä mainittuun Suomen Rikoslain 210 lainkohtaan.

Videotallennus
ON

paysafecard

Koodi: Summa:
100

1 2 3 4 5 6 7 8 9 0

Maksaa PaySafeCard

Mistä voin ostaa Paysafecard??

Voit ostaa paysafecard-kortteja maailmanlaajuisesti yli 350.000 myyntipisteestä. Suomessa paysafecard-kortteja myyvät kaikki R-Kioskit.

R-KIOSKI

Kuva 1. Reveton-poliisiviruksen lunnasvaatimus.

Tämäntyyppiset kiristyshaittaohjelmat ovat huomattavasti yleisempiä tavallisilla kotikoneilla, koska niiden tarkoitus on estää tietokoneen käyttö kokonaan. Tämä on tavalliselle kotikäyttäjälle yleensä vakavampi asia kuin yksittäisten tiedostojen käytön estäminen. Leviäminen tapahtuu tavanomaisesti sähköpostin liitetiedostojen tai ladattujen tiedostojen välityksellä. Leviäminen voi myös tapahtua Internet-selaimen avulla tietokoneen vierailtua saastuneella web-palvelimella, jonka kautta haittaohjelma käynnistää itsensä tietokoneelle. (F-Secure Labs 2013.)

Leviämisen mahdollistaa esimerkiksi Blackhole- tai Cool EK exploit kit -hyväksikäyttöalusta. Nämä hyödyntävät haavoittuvuuksia Javassa, Flash Playerissa tai Internet-selaimessa asentaakseen haittaohjelman käyttäjän tietokoneeseen. (Ortega 2013.)

2.2 Maksutavat

Ransomwaren tarkoituksena on tuottaa rahaa levittäjälleen laittomin keinoin, mistä syystä lunnasrahojen siirtoon on kiinnitetty erityistä huomiota koko ransomwaren elinkaaren aikana. Koska rahaliikenne halutaan pitää mahdollisimman salaisena levittäjän puolelta, on maksutapoja kehitetty useita kertoja kohti mahdollisimman anonyymia ratkaisua.

Ensimmäisenä varsinaisena maksutapana toimivat pankkien väliset tilisiirrot sekä maksulliset tekstiviestit eli niin sanotut premium-rate-SMS-viestit. Kuitenkin näiden helpon jäljitettävyyden takia maksutavaksi muuttui pian esimerkiksi Ukashin ja Paysafecardin tarjoamat etukäteen ostetut maksukupongit.

Viime aikoina vakiintuneeksi maksutavaksi on tullut kryptovaluutta Bitcoin. Bitcoin perustuu avoimen lähdekoodin protokollaan, jonka takana ei ole mikään tietty virallinen taho. Vaikka Bitcoin-siirrot eri tilien välillä ovat julkisia, ei Bitcoin-verkossa liiku ollenkaan henkilötietoja eikä rahansiirtoa valvo mikään keskitetty instituutio.

Ensimmäiset kiristyshaittaohjelmien vaatimat lunnassummat olivat 100 dollarin luokkaa, mutta vakiintuivat nopeasti 300 dollarin tasolle. Bitcoinin tullessa maksuvaihtoehtoksi ovat lunnassummat vaihdelleet huomattavasti Bitcoinin kurssin vaihdellessa jopa satoja dollareita päivässä. Tällä hetkellä lunnasvaatimus on yleensä 5 bitcoinia. (Jarvis 2013.)

2.3 Suojautuminen

Ransomwarelta suojautuminen käy samalla tavalla kuin suojautuminen kaikilta muiltakin haittaohjelmilta. Ransomware leviää useimmiten sähköpostin liitetiedostojen tai Internet-selaimen haavoittuvuuksien kautta. Tärkeimpinä varotoimenpiteinä voidaan pitää seuraavia:

- Käytetään aina ajan tasalla olevaa virustentorjuntaohjelmaa, jonka avulla pystytään mahdollisesti pysäyttämään ransomwaren ennen kuin se ehtii suoriutumaan tietokoneelle.
- Ei suoriteta epäilyttäviä tiedostoja tietokoneella. Ransomware liikkuu usein exe-tiedostoina.
- Pidetään ohjelmat ajan tasalla. Varsinkin selaimen, selaimen käyttämien lisäosien ja käyttöjärjestelmän uusimpien päivitysten on tärkeää olla kunnossa.
- Poistetaan Java-ohjelmisto tietokoneelta. Java toimii yhtenä yleisimmistä leviämisreiteistä haittaohjelmille.
- Varmuuskopioidaan tärkeät tiedostot säännöllisin väliajoin. (Hoffman 2013a.)

Salauksen suorittavalta kiristyshaittaohjelmalta suojautuessa on tärkeää tietää, että kyseinen haittaohjelma suorittaa usein salauksen myös kohdekoneessa oleviin ulkoisiin massamuisteihin sekä siihen liitettyihin verkkoasemiin. Useissa tapauksissa varmuuskopiot tietokoneesta otetaan säilytykseen toiselle näistä vaihtoehdoista ja näin ollen salaavan kiristyshaittaohjelman iskiessä palautus on mahdotonta tehdä varmuuskopioilta.

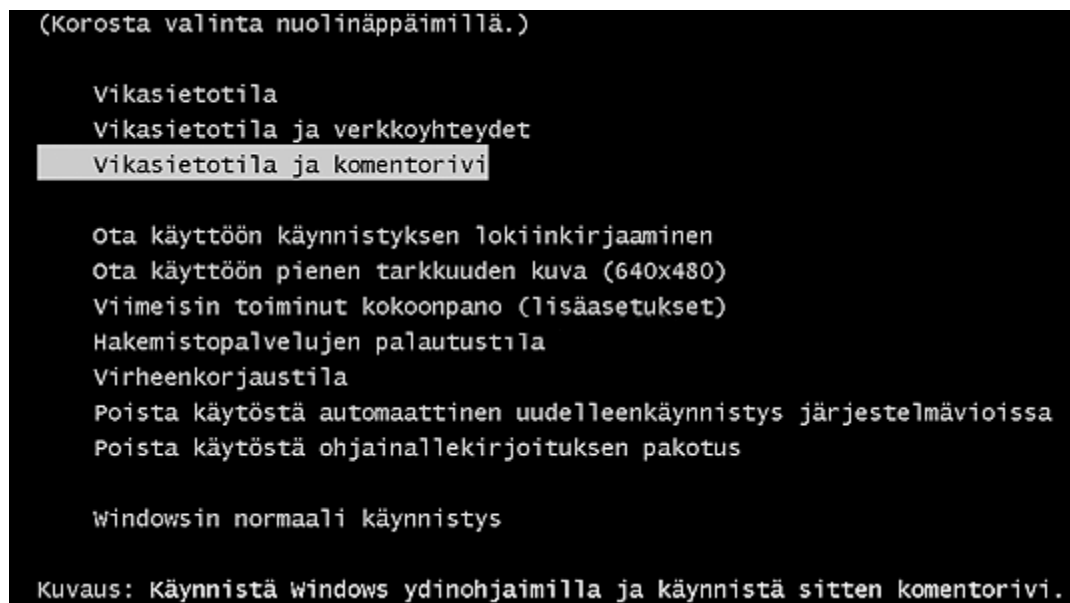
Edellä mainitusta syystä on tärkeää siirtää varmuuskopiot myös laitteelle, joka ei ole yhteydessä suoraan minkään verkossa olevan laitteen kanssa.

2.4 Poistaminen

Poliisiviruksen poistaminen Järjestelmän palauttamisen avulla

1. Käynnistetään tietokone Vikasietotila ja komentorivi -tilaan (Kuva 2).

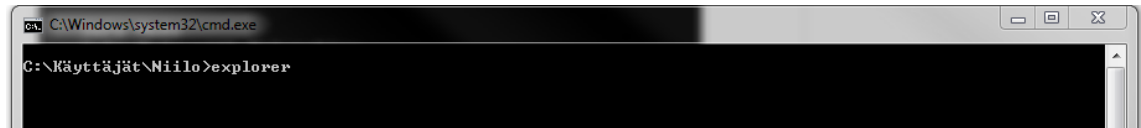
Käynnistetään tietokone uudelleen ja pidetään F8-näppäintä pohjassa käynnistyksen aikana ennen kuin Windows-logo ilmestyy ruutuun. Valitaan avautuvasta Käynnistyksen lisäasetukset -valikosta "Vikasietotila ja komentorivi". Kirjaututaan tietokoneeseen järjestelmänvalvojan käyttäjätunnuksella.



Kuva 2. Käynnistyksen lisäasetukset.

2. Siirrytään komentoriviltä Resurssienhallintaan.

Komentorivin avautuessa kirjoitetaan siihen nopeasti "explorer" ja painetaan Enteriä (Kuva 3). Liian hitaasti kirjoitettaessa kiristyshaittaohjelma ehtii lukitsemaan tietokoneen.



Kuva 3. Komentorivi.

3. Siirrytään Järjestelmän palauttaminen -toimintoon.

Siirrytään Resurssienhallinnan avulla seuraavaan alikansioon ja suoritetaan exe-tiedosto:

- Win XP: C:\windows\system32\restore\rstrui.exe (Kuva 4)
- Win Vista/7/8: C:\windows\system32\rstrui.exe



Kuva 4. Resurssienhallinta.

4. Suoritetaan Järjestelmän palauttaminen aikaisempaan ajankohtaan.

Seurataan Järjestelmän palauttamisen antamia ohjeita ja palautetaan tietokone aikaisempaan tilaan ennen kiristyshaittaohjelman tarttumista.

5. Varmistetaan että kiristyshaittaohjelma on poistettu tietokoneelta.

Varmistetaan tämä skannaamalla tietokone virustentorjuntaohjelmalla sekä haittaohjelmien poisto-ohjelmalla. (Foss 2013.)

Salauksen suorittavan kiristyshaittaohjelman poisto

Salauksen suorittava kiristysohjelma on mahdollista poistaa tietokoneelta, mutta tämä ei kuitenkaan poista tietokoneella olevien tiedostojen salausta. Vaikka kiristyshaittaohjelman saa kohtalaisen vaivattomasti poistettua, on henkilökohtaisten tiedostojen palauttaminen ymmärrettävään muotoon lähes mahdotonta.

On havaittu, että suurimmassa osassa tapauksista maksamalla kiristyshaittaohjelman vaatiman lunnasmaksun on salaus henkilökohtaisista tiedostoista poistunut ja kiristyshaittaohjelma itse on myös poistunut automaattisesti tietokoneelta (Abrams 2013). Tätä tiedostojen palautustapaa ei kuitenkaan voida mitenkään varmistaa etukäteen, joten siihen ei pitäisi turvautua kuin ehdottoman pakon edessä.

3 LEVINNEISYYS

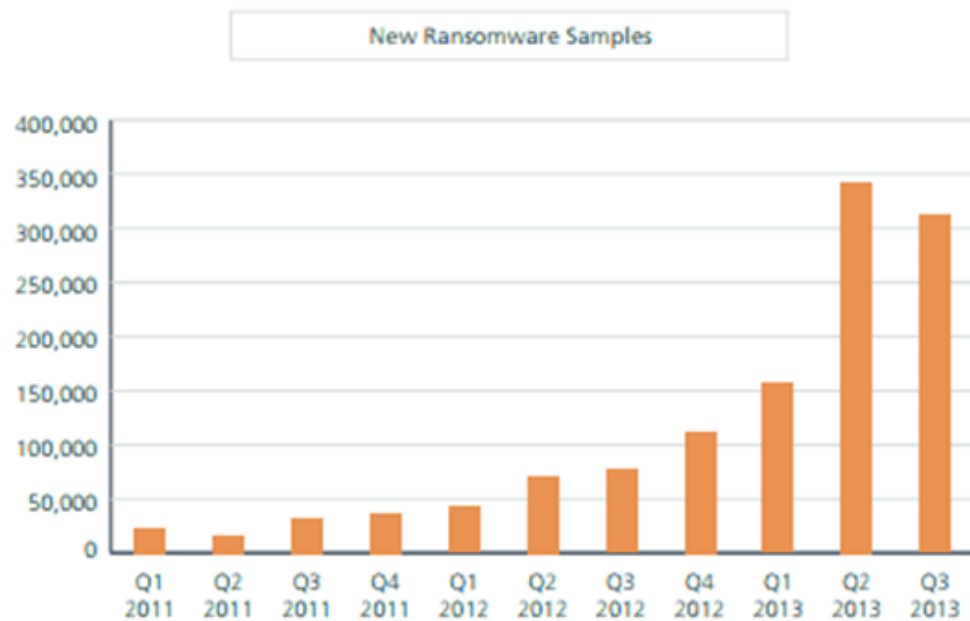
Tällä hetkellä ransomware on maailmanlaajuisesti noussut suureksi ongelmaksi niin tavallisille kuluttajille kuin myös yritysmaailmalle. Suurin osa ransomwaren havainnoista on tehty Pohjois-Amerikassa, Euroopassa ja Lähi-idässä. Aasiassa ensimmäiset suuret ransomware-tapaukset on havaittu vasta kryptovaluutta Bitcoinin suosion noustessa, sen ollessa maanosan ensimmäisiä anonyymejä maksutapoja. Kiinan ollessa yksi suurimmista ja nopeimmin kasvavista Bitcoin-markkina-alueista, se mahdollistaa samalla kyberrikosten huomattavan kasvun. (F-Secure Labs 2013.)

Syy ransomwaren räjähdysmäiseen kasvuun on sen erittäin tehokas tapa tuottaa rahaa haittaohjelman levittäjälle. Lunnasrahojen kerääminen hoidetaan useiden anonyymien maksupalvelujen kuten MoneyPakin, Paysafecardin tai Ukashin avulla. Tästä johtuen rahaliikenteen seuraaminen ja jäljittäminen on lähes mahdotonta viranomaisille. Ransomwaren helppoa levittämistä edesauttavat pimeillä markkinoilla myytävät valmiit haittaohjelmapaketit, jotka pitävät sisällään valmiin infrastruktuurin. (McAfee Labs 2013a, 12.)

Kentin yliopiston tekemän tutkimuksen mukaan joka kolmaskymmenes vastaajista on joutunut CryptoLocker-kiristyshaittaohjelman tartunnan uhriksi. Uhreista 40 prosenttia ilmoitti maksaneensa haittaohjelman pyytämät lunnasrahat saadaakseen tiedostonsa takaisin. Sama tutkimus paljastaa joka kymmenennen vastaajista saaneen tartunnan jostakin kiristyshaittaohjelmasta. (Hawes 2014.)

Tietoturvayhtiö Symantecin arvion mukaan CryptoLockerin kehittäjille maksaneita uhreja olisi kuitenkin vain noin 3 prosenttia edellä mainitun tutkimuksen 40 prosentin sijaan (Ferguson 2013).

McAfeen julkaisema tietoturvaraportti antaa käsityksen ransomwareen perustuvien haittaohjelmien räjähdysmäisestä kasvusta. McAfee ilmoittaa luvuksi yli 312 000 uniikkia näytettä loppuvuonna 2013, mikä on yli puolet enemmän alkuvuoteen verrattuna (Kuvio 1).



Kuvio 1. Ransomwareen levinneisyys (McAfee Labs 2013b, 19).

Android-käyttöjärjestelmälle on jo havaittu ei-salaavia kiristyshaittaohjelmia, jotka tarttuvat Internet-selaimen kautta. Kyseiset haittaohjelmat ovat naamioituneet tunnetuiksi virustentorjuntaohjelmiksi, jotka ilmoittavat itsestään kesken Internet-selailun. Käyttäjän ensin asentaessa ja sitten suorittaessa valevirustorjunnan ohjeiden mukaan on se löytävinään erilaisia haittaohjelmia laitteelta. Sen jälkeen valevirustorjuntaohjelma eli ns. FakeAV lukitsee käyttäjän laitteen vedoten turvallisuuteen. Mobiililaite on käyttökelvoton kunnes käyttäjä maksaa vaaditun lunnassumman. (Hamada 2013.)

4 TULEVAISUUDENNÄKYMÄT

Tulevaisuudessa on odotettavissa poliisivirustyylisten kiristyshaittaohjelmatapusten huomattava lasku. Ihmisten tietoisuuden lisääntyessä tämäntyyppisistä verkkohuijauksista yhä useampi jättää lunnasvaatimuksen maksamatta. Haittaohjelman levittäjät alkavat keskittyä enemmän salauksen suorittavien kiristyshaittaohjelmien levittämiseen, koska näissä tapauksissa tiedostojen takaisin saamiseksi on lunnasvaatimuksen maksaminen tällä hetkellä ainoa keino. (European Cybercrime Centre 2014.)

Haittaohjelman levittäjät tulevat yhä enenevässä määrin muuttamaan hyökkäyskeinojaan ja käyttämään enemmän sosiaalisia manipulointitaitoja saadakseen enemmän uhreja. On odotettavissa, että lunnasvaatimukset nousevat korkeammiksi ja vaatimukset tulevat yhä hyökkäävämmiksi. Tulevaisuudessa on myös odotettavissa erilaisia variaatioita esimerkiksi kiristyshaittaohjelmasta, joka varastaa samalla pankkitunnuksia. (European Cybercrime Centre 2014.)

Vuonna 2013 mobiililaitteille suunnattujen haittaohjelmien määrän kasvu oli huomattavasti suurempaa kuin PC-laitteiden vastaava määrän kasvu. Näistä leijonanosa kohdistui Android-käyttöjärjestelmään sen avoimuuden ja digitaalisen sisältöpalvelun heikomman valvonnan takia. Tämän takia vuonna 2014 on odotettavissa ensimmäinen oikea käyttäjän henkilökohtaiset tiedostot salaava kiristyshaittaohjelma Android-käyttöjärjestelmälle. (McAfee Labs 2013c.)

Kiristyshaittaohjelmat tulevat potentiaalisesti leviämään myös tulevaisuudessa Linux-, iOS- ja Windows Phone -käyttöjärjestelmille. Tällä tavalla verkkorikolliset haluavat levittää haittaohjelmaa mahdollisimman monille ekosysteemeille ja maksimoida lunnasvaatimusten tuotot.

Verkkorikollisten käyttämät toimintatavat mukautuvat yhä enemmän virustentorjunta-alan ja viranomaisten käyttämiin strategioihin. Tämän myötä voidaan odottaa, että kiristyshaittaohjelmat tulevat yhä monimutkaisemmiksi ja vaikeammin torjuttaviksi. (European Cybercrime Centre 2014.)

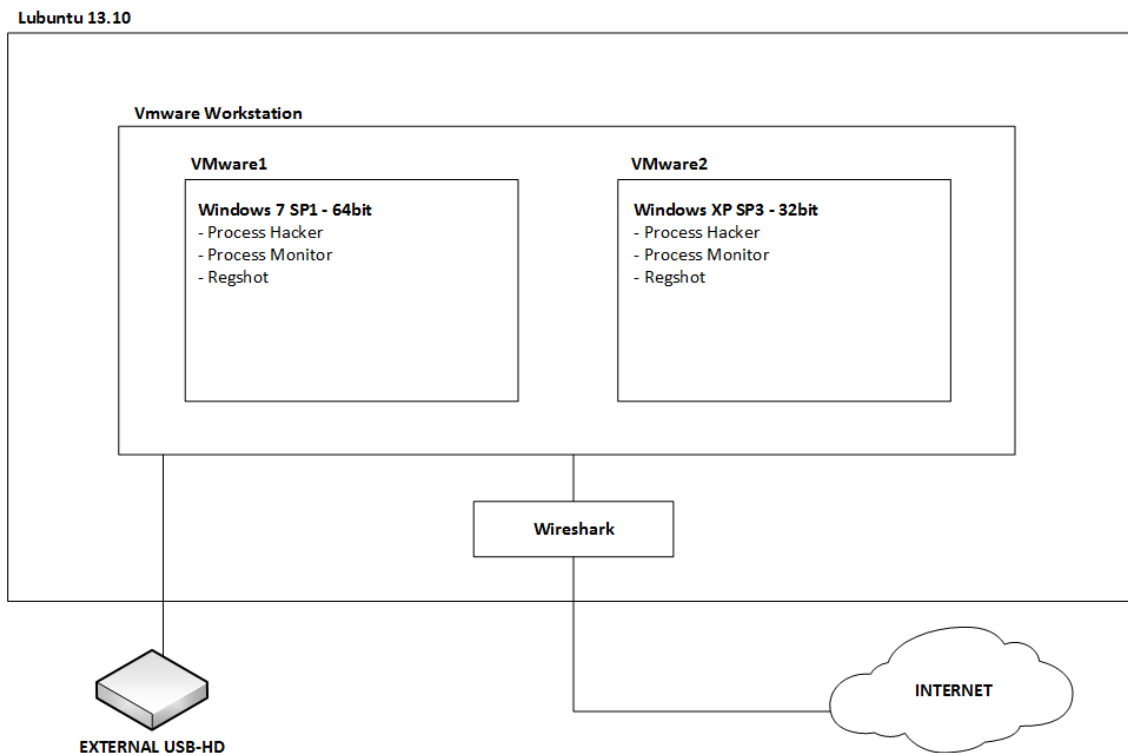
Bitcoinin tulevaisuuden ollessa muiden kryptovaluuttojen kanssa edelleen epävakaa pohjalla sen mahdollinen romahtaminen heijastuisi myös kiristyshaittaohjelmiin, koska Bitcoin on yksi yleisimmistä maksutavoista lunnasmaksuissa. Tällaisessa tapauksessa kuitenkin korvaava maksutapa löytynee nopeasti.

5 RANSOMWAREN TUTKIMINEN SULJETUSSA YMPÄRISTÖSSÄ

Ransomware-haittaohjelman käytännön toimintaa tutkittiin suljetussa ympäristössä. Testattavaksi valittiin CryptoLocker-niminen haittaohjelma, koska se on tällä hetkellä kuuma puheenaihe maailmalla sekä yksi eniten tuhoa aiheuttavista kiristyshaittaohjelmista. CryptoLocker eroaa muista yleisistä haittaohjelmista siten, että se salaa massamuisteilla olevia tiedostoja käyttökelvottomiksi ja on täten mielenkiintoisin testattavista ransomwareista.

Testiympäristön tärkeimmäksi lähtökohdaksi haluttiin täysin suljettu ympäristö, jossa kiristyshaittaohjelma on vaaratonta käynnistää ja josta sen leviäminen ulkopuolelle on käytännössä mahdotonta. Ympäristö luotiin koululta tarkoitukseen saatuun kannettavaan tietokoneeseen.

Ympäristön pääkäyttöjärjestelmäksi valittiin GNU/Linux-ytimeen perustuva Lubuntu 13.10 -distribuutio. Tämä lisää ylimääräisen turvakerroksen testiympäristöön, minkä seurauksena pääkäyttöjärjestelmä ei voi saada millään tavalla tartuntaa CryptoLockerista, koska sen toiminta on rajoittunut Windows-ympäristöön.

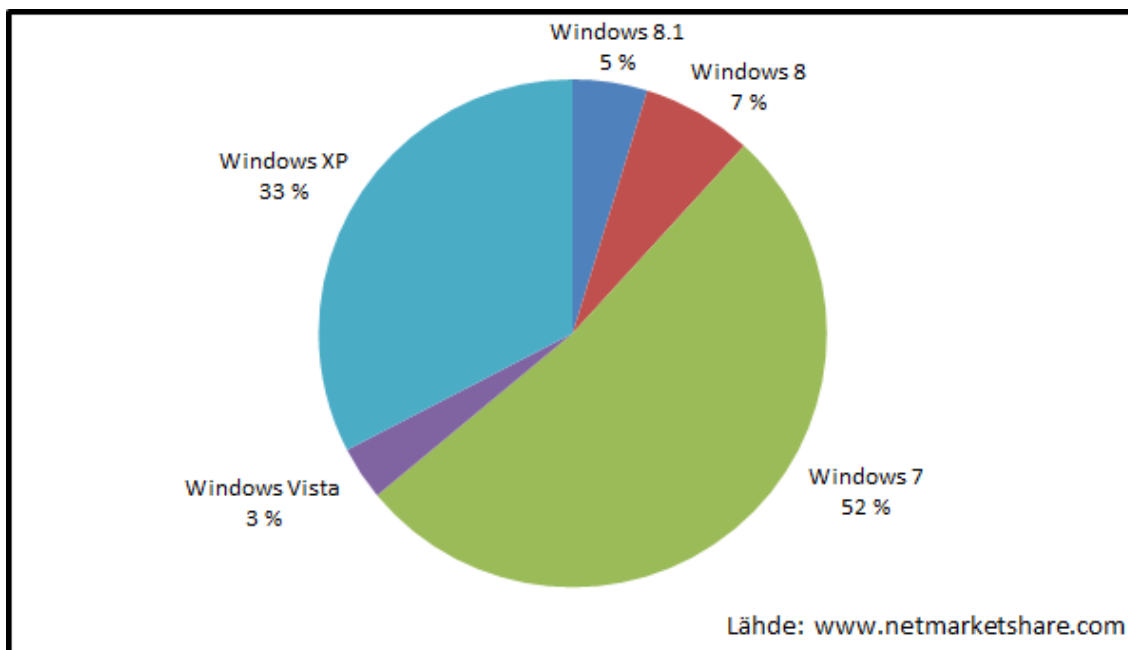


Kuvio 2. Suunnitelma toteutettavasta testausympäristöstä.

Koska CryptoLocker on tähän mennessä suunniteltu ainoastaan Windows-ympäristössä toimivaksi kiristyshaittaohjelmaksi, sen suorittamiseen tarvitaan valitussa Linux-järjestelmässä virtualisoitu Windows-käyttöjärjestelmä. Virtualisointi toteutettiin kaupallisella VMware Workstation for Linux 10.0 -ohjelmistolla. Virtuaalikoneissa ajettaviksi käyttöjärjestelmiksi valittiin 32-bittinen Windows XP SP3 ja 64-bittinen Windows 7 SP1 (Kuvio 2).

5.1 Ympäristön käyttöjärjestelmät

Testiympäristön pääkäyttöjärjestelmän osalta painotettiin keveyttä ja turvallisuutta. Windows-käyttöjärjestelmät valittiin niiden yleisyyden perusteella. Windows 7 ja XP ovat kaksi yleisintä Microsoftin käyttöjärjestelmää (Kuvio 3).



Kuvio 3. Windows-käyttöjärjestelmäversioiden markkinaosuus helmikuussa 2014 (NetMarketShare 2014).

Lubuntu 13.10

Lubuntu perustuu suosittuun Ubuntu-käyttöjärjestelmään. Ubuntusta poiketen Lubuntu sisältää erittäin kevyen LXDE-työpöydän, jonka valtteina ovat nopeus, energiatehokkuus ja RAM-muistin optimoitu käyttö (Lubuntu 2014). Tästä syystä se on optimaalinen ympäristöön, jossa on rajallinen määrä keskusmuistia, kuten esimerkiksi tässä testiympäristössä on vain 2 gigatavua käytössä.

Microsoft Windows XP

Windows XP on edelleen yksi suosituimmista käyttöjärjestelmistä, vaikka Microsoftin tuki sille loppui 8.4.2014 (Microsoft 2014). XP:stä valittiin testiympäristöön 32-bittinen versio, koska 64-bittinen versio on jäänyt puutteellisen tuen takia hyvin harvinaiseksi.

Microsoft Windows 7

Windows 7 on tämän hetken suosituin käyttöjärjestelmä (NetMarketShare 2014). 64-bittinen versio valittiin sen parempien tietoturvaominaisuuksien takia verrattuna 32-bittiseen versioon. Yksi monista lisäturvaa tuovista ominaisuuksista on esimerkiksi pakollinen ajureiden elektroninen allekirjoitus. Tällä varmistetaan, että mikään haittaohjelma ei pysty suoriutumaan käyttöjärjestelmän ydin-osana. (Hoffman 2013b.)

64-bittinen versio osaa myös käsitellä yli 4 gigatavua muistia kun taas 32-bittisen version maksimimuistimäärä on 4 gigatavua. Tästä ominaisuudesta ei kuitenkaan ollut hyötyä tässä tapauksessa, koska testikoneessa on vain 2 gigatavua muistia. (Hoffman 2013b.)

5.2 Ympäristön ohjelmistot

Testiympäristössä ajettaviksi ohjelmiksi pyrittiin valitsemaan ilmaisia tai avoimeen lähdekoodiin perustuvia, kevyitä ja yksinkertaisia ohjelmia. Maksulliseen VMware Workstationiin päädyttiin, koska ilmaisista vaihtoehdoista ei löytynyt testien suorittamiseen vaadittavia ominaisuuksia. Diagnostiikkaohjelmissa hyvien ominaisuuksien lisäksi tärkeimmäksi valintakriteeriksi muodostui selkeä lokiominaisuus, jonka avulla testitulosten analysointi helpottuu huomattavasti.

VMware Workstation

VMware Workstation for Linux 10.0 on ohjelmisto, jolla voidaan luoda virtuaalikoneita. Se mahdollistaa useamman virtualisoidun käyttöjärjestelmän asentamisen ja yhtäaikaisen käytön yhdellä isäntäkoneella.

Workstation mahdollistaa virtuaalikoneen verkon siltaamisen isäntäkoneen verkkokortin kanssa sekä fyysisten USB-laitteiden jakamisen suoraan virtuaalikoneiden suorittamien käyttöjärjestelmien käyttöön. Nämä ominaisuudet ovat

tarpeellisia testiympäristön toimivuuden takia, koska se helpottaa testien suorittamista.

Virtuaalikoneista pystyy tarvittaessa ottamaan ”snapshotteja”, jotka mahdollistavat helpon palaamisen aiempaan käyttöjärjestelmän tilaan, jossa muutokset ovat vielä tekemättä (VMware 2013). Tällä tavalla pystytään tekemään radikaalejakin muutoksia virtuaalikoneeseen ja vaikkapa kesken CryptoLockerin salauksen palaamaan takaisin alkutilanteeseen riskeeraamatta mitään tietoa.

Wireshark

Wireshark on ilmainen, avoimeen lähdekoodiin perustuva, tietoliikenneverkon tarkkailuun kehitetty ohjelma. Ohjelman avulla on mahdollista valita tietokoneessa sijaitseva verkkosovitin ja seurata reaaliajassa sovittimen ja muiden verkossa sijaitsevien laitteiden välillä kulkevia tietoliikennepaketteja.

Fyysisen verkkosovittimen lisäksi tarkkailtavaksi laitteeksi pystyy myös ottamaan VMware Workstationin luomat virtuaaliset verkkosovittimet, jolloin verkko liikenteen rajausta pelkäästään VMwaren sisällä tapahtuvaan liikenteeseen onnistuu helposti.

Process Hacker

Process Hacker on ilmainen, avoimeen lähdekoodiin perustuva prosessitarkkailija, jonka avulla on mahdollista seurata tietokoneen suorittamia prosesseja reaaliajassa. Process Hacker on verrattavissa Windows-käyttöjärjestelmän Task Manageriin, pitäen kuitenkin sisällään useita ominaisuuksia, joiden avulla prosessien seuraaminen on vaivattomampaa ja yksityiskohtaisempaa.

Ohjelmalla pystyy myös pysäyttämään, keskeyttämään ja rajoittamaan prosesseja ja prosessien pienempiä osia eli säikeitä oman mielensä mukaan. Tietyn prosessin suorittimen käyttöastetta ja kiintolevyaktiivisuutta pystyy seuraamaan helposti yhdellä vilkaisulla.

Process Monitor

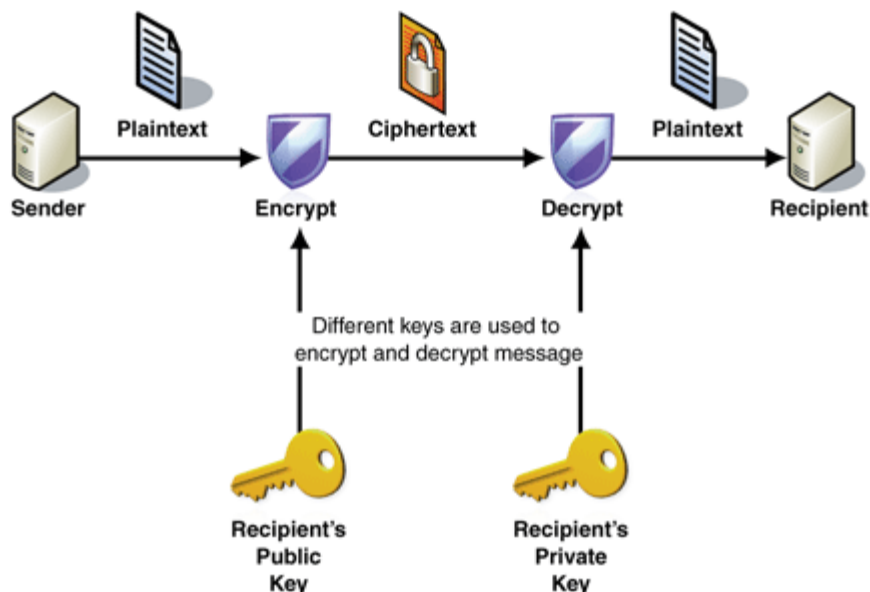
Process Monitor on ilmainen Windows-käyttöjärjestelmälle suunniteltu tiedostojen, rekisterin ja prosessien tarkkailuun kehitetty ohjelma. Process Monitor näyttää kaikki Windows-järjestelmässä tapahtuvat muutokset reaaliaikaisesti, ja on tämän takia erinomainen työkalu haittaohjelmien analysointiin. Ohjelma pitää sisällään ajastetun lokienkeräysominaisuuden, jonka avulla järjestelmän muutosten analysointia pystyy myös testien jälkeen tekemään helposti.

Regshot

Regshot on ilmainen, avoimeen lähdekoodiin perustuva ohjelma, jonka avulla pystyy ottamaan Windows-järjestelmän rekisteristä sekä tiedostojärjestelmästä ”snapshotin”. Ensimmäistä snapshottia pystyy ohjelman avulla vertaamaan toiseen snapshottiin, joka on otettu tehtyjen muutosten jälkeen. Regshot ilmoittaa vertailun tuloksena mahdollisista muutoksista rekisterissä ja tiedostojärjestelmässä, joita käyttöjärjestelmään tehdyt toimenpiteet ovat saaneet aikaan.

5.3 Kiristyshaittaohjelma – CryptoLocker

Testiympäristön kiristyshaittaohjelman valinta kohdistui suurta huomiota saaneeseen kiristyshaittaohjelmaan nimeltä CryptoLocker. Suoriutuessaan CryptoLocker salaa saastuneelta tietokoneelta ennalta määritellyt henkilökohtaiset tiedostot sisäisiltä sekä liitetyiltä ulkoisilta massamuisteilta julkisen avaimen salauksella. CryptoLocker käyttää salauksessa RSA- ja AES-algoritmien sekoitusta. (Abrams 2013.)



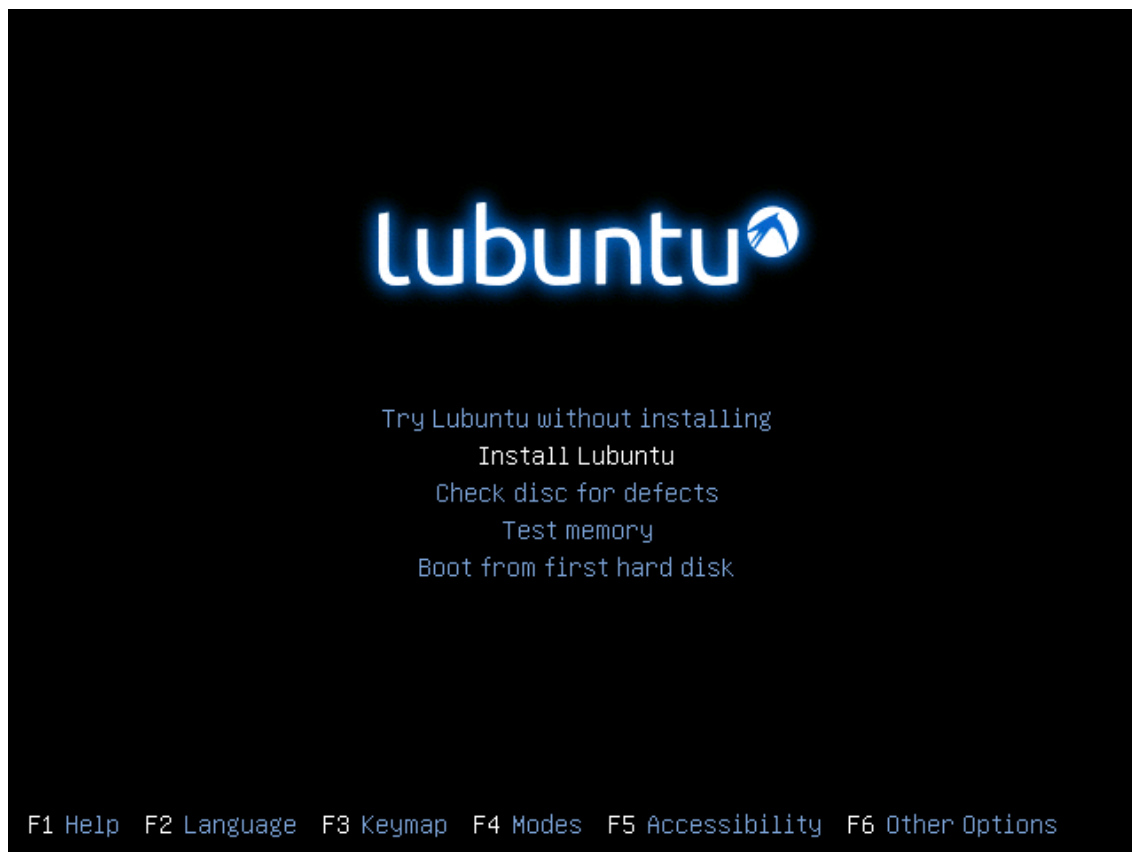
Kuva 5. Julkisen avaimen salaus (Microsoft 2005).

Julkisen avaimen salauksessa haittaohjelman tekijän salainen avain, jonka avulla tiedostot voidaan palauttaa, jää tekijän isäntäpalvelimelle odottamaan lunnasrahoja. Tekijän julkisen avaimen avulla tapahtuvan salauksen jälkeen haittaohjelma vaatii ponnahdusikkunan välityksellä lunnasrahoja saastuneen tietokoneen käyttäjältä. Käyttäjällä on 72 tuntia aikaa maksaa lunnaat, minkä jälkeen salainen avain tuhoutuu isäntäpalvelimelta, jos maksua ei suoriteta. Lunnasmaksun jälkeen haittaohjelma vapauttaa isäntäpalvelimella sijaitsevan salaisen avaimen, jonka avulla henkilökohtaisten tiedostojen salaus purkaantuu. (Kuva 5.)

5.4 Testiympäristön pystyttäminen

Testiympäristö toteutettiin HP Compaq 8710p -merkkisellä kannettavalla tietokoneella. Tietokoneen ominaisuuksista mainitsemisen arvoisia ovat Intel Core 2 Duo T7500 -suoritin, joka toimii 2,2 gigahertsin kellotaajuudella, sekä keskusmuistin määrä 2 gigatavua.

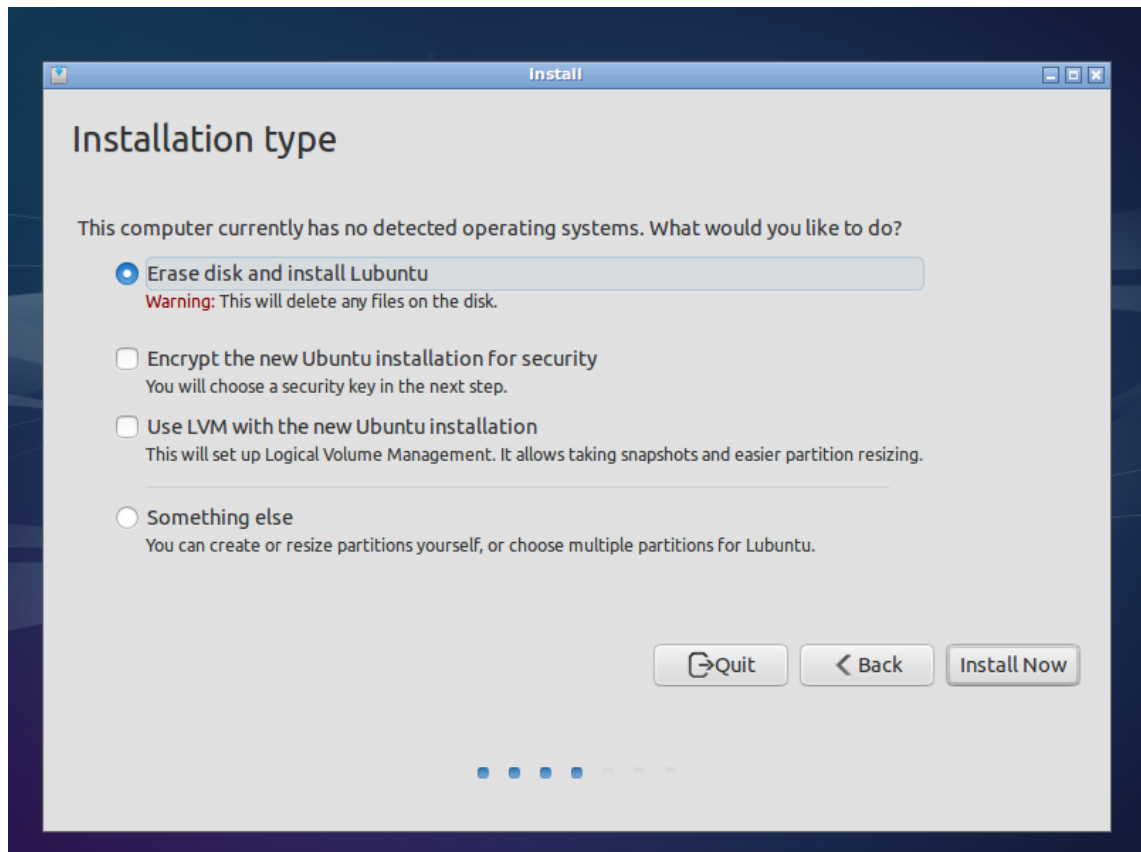
Ensimmäiseksi kannettavan tietokoneen kiintolevy alustettiin ja siihen asennettiin Ubuntu 13.10 -käyttöjärjestelmä oletusasetuksin. Levykuvasta luotiin USB-tikulta käynnistyvä asennusmedia käyttämällä Unetbootin-nimistä ohjelmaa.



Kuva 6. Asennusruutu 1.

Asennusmedian suorittamisen jälkeen ensimmäisestä asennusruudusta (Kuva 6) valittiin kohta "Install Ubuntu".

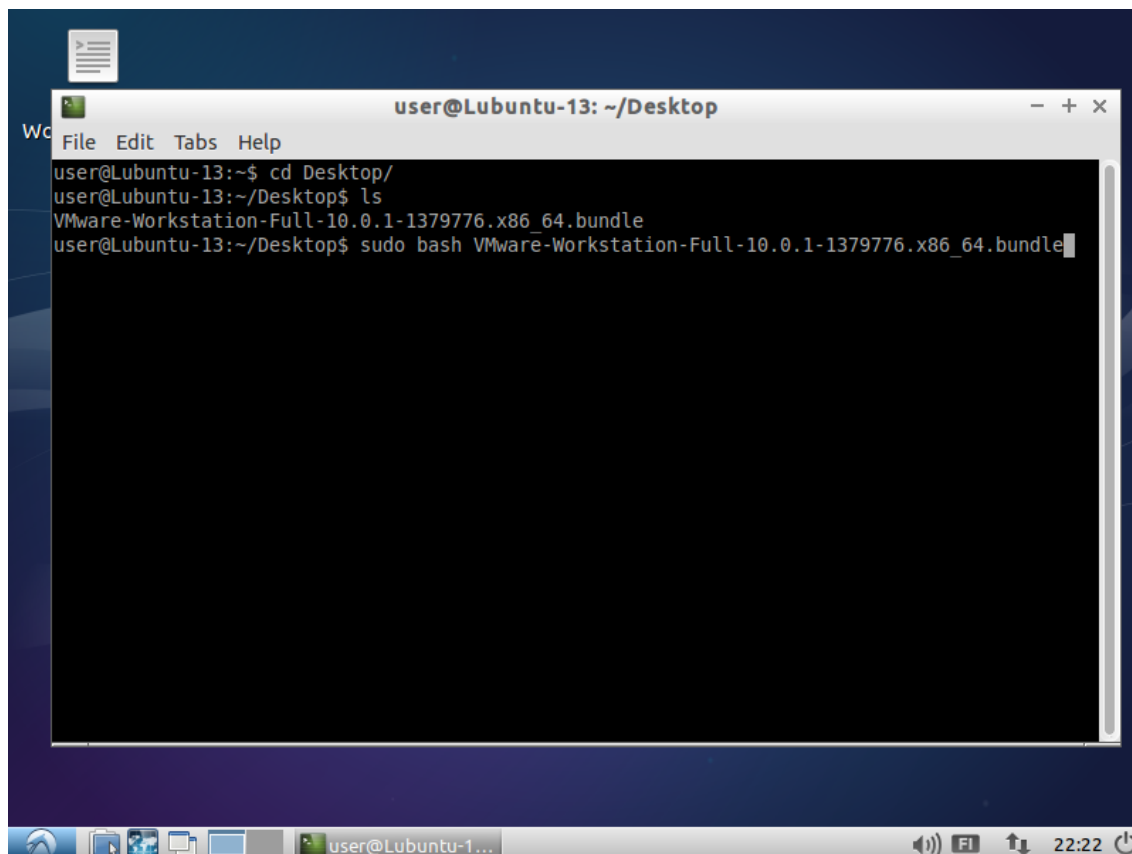
Sitten valittiin "Installation type" -valikosta valinta "Erase disk and install Ubuntu" (Kuva 7).



Kuva 7. Asennusruutu 2.

Seuraavaksi asennettiin VMware Workstation for Linux. Asennus tapahtui suoritettamalla komentokehoteessa seuraava komento, koska asennuspakettitiedosto sisältää valmiina bash-asennusskriptin (Kuva 8):

```
>sudo bash VMware-Workstation-Full-10.0.1-1379776.x86_64.bundle
```



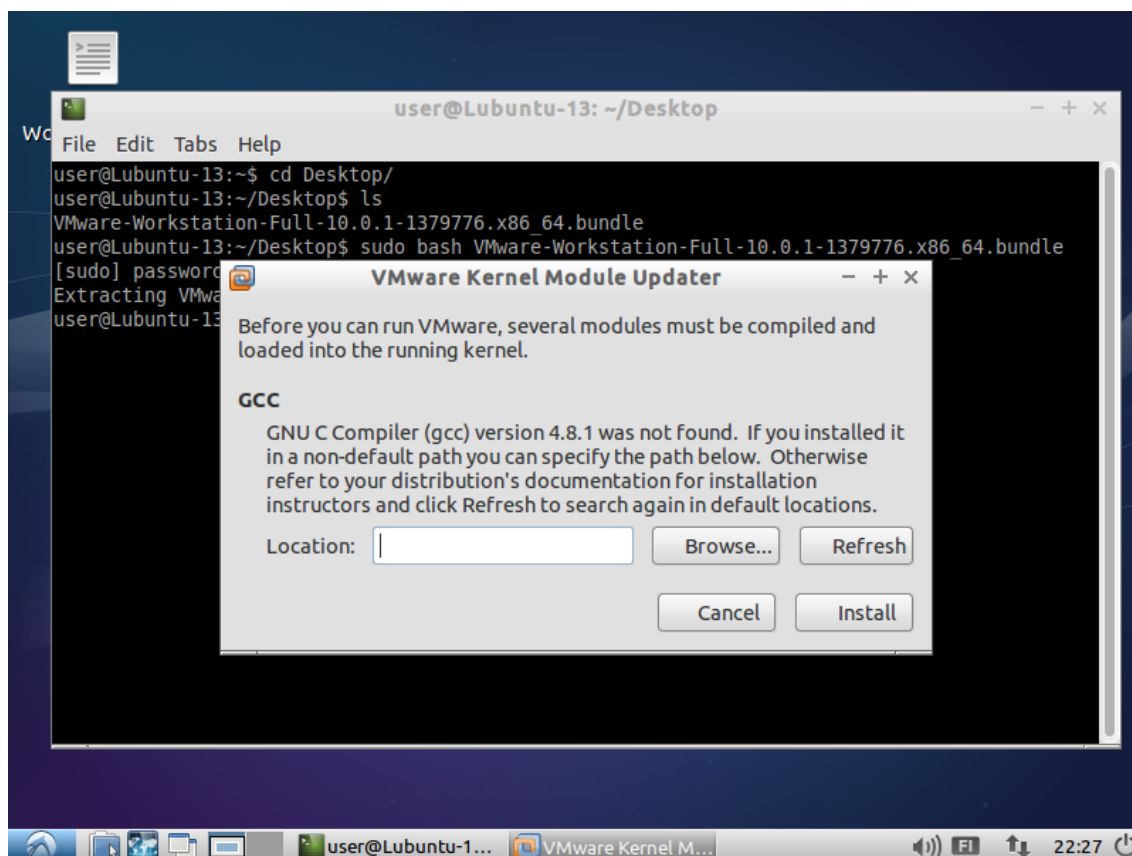
Kuva 8. VMwaren asennus komentoriviltä.

Asennuksen jälkeen ohjelma tarvitsi käynnistyäkseen käännettäväksi muuttaman moduulin käyttöjärjestelmän kerneliin. Tätä varten Lubuntuun asennettiin build-essential -niminen paketti, joka sisältää tarvittavat perustyökalut lähdekoodin kääntämiseen.

Asennus tapahtui seuraavanlaisesti komentoriviltä:

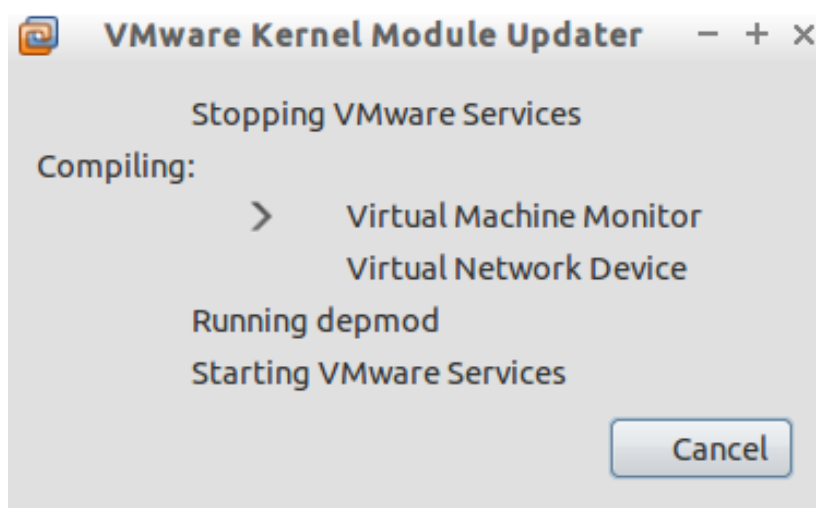
```
>sudo apt-get install build-essential
```

Tämän jälkeen moduulien kääntäminen alkoi painamalla Refresh- ja Install-näppäimiä VMware Kernel Module Updater -ikkunasta (Kuva 9).



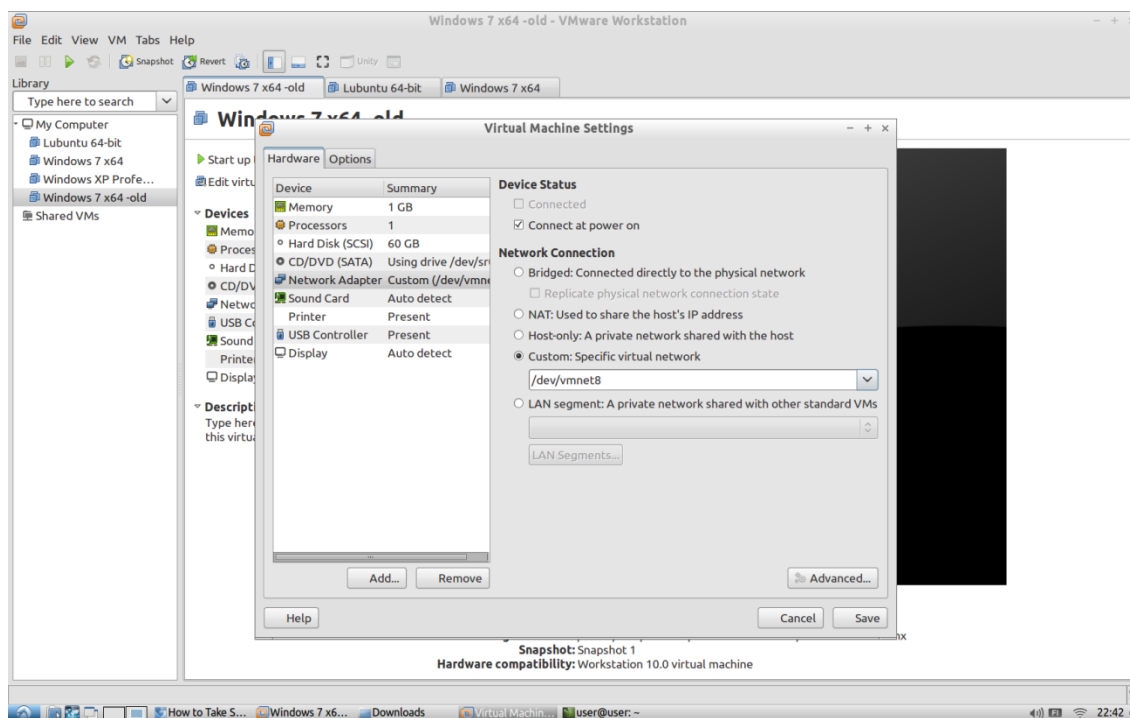
Kuva 9. VMwaren kernelin päivitysruutu.

VMware päivitti tämän jälkeen kernelin moduulin onnistuneesti (Kuva 10).



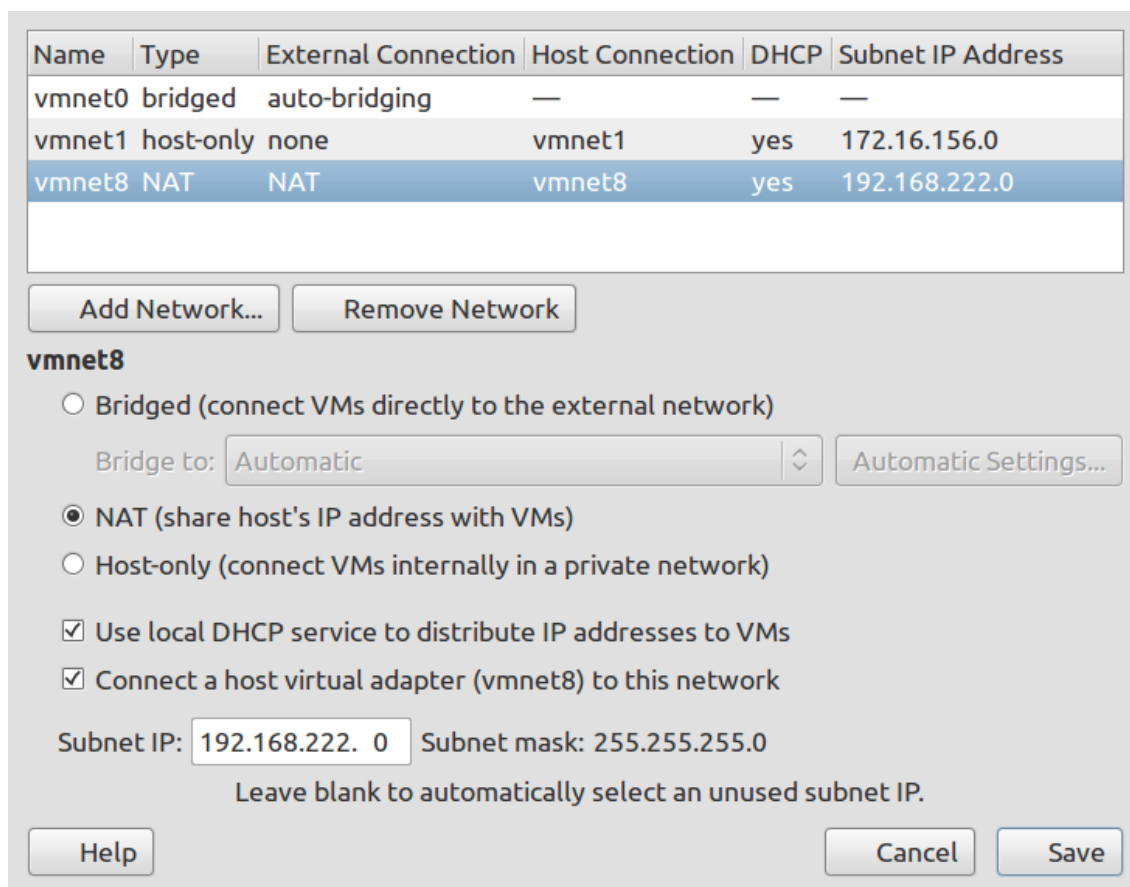
Kuva 10. VMware päivittää kernelin moduulia.

Seuraavaksi käynnistettiin VMware Workstation ja otettiin käyttöön kaksi esi-asennettua virtuaalikonetta, Windows XP ja Windows 7. Virtuaalikoneiden tiedot saatiin koululta. Virtuaalikoneiden asetuksiin tehtiin pieniä muutoksia, joista merkittävin työn kannalta oli Network Connection -kohtaan valittu vaihtoehto Custom (/dev/vmnet8) (Kuva 11).



Kuva 11. Virtuaaliverkkosovittimen valinta.

Tämä /dev/vmnet8 on virtuaaliverkkosovitin, joka asetettiin NAT-tilaan ja aliverkon peitteeksi syötettiin 192.168.222.0 (Kuva 12). Valinta tapahtui valikosta Edit -> Virtual Network Editor. Tällä tavalla virtuaalikoneiden verkkoliikennettä on helpompi kaapata Wireshark-ohjelman avulla, kun kaikki liikenne kulkee tämän virtuaaliverkkosovittimen kautta.



Kuva 12. Virtual Network Editor.

Kumpaankin virtuaalikoneeseen asennettiin uusimmat käyttöjärjestelmäpäivitykset, VMware Tools sekä seuraavat testaukseen liittyvät ohjelmat:

- Process Hacker
- Process Monitor
- Regshot.

Seuraavaksi pääkäyttöjärjestelmään asennettiin Wireshark-verkkovalvontaohjelma, jonka avulla verkkoliikenteen seuraaminen tapahtui. Wiresharkin asentaminen tapahtui komentoriviltä seuraavalla komennolla:

```
> sudo apt-get install wireshark
```

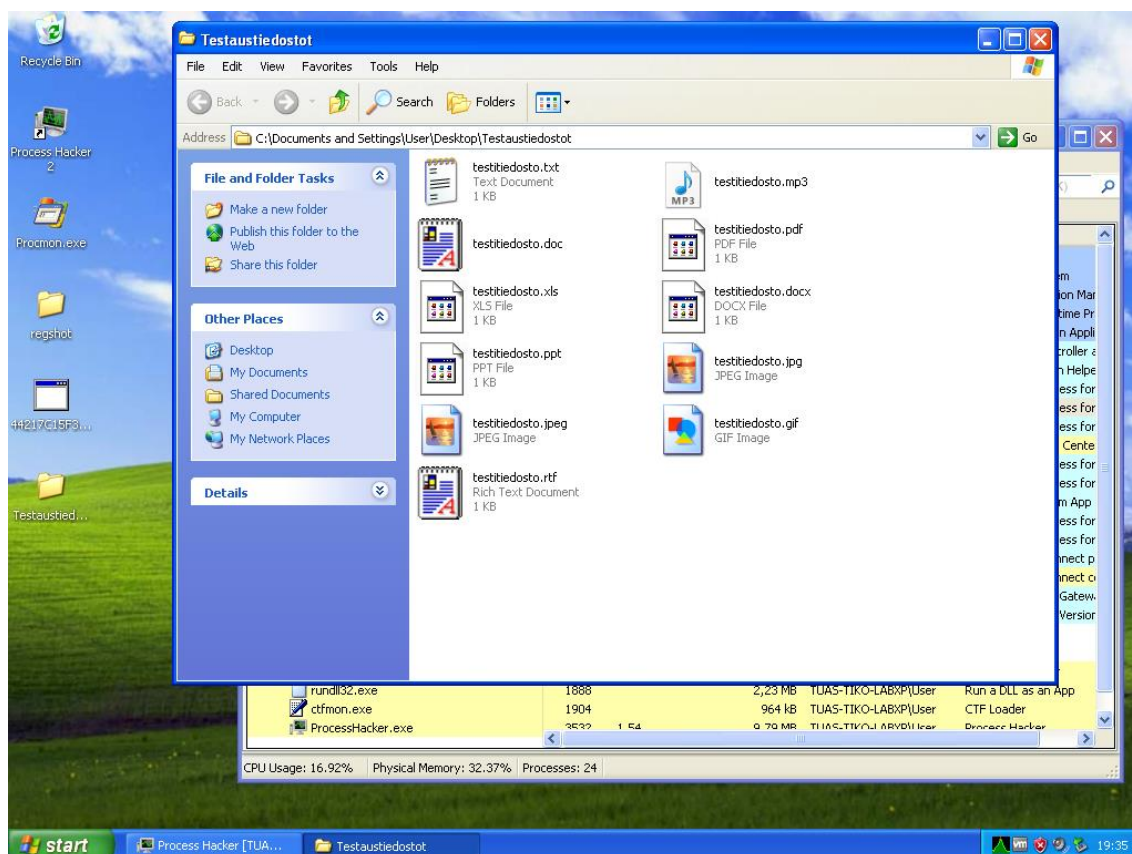
Wireshark piti käynnistää pääkäyttäjän oikeuksilla, jotta se tunnisti tietokoneessa olevat verkkosovittimet. Ohjelma käynnistyi komentoriviltä seuraavasti:

> sudo wireshark

5.5 CryptoLockerin testaus

CryptoLockerista valittiin testattavaksi luotettavalta sivustolta saatavissa oleva versio. Versio on sivuston uusin ja se on päivätty 10.2.2014. (Gibson Research Corporation 2014.) Suuren tietoturvuahan takia mahdollisesti uudempaa tai vaihtoehtoista versiota ei lähdetty etsimään epäilyttäviltä sivuilta.

Testiä varten molempien virtuaalikoneiden työpöydille luotiin identtiset hakemistot, jotka pitivät sisällään tiedostotyyppejä, joiden tiedettiin olevan CryptoLockerin salauksen kohteita (Kuva 13). Luotujen tiedostotyyppien päätteet ovat txt, doc, docx, xls, ppt, jpg, jpeg, rtf, mp3, pdf ja gif.



Kuva 13. CryptoLockerin kohdetiedostot XP-ympäristössä.

Ennen CryptoLockerin käynnistämistä virtuaalikoneympäristössä Wireshark asetettiin kaappaamaan virtuaaliverkkosovittimen lähettämää ja vastaanottamaa liikennettä. Tämä tapahtuu valitsemalla Wiresharkin asetuksista kaapattavaksi rajapinnaksi /dev/vmnet8-virtuaaliverkkosovitin. Tällä tavalla pystyttiin helposti rajaamaan testin kannalta tarpeellinen liikenne muusta liikenteestä.

Virtuaalikoneisiin asennetut seurantaohjelmat asetettiin tallentamaan lokitiedostoja CryptoLockerin aiheuttamista muutoksista.

Tämän jälkeen virtuaalitietokone yhdistettiin julkiseen verkkoon mobiililaajakais-
taa käyttämällä ja suoritettiin CryptoLockerin sisältävä ohjelmätiedosto.

CryptoLockeria ei tarvinnut käynnistää järjestelmänvalvojan oikeuksilla, koska sitä suoritettaessa se osasi tehdä kopion itsestään hakemistoon %LocalAppData% nimellä flmhcbux.exe. %LocalAppData% on järjestelmämuuttuja, joka tässä tapauksessa viittaa hakemistoon C:\User\user\AppData\Local, josta kohta "user" taas viittaa käyttäjätunnukseen. Tästä hakemistosta CryptoLocker pystyi käynnistämään itsensä täysillä järjestelmänvalvojan oikeuksilla ilman, että niitä erikseen sille annettiin.

Kun CryptoLocker käynnistettiin, se vaihtoi julkiset avaimet isäntäpalvelimen kanssa. Wireshark-lokeissa näkyy, että osoitteelle shalunishka12.org suoritettiin DNS-kysely ja DNS-palvelin vastasi IP-osoitteen olevan 77.72.133.146. Sen jälkeen salattua tietoa lähetettiin HTTP-protokollan kautta osoitteesta <http://shalunishka12.org/e.php> (Liite 1).

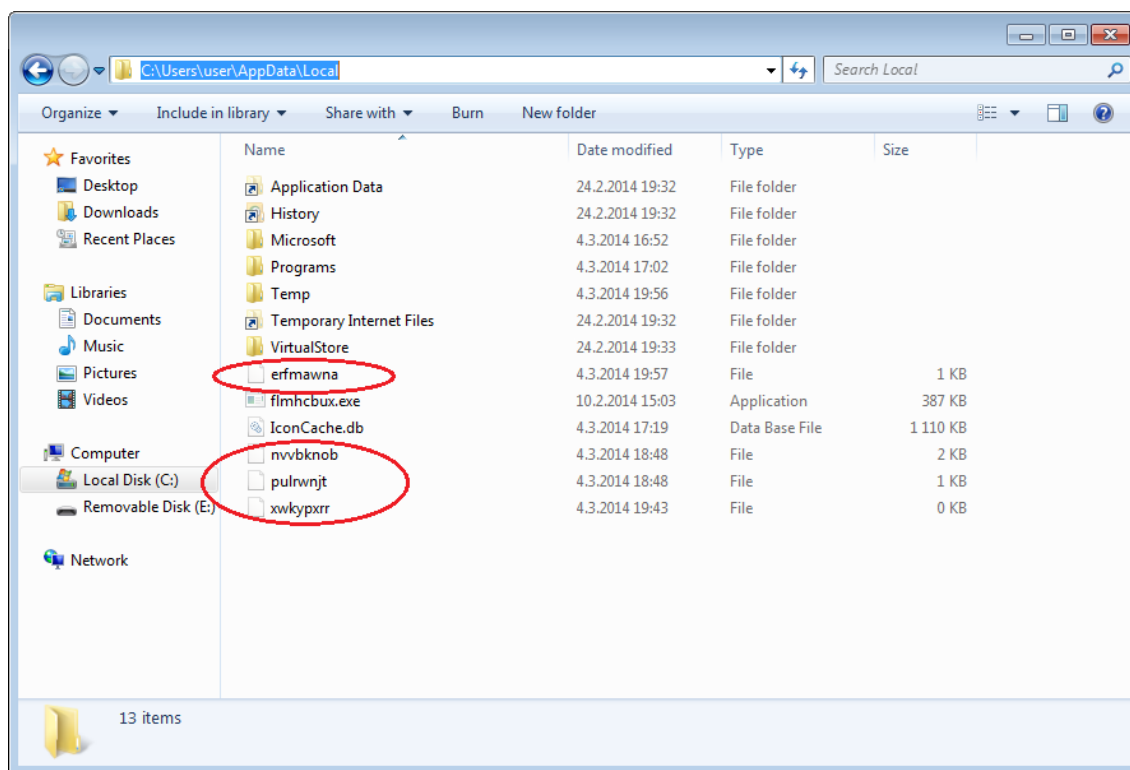
CryptoLocker loi päätteettömät tiedostot nimeltä erfmawna, nvvbknob, pulrwnjt, xwkypxrr (Kuva 14). Näiden tiedostojen tarkoitusperästä ei ole varmaa tietoa, mutta todennäköisesti kyseessä on ohjelman ja palvelimen välisen tiedonsiirron aikaansaannoksena syntyneet julkiset avaimet sekä lista salatuista tiedostoista.

Yllä mainitut CryptoLockerin luomat tiedostot syntyivät Windows 7 -ympäristössä. Windows XP:ssä syntyi erinimiset satunnaisia kirjaimia sisältävät tiedostot, kuten itse CryptoLocker tiedostonnimellä zafshfd.exe. Mielenkiintoista kyllä, vaikka Windows 7 -ympäristössä käynnistettiin useita eri testikertoja pa-

laamalla aina takaisin alkutilanteeseen, syntyi aina samannimiset tiedostot. Tiedostonnimien satunnaisuus siis tuntui olevan jollain tavalla kone- tai käyttöjärjestelmäkohtaista.

CryptoLocker lisäsi Windowsin rekisteriin muutamia arvoja, joista tärkein ja selvinkin oli se, että Windowsin käynnistyessä myös CryptoLocker käynnistyy automaattisesti (Liite 2). Rekisterin kohta oli seuraava:

- *HKU\S-1-5-21-299502267-1004336348-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Run\:
C:\Documents and Settings\User\Local Settings\Application Data\zaf\shfd.exe*



Kuva 14. CryptoLockerin luomat tiedostot.

Avainten vaihdon jälkeen CryptoLocker kävi läpi koneen tiedostot, ja salasi ennalta määritellyt tietyntyyppiset tiedostot. CryptoLocker ei salaa esim. exe- tai dll-tiedostoja, koska silloin käyttöjärjestelmä ei toimisi.



Kuva 15. CryptoLockerin saastuttama kone.

Salauksen jälkeen ruutuun aukesi ikkuna, joka kertoi henkilökohtaisten tiedostojen salaamisesta. Seuraava teksti on suora suomennos ikkunassa olevasta tekstistä (Kuva 15):

“Henkilökohtaiset tiedostosi ovat salattu!

Tärkeiden tiedostojesi salaus tuotettu tässä tietokoneessa: valokuvat, videot, dokumentit, yms.

Salaus on tehty käyttämällä uniikkia julkista avainta RSA-2048 generoituna tälle tietokoneelle. Salauksen purkua varten tarvitset yksityisen avaimen.

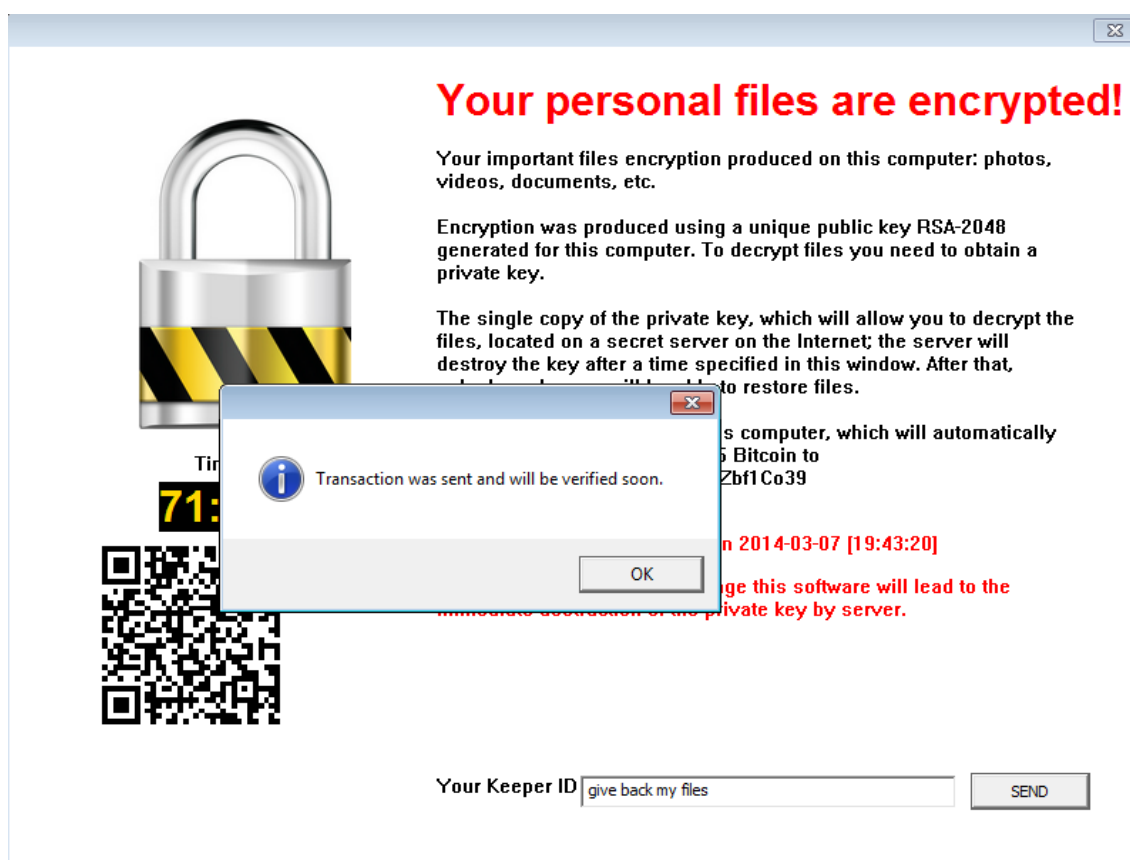
Yksityisen avaimen ainoa kopio, jolla voit purkaa tiedostojen salauksen, on salaisella palvelimella Internetissä; palvelin tuhoaa avaimen tässä ikkunassa määritellyn ajan jälkeen. Sen jälkeen kukaan ei koskaan pysty palauttamaan tiedostoja.

Saadaksesi yksityisen avaimen tälle tietokoneelle, joka automaattisesti purkaa tiedostojen salauksen, sinun tarvitsee maksaa 5 bitcoinia tilille xxx.

HUOMIO!

Yksityinen avain tuhoutuu 2.3.2014 [19:49:20]

Jokainen yritys poistaa tai vahingoittaa tätä ohjelmaa johtaa yksityisen avaimen välittömään tuhoutumiseen palvelimelta.”

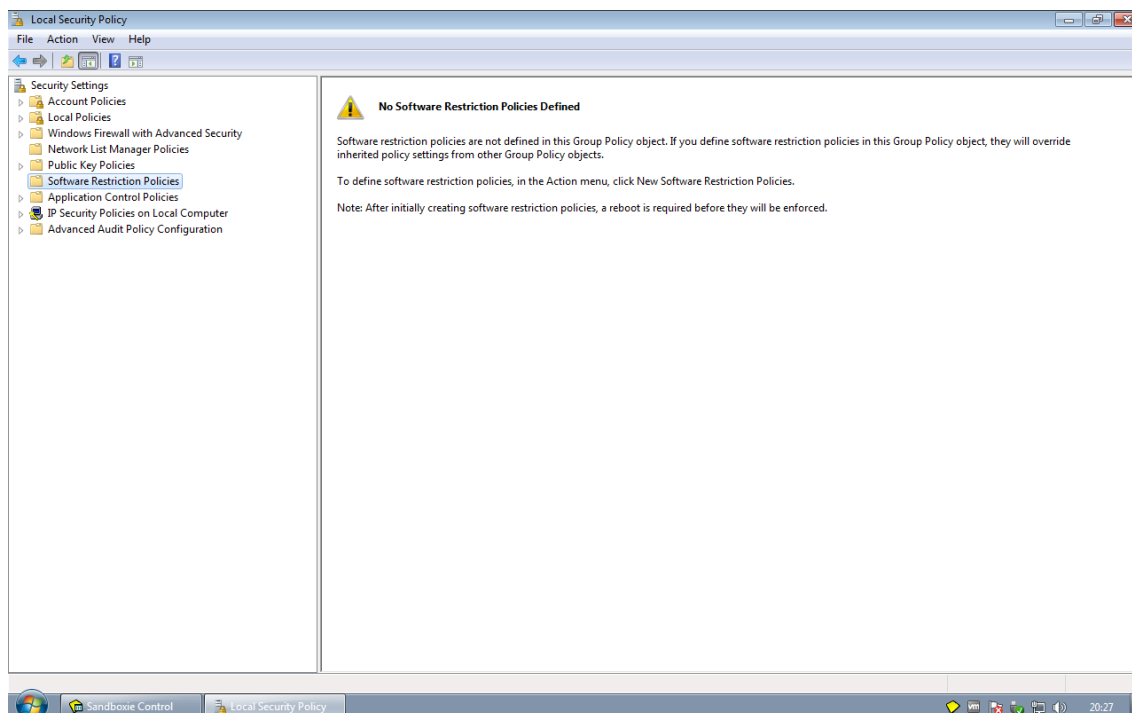


Kuva 16. CryptoLockerille syötetty keksitty purkukoodi.

CryptoLockerin pyytämien lunnaiden maksua ei testattu, mutta jos ikkunassa olevaan tekstikenttään syötti mitä tahansa tekstiä, tuli ponnahdusikkuna, jossa luki ”Transaction was sent and will be verified soon.” (Kuva 16).

5.6 CryptoLockerilta suojautuminen

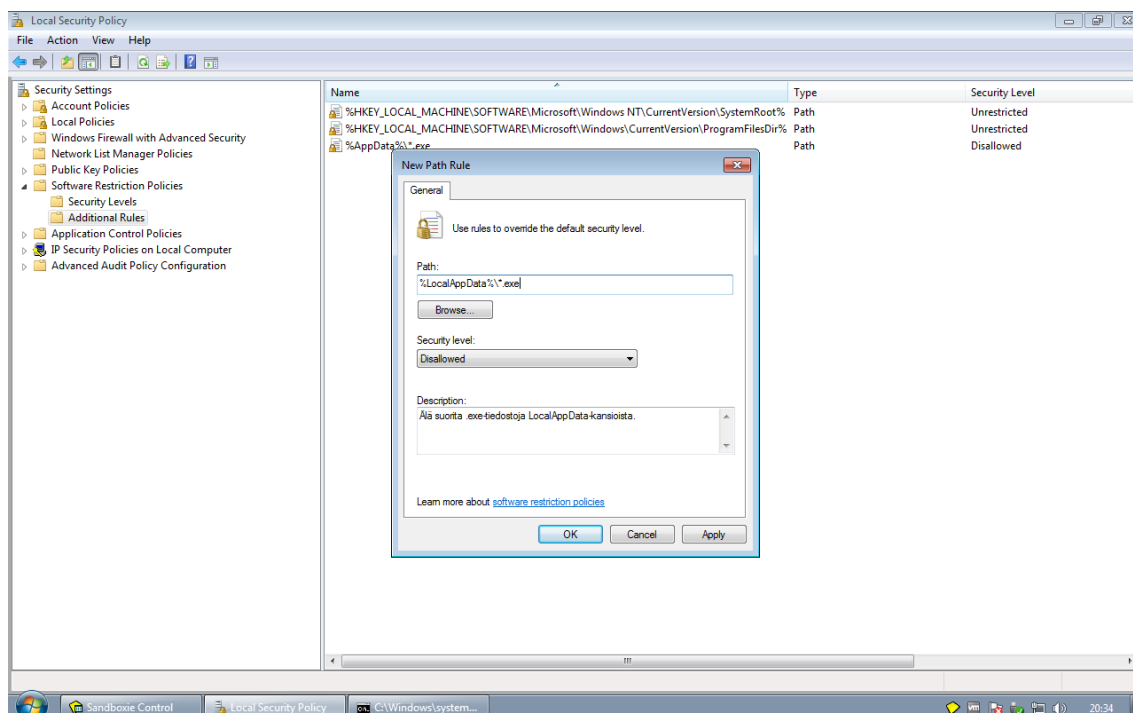
CryptoLockerin suorituksen estämiseksi on yksi hyvin spesifinen, mutta tehokas tapa, jota testattiin käytännössä (Abrams 2013). Tätä varten tarvittiin käyttöön Local Security Policy -ohjelma, jonka saa käynnistettyä painamalla Win+R ja kirjoittamalla käynnistyskohtaan secpol.msc (Kuva 17).



Kuva 17. Local Security Policy.

Seuraavaksi ohjelmassa luotiin sääntö, joka estää exe-päätteisten tiedostojen suorittamisen %LocalAppData%-hakemistossa, eli hakemistossa, jossa CryptoLocker toimii.

Tämän sääntö luotiin valitsemalla oikealla hiiren näppäimellä Software Restriction Policies -kansion alta kohta Additional Rules. Tästä auenneesta valikosta valittiin New Path Rule. Path-kohtaan kirjoitettiin “%LocalAppData%*.exe”, Security Level -kohtaan valittiin Disallowed (Kuva 18).



Kuva 18. Uuden säännön luominen.

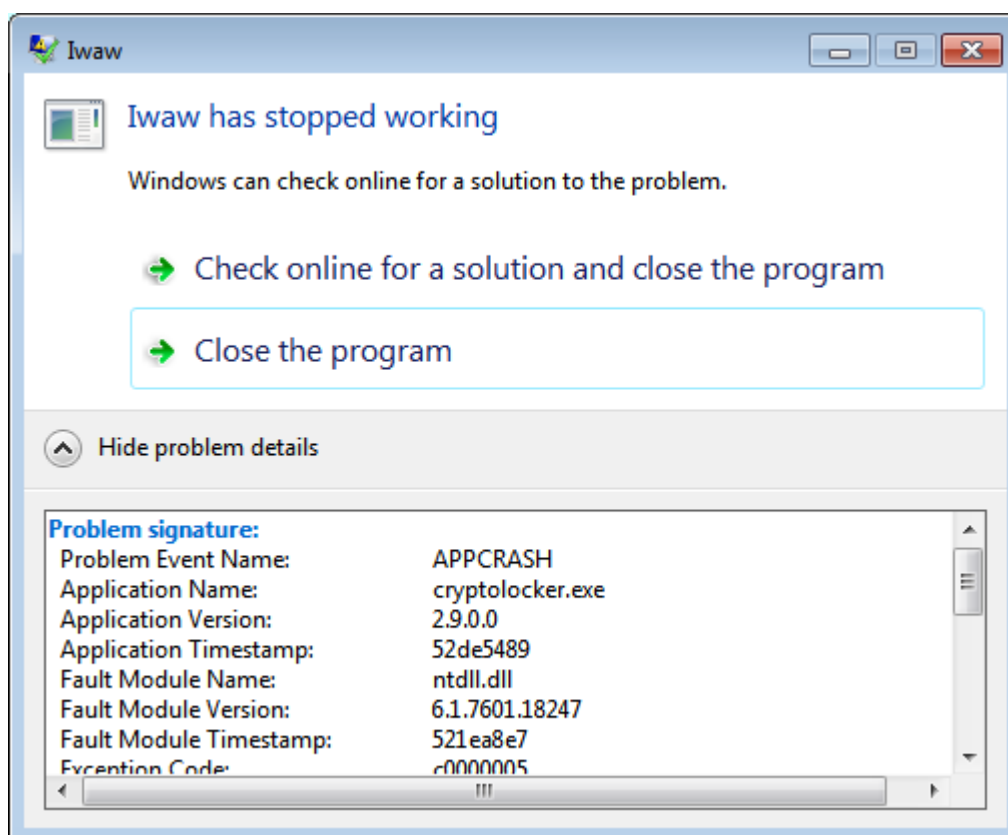
Kuten yllä olevasta kuvankaappauksesta voi havaita (Kuva 18) myös %AppData%-hakemiston exe-tiedostojen suorittaminen on estetty. Tämä ei kuitenkaan ole tarpeellista testissä käytetyn CryptoLocker-version taltuttamiseksi, koska se ei käytä kyseistä hakemistoa mihinkään.

23:50:40.3080070	cryptolocker.exe	856	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length:
23:50:40.3080341	cryptolocker.exe	856	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\...	SUCCESS	Type: REG_SZ, Length: 2, Data:
23:50:40.3080644	cryptolocker.exe	856	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\...	SUCCESS	Type: REG_QWORD, Length: 8, Data:
23:50:40.3080961	cryptolocker.exe	856	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\...	SUCCESS	
23:50:40.3082347	cryptolocker.exe	856	CloseFile	C:\Users\Test\AppData\Local\vmhgntf.exe	SUCCESS	
23:50:40.3083621	vmhgntf.exe	2440	Load Image	C:\Users\Test\AppData\Local\vmhgntf.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x63000
23:50:40.3085450	vmhgntf.exe	2440	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x771a0000, Image Size: 0x1a9000
23:50:40.3086948	vmhgntf.exe	2440	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77380000, Image Size: 0x180000
23:50:40.3089659	vmhgntf.exe	2440	CreateFile	C:\Windows\Prefetch\MRHGRHTE.EXE-ECC06301.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options: Sync
23:50:40.3090349	vmhgntf.exe	2440	Thread Exit		SUCCESS	Thread ID: 2264, User Time: 0.0000000, Kernel Time: 0.0156001
23:50:40.3090951	vmhgntf.exe	2440	QueryNameInformationFile	C:\Windows\System32\apisetschema.dll	SUCCESS	Name: \Windows\System32\apisetschema.dll
23:50:40.3091549	vmhgntf.exe	2440	QueryNameInformationFile	C:\Users\Test\AppData\Local\vmhgntf.exe	SUCCESS	Name: \Users\Test\AppData\Local\vmhgntf.exe
23:50:40.3092039	vmhgntf.exe	2440	QueryNameInformationFile	C:\Windows\System32\ntdll.dll	SUCCESS	Name: \Windows\System32\ntdll.dll
23:50:40.3092701	vmhgntf.exe	2440	QueryNameInformationFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Name: \Windows\SysWOW64\ntdll.dll
23:50:40.3093298	vmhgntf.exe	2440	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.01:
23:50:40.3094708	cryptolocker.exe	856	CreateFile	C:\	SUCCESS	Desired Access: Synchronize, Disposition: Open, Options: Direct
23:50:40.3095249	cryptolocker.exe	856	QueryNameInformationFile	C:\	SUCCESS	Name: \
23:50:40.3095645	cryptolocker.exe	856	QueryInformationVolume	C:\	SUCCESS	VolumeCreationTime: 29.5.2014 9:49:08, VolumeSerialNumber: F
23:50:40.3096005	cryptolocker.exe	856	CloseFile	C:\	SUCCESS	

Kuva 19. Kuvankaappaus osasta Process Monitor -lokiä.

Local Security Policy -säännön toimivuus todettiin käyttämällä Process Monitor - ja Wireshark-ohjelmia. Process Monitor -ohjelman lokeista paljastui, että CryptoLocker siirsi kopion itsestään %LocalAppData%-hakemistoon ja yritti aloittaa

toiminnan, mutta ei pystynyt toimimaan halutulla tavalla ja ylipäättäänkin vain sekunnin murto-osia, koska oikeuksia oli rajoitettu (Kuva 19).



Kuva 20. CryptoLockerin suoritus keskeytyy.

Hetken tyhjäkäynnin jälkeen CryptoLocker kaatui ja sen suoritus loppui (Kuva 20). Wiresharkiin ei tullut minkäänlaista lokitietoa verkkoliikenteestä ja myös testitiedostot pysyivät salaamattomina.

6 TYÖN TOTEUTTAMISEN HAASTEET

Testiympäristöä varten saatu tietokone oli resursseiltaan aivan liian tehoton suorittamaan virtuaalikoneita jouhevasti. Varsinkin keskusmuistin vähäinen määrä aiheutti sen, että tietokone joutui käyttämään hidasta massamuistia, eli tässä tapauksessa kiintolevyä, "swappaamiseen".

Testiympäristön ohjelmiksi olisi mielellään valittu avoimeen lähdekoodiin perustuvia ohjelmistoja. Näitä ei kuitenkaan löytynyt tarvittavilla ominaisuuksilla varusteltuna kuin oikeastaan Ubuntu-käyttöjärjestelmä. Onneksi koulun kautta saatiin hankittua tarvittavat lisenssit maksullisiin ohjelmiin.

Virtuaalikoneiden luomisessa oli ongelmia, koska VMware ilmoitti prosessorin virtualisointiominaisuuden puutteesta. 32-bittinen käyttöjärjestelmä asentui ongelmitta, mutta 64-bittinen ei. Ongelma korjaantui laittamalla Virtualization Technology -ominaisuus päälle tietokoneen BIOS:sta.

Itse CryptoLocker-ohjelman etsiminen oli vaikeaa, koska ei tiennyt mistä alkaa etsiä. Internetissä ei ole olemassa ainakaan julkisesti mitään keskitettyä haittaohjelmatietokantaa. "CryptoLocker"-hakusanalla etsimällä ei löydy itse haittaohjelmaa, vaan tietoa siitä. CryptoLocker kuitenkin löytyi lopulta onnen kaupalla ja vielä luotettavan IT-yrityksen verkkosivuilta.

Ongelmaksi muodostui myös testiympäristön pääsy julkiseen verkkoon, jota ilman CryptoLocker ei pysty toimimaan. Koulun verkon käyttämiseen olisi tarvittu huomattava määrä selvitystyötä ja yhteydenottoja useisiin verkkoa ylläpitäviin tahoihin. Tähän kuitenkaan ei ryhdytty, vaan päädyttiin käyttämään omia yhteyksiä testauksessa.

Käytetyn CryptoLocker-version isäntäpalvelin lakkasi vastaamasta pyyntöihin testauksen loppupuolella. On syytä olettaa, että palvelin on tietoisesti otettu pois verkosta esimerkiksi viranomaisen toimesta. Tarpeelliset testaustoimenpiteet saatiin kuitenkin suoritettua ennen palvelimen alasajoa.

7 POHDINTA

Opinnäytetyön empiriaosan tavoitteena oli tutkia salaavan ransomwaren toimintaa yksityiskohtaisemmin. Aloitimme työn suljetun ympäristön toteutussuunnitelmalla. Päätettyämme mitä ohjelmistoja käyttäisimme ympäristössä ja miten, aloitimme ympäristön toteutuksen. Lopputulos oli mieleinen, vaikka ongelmilta ei välttyttykään.

Opimme työn aikana Linux-käyttöjärjestelmästä paljon uutta asiaa. Vaikka CryptoLocker toimii vain Windows-käyttöjärjestelmässä, päätimme ajaa virtuaalikooneet Linux-käyttöjärjestelmässä. Lisäksi Wireshark-analysointiohjelma ajettiin Linuxin puolella. Wiresharkia opimme käyttämään tehokkaammin ja tulkitsemaan lokitietoja tarkemmin.

CryptoLockerista huomasimme saman mitä useat muutkin tietokoneenkäyttäjät ja haittaohjelman uhrit: se on erittäin vaarallinen haittaohjelma, joka tekee tuhoa mahdollisesti tärkeille tiedostoille. Totesimme kuitenkin, että testaamassamme CryptoLockerin versiossa oli suuri heikkous: kun haittaohjelman käyttämä palvelin joutui alas ajetuksi, ei haittaohjelma pystynyt enää toimimaan. CryptoLocker olisi voinut tehdä peruuttamatonta tuhoa tiedostoille kuten virukset, mutta jätti sen tekemättä.

Syynä lienee se, että kiristyshaittaohjelman maine olisi saattanut tahraantua, niin ironiselta kuin se kuulostaakin. Jos peruuttamatonta tuhoa olisi tehty tiedostoille, uutinen asiasta olisi levinnyt saman tien tiedotusvälineisiin ja harrastajafoorumeille, ja luotto siihen, että maksamalla lunnaat tiedostot palautuvat. Tällöin vähemmistö uhreista maksaisi ja rikollisten tulot pienenisivät.

Havaitsimme myös, että CryptoLocker-ohjelman saa poistettua tietokoneelta hyvin pienellä vaivalla ja sen esimerkiksi jokainen paremman luokan virustorjuntaohjelma tekee automaattisesti. Siitä on hyötyä vielä silloin, kun haittaohjelmaa ei ole ehtinyt käynnistämään.

Jos CryptoLocker on saanut jo tiedostot salattua, siitä on enemmän haittaa kuin hyötyä. Tällöin uhri, joka haluaisi kaikesta huolimatta tiedostot palauttaa, ei sitä pysty tekemään, koska CryptoLocker on ainakin vielä tällä hetkellä täysin murtamaton. Ainoastaan maksamalla saadaan tiedostot palautettua, jos varmuuskopiot ovat jääneet tekemättä.

Testin suorittamisen jälkeen tulimme siihen tulokseen, että CryptoLocker käyttäytyy samalla tavalla molemmilla Windows-käyttöjärjestelmillä. Haittaohjelma suorittaa itsensä molemmissa samankaltaisesti ja lopputulokset ovat samat: tiedostot salautuvat. Windows 7:n uusista tietoturvaominaisuuksista ei hyötyä kiristyshaittaohjelman torjumiseen ole. Tästä syystä jätimme kahden eri käyttöjärjestelmän erottamisen toisistaan käsittelemättä tarkemmin.

Toivomme, että opinnäytetyömme innostaa jatkamaan ransomwaren ja erityisesti salaavien kiristyshaittaohjelmien tutkimista. Rakentamaamme testiympäristöä voi käyttää myös muidenkin haittaohjelmien tutkimiseen joko sellaisenaan tai hienosäätämällä oman maun mukaan. Toivottavasti esimerkki testiympäristöstämme antaa suuntaviivoja muille rakentaa vielä parempi, tehokkaampi ja helposti hallittavampi testiympäristö haittaohjelmatutkimukselle.

Toivottavaa olisi, että myös CryptoLockerin kaltaisten kiristyshaittaohjelmien salaukset pystyttäisiin murtamaan ilman lunnaiden maksamista. Vaikeaa se tulee olemaan, mutta toivottavasti ei mahdotonta.

LÄHTEET

- Abrams, L. 2013. CryptoLocker Ransomware Information Guide and FAQ. Viitattu 8.5.2014 <http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information>.
- Emelyanova, O. & Nazarov, D. 2006. Blackmailer: the story of Gpcode. Viitattu 8.5.2014 <http://www.securelist.com/en/analysis?pubid=189678219>.
- European Cybercrime Centre 2014. Police Ransomware Threat Assessment. Viitattu 15.5.2014 <https://www.europol.europa.eu/sites/default/files/publications/policeransomware-threatassessment.pdf>.
- F-Secure Labs 2013. Threat Report H1 2013. Viitattu 5.5.2014 http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf.
- Ferguson, D. 2013. CryptoLocker attacks that hold your computer to ransom. Viitattu 5.5.2014 <http://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomware>.
- Foss, Alan. 2013. How to Remove Win32/Reveton Infection (Ransomware Removal Guide). Viitattu 20.5.2014 <http://www.dotfab.com/resources/how-to-remove-win32reveton-infection-ransomware-removal-guide>.
- Gibson Research Corporation 2014. Malware Research Experimental Repository. Viitattu 8.5.2014 <https://www.grc.com/malware.htm>.
- Hamada, J. 2013. FakeAV holds Android Phones or Ransom. Viitattu 6.5.2014 <http://www.symantec.com/connect/blogs/fakeav-holds-android-phones-ransom>.
- Hawes, J. 2014. 1 in 30 have been hit by CryptoLocker and 40% pay the ransom, says study. Viitattu 5.5.2014 <http://nakedsecurity.sophos.com/2014/03/07/1-in-30-have-been-hit-by-cryptolocker-and-40-pay-the-ransom-says-study>.
- Hoffman, C. 2013a. 10 Important Computer Security Practices You Should Follow. Viitattu 6.5.2014 <http://www.howtogeek.com/173478/10-important-computer-security-practices-you-should-follow>.
- Hoffman, C. 2013b. Why the 64-bit Version of Windows is More Secure. Viitattu 6.5.2014 <http://www.howtogeek.com/165535/why-the-64-bit-version-of-windows-is-more-secure>.
- Jarvis, K. 2013. CryptoLocker Ransomware. Viitattu 20.5.2014 <http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware>.
- Kaspersky Lab 2008. Kaspersky Lab reports a new and dangerous blackmailing virus. Viitattu 8.5.2014 http://www.kaspersky.com/about/news/virus/2008/Kaspersky_Lab_reports_a_new_and_dangerous_blackmailing_virus.
- Kassner, M. 2010. Ransomware: Extortion via the Internet. Viitattu 8.5.2014 <http://www.techrepublic.com/blog/it-security/ransomware-extortion-via-the-internet/2976>.
- Lubuntu 2014. Lubuntu. Viitattu 6.5.2014 <http://lubuntu.net>.
- McAfee Labs 2013a. McAfee Threats Report: First Quarter 2013. Viitattu 16.2.2014 <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf>.
- McAfee Labs 2013b. McAfee Labs Threats Report: Third Quarter 2013. Viitattu 16.2.2014 <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf>.

McAfee Labs 2013c. McAfee Labs 2014 Threats Predictions. Viitattu 5.5.2014 <http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf>.

Microsoft 2005. X.509 Technical Supplement. Viitattu 3.6.2014 <http://msdn.microsoft.com/en-us/library/ff647097.aspx>.

Microsoft 2014. Windows XP support has ended. Viitattu 6.5.2014 <http://windows.microsoft.com/en-US/windows/end-support-help>.

NetMarketShare 2014. Desktop Operating System Market Share. Viitattu 6.5.2014 <http://www.netmarketshare.com/report.aspx?qprid=10&qptimeframe=M&qpsp=181&qpch=350&qpmr=24&qpdt=1&qpct=3&qpcustomd=0&qpcid=fw494472&qpf=1>.

Ortega, A. 2013. Urausy ransomware family, a quick internals overview. Viitattu 8.5.2014 <http://www.alienvault.com/open-threat-exchange/blog/urausy-ransomware-family-a-quick-internals-overview>.

VMware 2014. VMware KB: Working with snapshots. Viitattu 6.5.2014 http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1009402.

Wireshark-loki

Ote Wireshark-lokista:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.222.129	192.168.222.2	DNS	77	Standard query 0x8b43 A shalunishka12.org

Frame 1: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)

Ethernet II, Src: Vmware_3b:8d:be (00:0c:29:3b:8d:be), Dst: Vmware_f5:79:77 (00:50:56:f5:79:77)

Internet Protocol Version 4, Src: 192.168.222.129 (192.168.222.129), Dst: 192.168.222.2 (192.168.222.2)

User Datagram Protocol, Src Port: 65484 (65484), Dst Port: domain (53)

Domain Name System (query)

[Response In: 4]

Transaction ID: 0x8b43

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

shalunishka12.org: type A, class IN

Name: shalunishka12.org

Type: A (Host address)

Class: IN (0x0001)

No.	Time	Source	Destination	Protocol	Length	Info
4	0.105340	192.168.222.2	192.168.222.129	DNS	129	

Standard query response 0x8b43 A 77.72.133.146

Frame 4: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits)

Ethernet II, Src: Vmware_f5:79:77 (00:50:56:f5:79:77), Dst: Vmware_3b:8d:be (00:0c:29:3b:8d:be)

Internet Protocol Version 4, Src: 192.168.222.2 (192.168.222.2), Dst: 192.168.222.129 (192.168.222.129)

User Datagram Protocol, Src Port: domain (53), Dst Port: 65484 (65484)

Domain Name System (response)

[Request In: 1]

[Time: 0.105340000 seconds]

Transaction ID: 0x8b43

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 2

Additional RRs: 0

Queries

shalunishka12.org: type A, class IN

Name: shalunishka12.org

Type: A (Host address)

Class: IN (0x0001)

Answers

shalunishka12.org: type A, class IN, addr 77.72.133.146

Name: shalunishka12.org

Type: A (Host address)

Class: IN (0x0001)

Time to live: 5 seconds

Data length: 4

Addr: 77.72.133.146 (77.72.133.146)

Authoritative nameservers

shalunishka12.org: type NS, class IN, ns ns2.shalunishka12.org

Name: shalunishka12.org

Type: NS (Authoritative name server)

Class: IN (0x0001)

Time to live: 5 seconds

Data length: 6

Name Server: ns2.shalunishka12.org

shalunishka12.org: type NS, class IN, ns ns1.shalunishka12.org

Name: shalunishka12.org

Type: NS (Authoritative name server)

Class: IN (0x0001)

Time to live: 5 seconds

Data length: 6

Name Server: ns1.shalunishka12.org

No.	Time	Source	Destination	Protocol	Length	Info
5	0.137619	192.168.222.129	77.72.133.146	TCP	62	xrl > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1

Frame 5: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Ethernet II, Src: Vmware_3b:8d:be (00:0c:29:3b:8d:be), Dst: Vmware_f5:79:77 (00:50:56:f5:79:77)

Internet Protocol Version 4, Src: 192.168.222.129 (192.168.222.129), Dst: 77.72.133.146 (77.72.133.146)

Transmission Control Protocol, Src Port: xrl (1104), Dst Port: http (80), Seq: 0, Len: 0

Source port: xrl (1104)

Destination port: http (80)

[Stream index: 0]

Sequence number: 0 (relative sequence number)

Header length: 28 bytes

Flags: 0x002 (SYN)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... .0. = Urgent: Not set

.... ...0 = Acknowledgment: Not set

.... 0... = Push: Not set

....0.. = Reset: Not set

....1. = Syn: Set

....0 = Fin: Not set

Window size value: 64240

[Calculated window size: 64240]

Checksum: 0x99ff [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted

No.	Time	Source	Destination	Protocol	Length	Info
6	0.203879	77.72.133.146	192.168.222.129	TCP	60	http > xrl [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Vmware_f5:79:77 (00:50:56:f5:79:77), Dst: Vmware_3b:8d:be (00:0c:29:3b:8d:be)

Internet Protocol Version 4, Src: 77.72.133.146 (77.72.133.146), Dst: 192.168.222.129 (192.168.222.129)

Transmission Control Protocol, Src Port: http (80), Dst Port: xrl (1104), Seq: 0, Ack: 1, Len: 0

Source port: http (80)

Destination port: xrl (1104)

[Stream index: 0]

Sequence number: 0 (relative sequence number)

Acknowledgment number: 1 (relative ack number)

Header length: 24 bytes

Flags: 0x012 (SYN, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 0... = Push: Not set

....0.. = Reset: Not set

....1. = Syn: Set

....0 = Fin: Not set

Window size value: 64240

[Calculated window size: 64240]

Checksum: 0x1fda [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

Options: (4 bytes), Maximum segment size

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 5]

[The RTT to ACK the segment was: 0.066260000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
7	0.203987	192.168.222.129	77.72.133.146	TCP	54	xrl > http [ACK] Seq=1 Ack=1 Win=64240 Len=0

Frame 7: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: Vmware_3b:8d:be (00:0c:29:3b:8d:be), Dst: Vmware_f5:79:77 (00:50:56:f5:79:77)

Internet Protocol Version 4, Src: 192.168.222.129 (192.168.222.129), Dst: 77.72.133.146 (77.72.133.146)

Transmission Control Protocol, Src Port: xrl (1104), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

Source port: xrl (1104)

Destination port: http (80)

[Stream index: 0]

Sequence number: 1 (relative sequence number)

Acknowledgment number: 1 (relative ack number)

Header length: 20 bytes

Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 0... = Push: Not set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

Window size value: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x3797 [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 6]

[The RTT to ACK the segment was: 0.000108000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
8	0.204534	192.168.222.129	77.72.133.146	TCP	318	[TCP segment of a reassembled PDU]

Frame 8: 318 bytes on wire (2544 bits), 318 bytes captured (2544 bits)

Ethernet II, Src: Vmware_3b:8d:be (00:0c:29:3b:8d:be), Dst: Vmware_f5:79:77 (00:50:56:f5:79:77)

Internet Protocol Version 4, Src: 192.168.222.129 (192.168.222.129), Dst: 77.72.133.146 (77.72.133.146)

Transmission Control Protocol, Src Port: xrl (1104), Dst Port: http (80), Seq: 1, Ack: 1, Len: 264

Source port: xrl (1104)

Destination port: http (80)

[Stream index: 0]

Sequence number: 1 (relative sequence number)

[Next sequence number: 265 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header length: 20 bytes

Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

Window size value: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x0085 [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[SEQ/ACK analysis]

[Bytes in flight: 264]

TCP segment data (264 bytes)

No.	Time	Source	Destination	Protocol	Length	Info
9	0.204752	77.72.133.146	192.168.222.129	TCP	60	http > xrl [ACK] Seq=1 Ack=265 Win=64240 Len=0

Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Vmware_f5:79:77 (00:50:56:f5:79:77), Dst: Vmware_3b:8d:be (00:0c:29:3b:8d:be)

Internet Protocol Version 4, Src: 77.72.133.146 (77.72.133.146), Dst: 192.168.222.129 (192.168.222.129)

Transmission Control Protocol, Src Port: http (80), Dst Port: xrl (1104), Seq: 1, Ack: 265, Len: 0

Source port: http (80)

Destination port: xrl (1104)

[Stream index: 0]

Sequence number: 1 (relative sequence number)

Acknowledgment number: 265 (relative ack number)

Header length: 20 bytes

Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 0... = Push: Not set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

Window size value: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x368f [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 8]

[The RTT to ACK the segment was: 0.000218000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
10	0.205051	192.168.222.129	77.72.133.146	HTTP	1507	POST /e.php HTTP/1.1 (application/x-www-form-urlencoded)

Frame 10: 1507 bytes on wire (12056 bits), 1507 bytes captured (12056 bits)

Ethernet II, Src: Vmware_3b:8d:be (00:0c:29:3b:8d:be), Dst: Vmware_f5:79:77 (00:50:56:f5:79:77)

Internet Protocol Version 4, Src: 192.168.222.129 (192.168.222.129), Dst: 77.72.133.146 (77.72.133.146)

Transmission Control Protocol, Src Port: xrl (1104), Dst Port: http (80), Seq: 265, Ack: 1, Len: 1453

Source port: xrl (1104)

Destination port: http (80)

[Stream index: 0]

Sequence number: 265 (relative sequence number)

[Next sequence number: 1718 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header length: 20 bytes

Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

Window size value: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x75ac [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[SEQ/ACK analysis]

[Bytes in flight: 1453]

TCP segment data (1453 bytes)

[2 Reassembled TCP Segments (1717 bytes): #8(264), #10(1453)]

Hypertext Transfer Protocol

POST /e.php HTTP/1.1\r\n

[Expert Info (Chat/Sequence): POST /e.php HTTP/1.1\r\n]

[Message: POST /e.php HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: POST

Request URI: /e.php

Request Version: HTTP/1.1

Content-Type: application/x-www-form-urlencoded\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:26.0)
Gecko/20100101 Firefox/26.0\r\n

Host: shalunishka12.org\r\n

Content-Length: 1453\r\n

[Content length: 1453]

Connection: Keep-Alive\r\n

Cache-Control: no-cache\r\n

\r\n

[Full request URI: http://shalunishka12.org/e.php]

[HTTP request 1/1]

[Response in frame: 12]

Line-based text data: application/x-www-form-urlencoded

[truncated]

da-

ta=ATAxOGZiMTViMjE0YmIxYTcABgAAz+NMFx1gniUk0SLUcASSrYvtceHlVV
X6RMWzyAlvyvOMno8rQgoK7LiJr5kGKtzaRKHIq98gKI3J8Q2/blsKFuPj3a1XTI
7JgVnLtMB+H1WEbxT2BNN1TvTnFiUOnTEkAanoyJ/49BkVTIZ6mzQNHf93q5
gOuy2OACRV/vuxQTiD8V46/3+StWhRN899WCkky4

\r

[truncated]

1vE4AFxooWLQfNGTH9t7W/R8HCUndfe1F2Ggn1QUbNQvwkTmAG1SywTco
QsNp2ikXMbyvw4fccUbUDhP4FLKqJnFfV3Dlkk3KeZHnNJfcHwr1ShjiUYyXds
HvXvVLvLuFKErFjhFQtBHLtCzRITFX-
PRlvNtj+V0VWPhkGUmQ/HDEBON+mIJfE0zynmVb4Hk3X/y5KV+6BsyNdasR
9hNdzJvRGZmas/h/hnw

\r

[truncated]

YiHq+jYOqYwGSTDWQh/yrYaf8oVVd4bwwDL7AGlhh9gJSC6AXrp//vs9Trre67If
dl9bEr3qLTGEbXSntVQiXVi/JWeyhSjg/LhK/t3giKWYzXv8FHphPexIXOxgndP5
YMnSkd01jmoUUzr6qd9xphj/ZjUrma+5bX1NkhQQYhnIjKjLSpkVQi5Q5PH/e+x
xMv1LBfdQn55tRbY6rnhudRIflOOsNu8oX1j

\r

[truncated]

AFsLdVdKT8z4TKkj22guJjQY20OglNgTrKF85ynz+ZoRNtiJedsIxfQYMDFKVi6
dKJ5f7zeJGLCKDRozzpkA3SHy/stsTbOeU/L/XH6gfMjWRstjTJ9KiMAGMEUSy
/vIOYoa9X61bJjKOkIqWJFeo0DaT/aOYAMq8QbtsUR1Td+1k8ks0zk+Y57d1dj
O3CNaE3dOnoi9VHyeYjIFGNBNtw0J1D/cedEHfZ

\r

[truncated]

OGKnHsuPMnjYJOCmDb0O6p4Ztwh83zlrN0qUtj43VrhlJ0/F3C9hxiZmV0nhaB
A2kUIaKWcoHYdbNEEuXmDXSFQEF9T9dAl/zMwJWpVGAzNzzkw8iQ/ZXwC
gJwzdk-
snf79WKj1sFtZm5bfeHtK2kEmv6yInK9a0fmTnAEnBWH2dDkxYjt7wagxE+qg8
Zi/cAlj4342d1XHa7iawPVGEQOnkCIGE/Sco2jc9

\r

kQ7c6uoNCjtD+y3QsKDXyX0J2pp1MMtSnTTcKdoUMvTsr/5TOHHkV0ZbQBtu
3Bdsp7qKPbAMF0aPe2LN1mg/nUr9BX9REL736WmTsTJQQO/T4Ghvl2E7Au
0oEe7R5wo4BdJMw8RmTTeFTUU5/LwqVczWBTg3+IBIs4ILmOjco1yyKJMu\n

\r

No.	Time	Source	Destination	Protocol	Length	Info
11	0.205454	77.72.133.146	192.168.222.129	TCP	60	http > xrl [ACK] Seq=1 Ack=1718 Win=64240 Len=0

Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Vmware_f5:79:77 (00:50:56:f5:79:77), Dst: Vmware_3b:8d:be (00:0c:29:3b:8d:be)

Internet Protocol Version 4, Src: 77.72.133.146 (77.72.133.146), Dst: 192.168.222.129 (192.168.222.129)

Transmission Control Protocol, Src Port: http (80), Dst Port: xrl (1104), Seq: 1, Ack: 1718, Len: 0

Source port: http (80)

Destination port: xrl (1104)

[Stream index: 0]

Sequence number: 1 (relative sequence number)

Acknowledgment number: 1718 (relative ack number)

Header length: 20 bytes

Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 0... = Push: Not set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

Window size value: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x30e2 [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 10]

[The RTT to ACK the segment was: 0.000403000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
12	0.382258	77.72.133.146	192.168.222.129	HTTP	257	HTTP/1.1 200 OK

Frame 12: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits)

Ethernet II, Src: Vmware_f5:79:77 (00:50:56:f5:79:77), Dst: Vmware_3b:8d:be (00:0c:29:3b:8d:be)

Internet Protocol Version 4, Src: 77.72.133.146 (77.72.133.146), Dst: 192.168.222.129 (192.168.222.129)

Transmission Control Protocol, Src Port: http (80), Dst Port: xrl (1104), Seq: 1, Ack: 1718, Len: 203

Source port: http (80)

Destination port: xrl (1104)

[Stream index: 0]

Sequence number: 1 (relative sequence number)

[Next sequence number: 204 (relative sequence number)]

Acknowledgment number: 1718 (relative ack number)

Header length: 20 bytes

Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

Window size value: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x635a [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[SEQ/ACK analysis]

[Bytes in flight: 203]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[Message: HTTP/1.1 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Version: HTTP/1.1

Status Code: 200

Response Phrase: OK

Server: nginx\r\n

Date: Thu, 27 Feb 2014 17:42:40 GMT\r\n

Content-Type: text/html; charset=utf-8\r\n

Content-Length: 0\r\n

[Content length: 0]

Connection: keep-alive\r\n

Keep-Alive: timeout=60\r\n

X-Powered-By: PHP/5.3.3\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.177207000 seconds]

[Request in frame: 10]

No.	Time	Source	Destination	Protocol	Length	Info
14	0.482408	192.168.222.129	77.72.133.146	TCP	54	xrl > http [ACK] Seq=1718 Ack=204 Win=64037 Len=0

Frame 14: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: Vmware_3b:8d:be (00:0c:29:3b:8d:be), Dst: Vmware_f5:79:77 (00:50:56:f5:79:77)

Internet Protocol Version 4, Src: 192.168.222.129 (192.168.222.129), Dst: 77.72.133.146 (77.72.133.146)

Transmission Control Protocol, Src Port: xrl (1104), Dst Port: http (80), Seq: 1718, Ack: 204, Len: 0

Source port: xrl (1104)

Destination port: http (80)

[Stream index: 0]

Sequence number: 1718 (relative sequence number)

Acknowledgment number: 204 (relative ack number)

Header length: 20 bytes

Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 0... = Push: Not set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

Window size value: 64037

[Calculated window size: 64037]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x30e2 [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 12]

[The RTT to ACK the segment was: 0.100150000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
19	60.822505	77.72.133.146	192.168.222.129	TCP	60	http > xrl [FIN, PSH, ACK] Seq=204 Ack=1718 Win=64240 Len=0

Frame 19: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Vmware_f5:79:77 (00:50:56:f5:79:77), Dst: Vmware_3b:8d:be (00:0c:29:3b:8d:be)

Internet Protocol Version 4, Src: 77.72.133.146 (77.72.133.146), Dst: 192.168.222.129 (192.168.222.129)

Transmission Control Protocol, Src Port: http (80), Dst Port: xrl (1104), Seq: 204, Ack: 1718, Len: 0

Source port: http (80)

Destination port: xrl (1104)

[Stream index: 0]

Sequence number: 204 (relative sequence number)

Acknowledgment number: 1718 (relative ack number)

Header length: 20 bytes

Flags: 0x019 (FIN, PSH, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....1 = Fin: Set

Window size value: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x300e [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

No.	Time	Source	Destination	Protocol	Length	Info
20	60.822638	192.168.222.129	77.72.133.146	TCP	54	xrl > http [ACK] Seq=1718 Ack=205 Win=64037 Len=0

Frame 20: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: Vmware_3b:8d:be (00:0c:29:3b:8d:be), Dst: Vmware_f5:79:77 (00:50:56:f5:79:77)

Internet Protocol Version 4, Src: 192.168.222.129 (192.168.222.129), Dst: 77.72.133.146 (77.72.133.146)

Transmission Control Protocol, Src Port: xrl (1104), Dst Port: http (80), Seq: 1718, Ack: 205, Len: 0

Source port: xrl (1104)

Destination port: http (80)

[Stream index: 0]

Sequence number: 1718 (relative sequence number)

Acknowledgment number: 205 (relative ack number)

Header length: 20 bytes

Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 0... = Push: Not set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

Window size value: 64037

[Calculated window size: 64037]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x30e1 [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 19]

[The RTT to ACK the segment was: 0.000133000 seconds]

Regshot-loki

Regshot 1.9.0 x86 Unicode

Comments: CryptoLocker (Windows XP)

Datetime: 2014/2/27 16:59:03 , 2014/2/27 17:19:36

Computer: TUAS-TIKO-LABXP , TUAS-TIKO-LABXP

Username: User , User

Values deleted: 23

HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces\Tcpip_{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpNameServerList: 31 00 39 00 32 00 2E 00 31 00 36 00 38 00 2E 00 32 00 32 00 32 00 2E 00 32 00 00 00 00 00

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\DhcpNameServer: "192.168.222.2"

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\DhcpDomain: "localdomain"

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpRetryTime: 0x00000384

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpRetryStatus: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpNameServer: "192.168.222.2"

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpDefaultGateway: 31 00 39 00 32 00 2E 00 31 00 36 00 38 00 2E 00 32 00 32 00 32 00 2E 00 32 00 00 00 00 00

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpDomain: "localdomain"

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpSubnetMaskOpt: 32 00 35 00 35 00 2E 00 32 00 35 00 35 00 2E 00 32 00 35 00 35 00 2E 00 30 00 00 00 00 00

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\DhcpDefaultGateway: 31 00 39 00 32 00 2E 00 31 00 36 00 38 00 2E 00 32 00 32 00 32 00 2E 00 32 00 00 00 00 00

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\DhcpSubnetMaskOpt: 32 00 35 00 35 00 2E 00 32 00 35 00 35 00 2E 00 32 00 35 00 35 00 2E 00 30 00 00 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\Tcpip_{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpNameServerList: 31 00 39 00 32 00 2E 00 31 00 36 00 38 00 2E 00 32 00 32 00 32 00 2E 00 32 00 00 00 00 00 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DhcpNameServer: "192.168.222.2"

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DhcpDomain: "localdomain"

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpRetryTime: 0x00000384

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpRetryStatus: 0x00000000

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpNameServer: "192.168.222.2"

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpDefaultGateway: 31 00 39 00 32 00 2E 00 31 00 36 00 38 00 2E 00 32 00 32 00 32 00 2E 00 32 00 00 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpDomain: "localdomain"

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\DhcpSubnetMaskOpt: 32 00 35 00 35 00 2E 00 32 00 35 00 35 00 2E 00 32 00 35 00 35 00 2E 00 30 00 00 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\DhcpDefaultGateway: 31 00 39 00 32 00 2E 00 31 00 36 00 38 00 2E 00 32 00 32 00 32 00 2E 00 32 00 00 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\DhcpSubnetMaskOpt: 32 00 35 00 35 00 2E 00 32 00 35 00 35 00 2E 00 32 00 35 00 35 00 2E 00 30 00 00 00 00 00

HKU\S-1-5-21-299502267-1004336348-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\1: 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 74 00 78 00 74 00 00 00 66 00 32 00 00 00 00 00 00 00 00 00 00 00 74 65 73 74 69 74 69 65 64 6F 73 74 6F 2E 74 78 74 2E 6C 6E 6B 00 42 00 03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 74 00 78 00 74 00 2E 00 6C 00 6E 00 6B 00 00 00 24 00 00 00

Values added: 7

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\..txt\2:

74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F
00 2E 00 74 00 78 00 74 00 00 00 66 00 32 00 00 00 00 00 00 00 00 00 00
74 65 73 74 69 74 69 65 64 6F 73 74 6F 2E 74 78 74 2E 6C 6E 6B 00 42 00 03
00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00 00 00 74 00 65 00 73 00 74 00
69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 74 00 78 00 74
00 2E 00 6C 00 6E 00 6B 00 00 00 24 00 00 00

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{750487
00-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:Cebprff Un-
pxre 2.yax: 02 00 00 00 06 00 00 00 20 26 68 A1 DD 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{750487
00-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Cebtenz
Svyrf\Cebprff Unpxre 2\CebprffUnpxre.rkr: 02 00 00 00 06 00 00 00 10 6B D3
A1 DD 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{750487
00-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf
naq Frggvatf\Hfre\Qrfxgbc\44217P15S30538N1SOQS614P9785P9O7.rkr: 02
00 00 00 06 00 00 00 F0 90 D2 8B DF 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\CurrentVersion\Run\: 43 00 3A 00 5C 00 44
00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00
20 00 53 00 65 00 74 00 74 00 69 00 6E 00 67 00 73 00 5C 00 55 00 73 00 65
00 72 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 20 00 53 00 65 00 74 00 74 00

69 00 6E 00 67 00 73 00 5C 00 41 00 70 00 70 00 6C 00 69 00 63 00 61 00 74
00 69 00 6F 00 6E 00 20 00 44 00 61 00 74 00 61 00 5C 00 7A 00 61 00 66 00
6C 00 73 00 68 00 66 00 64 00 2E 00 65 00 78 00 65 00 00 00 00 00

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\ShellNoRoam\Bags\15\Shell\FolderType:

"Documents"

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and
Settings\User\Desktop\44217C15F30538A1FBDF614C9785C9B7.exe:

"44217C15F30538A1FBDF614C9785C9B7"

Values modified: 31

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: EC BB CD 82 4A B7
40 F5 FB D4 E2 C0 44 4B BB 7F B8 65 0A 03 75 A8 F5 D5 6B 82 4C 23 0E 16
97 7E CF 58 96 F3 E2 7D 6F C4 74 F2 11 22 00 E2 69 58 CC 1D 3F A5 B7 4E
BE 28 2A 62 AD 7B 4C 3D 75 36 B6 9A 49 1E 35 49 54 10 D1 25 8C 53 7F A9
87 CB

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 3D 94 32 DC 3C 61
B1 2B F9 CC 4C 04 6F 42 6D 74 D2 CA 77 11 80 F5 BD 6B 6A 83 CB CB CA
3D DF DA 4E D1 E1 D7 FD EF 98 E8 0A AE A5 DD 0A C5 B5 75 E5 BA DC 64
2F 6D BC E6 1F 42 BD 96 68 01 02 63 08 C8 F7 01 1C 01 C1 5B B0 F1 A8 41
E7 44 D7 16

HKLM\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{47D04E80-B172-

40A9-9B4C-6188F2DDB743}: 2C 00 00 00 00 00 00 00 04 00 00 00 00 00 00
00 CE 73 0F 53 C0 A8 DE 02 06 00 00 00 00 00 00 00 04 00 00 00 00 00 00
CE 73 0F 53 C0 A8 DE 02 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00

CE 73 0F 53 C0 A8 DE 02 0F 00 00 00 00 00 00 0B 00 00 00 00 00 00
CE 73 0F 53 6C 6F 63 61 6C 64 6F 6D 61 69 6E 00 01 00 00 00 00 00 00
04 00 00 00 00 00 00 00 CE 73 0F 53 FF FF FF 00 33 00 00 00 00 00 00 04
00 00 00 00 00 00 00 CE 73 0F 53 00 00 07 08 36 00 00 00 00 00 00 04 00
00 00 00 00 00 00 CE 73 0F 53 C0 A8 DE FE 35 00 00 00 00 00 00 00 01 00
00 00 00 00 00 00 CE 73 0F 53 05 00 00 00

HKLM\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{47D04E80-B172-
40A9-9B4C-6188F2DDB743}: 2C 00 00 00 00 00 00 00 04 00 00 00 00 00 00
00 52 77 0F 53 C0 A8 DE 02 06 00 00 00 00 00 00 04 00 00 00 00 00 00
52 77 0F 53 C0 A8 DE 02 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 52
77 0F 53 C0 A8 DE 02 0F 00 00 00 00 00 00 00 0B 00 00 00 00 00 00 52 77
0F 53 6C 6F 63 61 6C 64 6F 6D 61 69 6E 00 01 00 00 00 00 00 00 04 00 00
00 00 00 00 00 52 77 0F 53 FF FF FF 00 33 00 00 00 00 00 00 04 00 00 00
00 00 00 00 52 77 0F 53 00 00 07 08 36 00 00 00 00 00 00 04 00 00 00 00
00 00 00 52 77 0F 53 C0 A8 DE FE 35 00 00 00 00 00 00 00 01 00 00 00 00
00 00 52 77 0F 53 05 00 00 00

HKLM\SYSTEM\ControlSet001\Services\SharedAccess\EPOCH\EPOCH:
0x00000094

HKLM\SYSTEM\ControlSet001\Services\SharedAccess\EPOCH\EPOCH:
0x00000097

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E
80-B172-40A9-9B4C-6188F2DDB743}\LeaseObtainedTime: 0x530F6CC6

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E
80-B172-40A9-9B4C-6188F2DDB743}\LeaseObtainedTime: 0x530F704A

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E
80-B172-40A9-9B4C-6188F2DDB743}\T1: 0x530F704A

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E
80-B172-40A9-9B4C-6188F2DDB743}\T1: 0x530F73CE

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\T2: 0x530F72ED

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\T2: 0x530F7671

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\LeaseTerminatesTime: 0x530F73CE

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\LeaseTerminatesTime: 0x530F7752

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\LeaseObtainedTime: 0x530F6CC6

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\LeaseObtainedTime: 0x530F704A

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\T1: 0x530F704A

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\T1: 0x530F73CE

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\T2: 0x530F72ED

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\T2: 0x530F7671

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\LeaseTerminatesTime: 0x530F73CE

HKLM\SYSTEM\ControlSet001\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\LeaseTerminatesTime: 0x530F7752

HKLM\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{47D04E80-B172-40A9-9B4C-6188F2DDB743}: 2C 00 00 00 00 00 00 00 04 00 00 00 00

00 00 00 CE 73 0F 53 C0 A8 DE 02 06 00 00 00 00 00 00 04 00 00 00 00 00
00 00 CE 73 0F 53 C0 A8 DE 02 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00
00 CE 73 0F 53 C0 A8 DE 02 0F 00 00 00 00 00 00 00 0B 00 00 00 00 00 00
00 CE 73 0F 53 6C 6F 63 61 6C 64 6F 6D 61 69 6E 00 01 00 00 00 00 00 00
00 04 00 00 00 00 00 00 00 CE 73 0F 53 FF FF FF 00 33 00 00 00 00 00 00
04 00 00 00 00 00 00 00 CE 73 0F 53 00 00 07 08 36 00 00 00 00 00 00 04
00 00 00 00 00 00 00 CE 73 0F 53 C0 A8 DE FE 35 00 00 00 00 00 00 01
00 00 00 00 00 00 00 CE 73 0F 53 05 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{47D04E80-
B172-40A9-9B4C-6188F2DDB743}: 2C 00 00 00 00 00 00 00 04 00 00 00 00
00 00 00 52 77 0F 53 C0 A8 DE 02 06 00 00 00 00 00 00 04 00 00 00 00
00 00 52 77 0F 53 C0 A8 DE 02 03 00 00 00 00 00 00 04 00 00 00 00 00
00 52 77 0F 53 C0 A8 DE 02 0F 00 00 00 00 00 00 00 0B 00 00 00 00 00 00
52 77 0F 53 6C 6F 63 61 6C 64 6F 6D 61 69 6E 00 01 00 00 00 00 00 00 04
00 00 00 00 00 00 00 52 77 0F 53 FF FF FF 00 33 00 00 00 00 00 00 04 00
00 00 00 00 00 00 52 77 0F 53 00 00 07 08 36 00 00 00 00 00 00 04 00 00
00 00 00 00 00 52 77 0F 53 C0 A8 DE FE 35 00 00 00 00 00 00 01 00 00 00
00 00 00 00 52 77 0F 53 05 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\EPOCH\EPOCH:
0x00000094

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\EPOCH\EPOCH:
0x00000097

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D
04E80-B172-40A9-9B4C-6188F2DDB743}\LeaseObtainedTime: 0x530F6CC6

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D
04E80-B172-40A9-9B4C-6188F2DDB743}\LeaseObtainedTime: 0x530F704A

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D
04E80-B172-40A9-9B4C-6188F2DDB743}\T1: 0x530F704A

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\T1: 0x530F73CE

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\T2: 0x530F72ED

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\T2: 0x530F7671

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\LeaseTerminatesTime:
0x530F73CE

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\LeaseTerminatesTime: 0x530F7752

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\LeaseObtainedTime: 0x530F6CC6

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\LeaseObtainedTime: 0x530F704A

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\T1: 0x530F704A

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\T1: 0x530F73CE

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\T2: 0x530F72ED

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\T2: 0x530F7671

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\LeaseTerminatesTime: 0x530F73CE

HKLM\SYSTEM\CurrentControlSet\Services\{47D04E80-B172-40A9-9B4C-6188F2DDB743}\Parameters\Tcpip\LeaseTerminatesTime: 0x530F7752

HKU\S-1-5-21-299502267-1004336348-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.\txt\MRUListEx: 01 00 00 00 00 00 00 00 FF FF FF FF

HKU\S-1-5-21-299502267-1004336348-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.\txt\MRUListEx: 02 00 00 00 00 00 00 00 FF FF FF FF

HKU\S-1-5-21-299502267-1004336348-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU: 02 00 00 00 1D 00 00 00 50 9B 56 27 DD 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU: 02 00 00 00 22 00 00 00 C0 E3 75 0B E0 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\pzq.rkr: 02 00 00 00 08 00 00 00 D0 2D 81 77 DC 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\pzq.rkr: 02 00 00 00 09 00 00 00 D0 39 CC 79 DD 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{750487

00-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_HVFPHG: 02 00 00 00
0B 00 00 00 F0 69 ED 21 DD 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{750487
00-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_HVFPHG: 02 00 00 00
0E 00 00 00 B0 5D 7C 09 E0 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{750487
00-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\ABGRCNQ.R
KR: 02 00 00 00 07 00 00 00 70 78 29 49 DC 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{750487
00-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\ABGRCNQ.R
KR: 02 00 00 00 08 00 00 00 C0 E3 75 0B E0 33 CF 01

HKU\S-1-5-21-299502267-1004336348-682003330-
1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Settings\Connections\SavedLegacySettings: 46 00 00 00 38 00 00 00 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 B0 47 17 A0 69
1B CF 01 01 00 00 00 C0 A8 D8 81 00 00 00 00 00 00 00 00 00 00 00 00

HKU\S-1-5-21-299502267-1004336348-682003330-
1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Settings\Connections\SavedLegacySettings: 46 00 00 00 3B 00 00 00 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 B0 47 17 A0 69
1B CF 01 01 00 00 00 C0 A8 D8 81 00 00 00 00 00 00 00 00 00 00 00 00

HKU\S-1-5-21-299502267-1004336348-682003330-
1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 03 00

00 00 05 00 00 00 01 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 FF FF FF
FF

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 05 00
00 00 03 00 00 00 01 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 FF FF FF
FF

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\ShellNoRoam\Bags\15\Shell\CollInfo: 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FD DF DF FD 0F 00 07 00 2C 00
10 00 3A 00 4E 00 00 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 00
00 05 00 00 00 06 00 00 00 B4 00 60 00 78 00 78 00 78 00 78 00 78 00 00 00
00 00 01 00 00 00 02 00 00 00 03 00 00 00 FF FF FF FF 00 00 00 00 00 00 00
00
00 00 00 00

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\ShellNoRoam\Bags\15\Shell\CollInfo: 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FD DF DF FD 0F 00 09 00 34 00 10
00 46 00 5A 00 00 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00
05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 B4 00 60 00 78 00 78 00 78
00 78 00 5A 00 5A 00 78 00 00 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00
FF FF FF FF 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\ShellNoRoam\Bags\15\Shell\ItemPos1024x7
68(1): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 02 00 00
00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 31 2E 54
58 54 00 00 3A 00 03 00 04 00 EF BE 5B 44 85 86 5B 44 95 86 14 00 00 00 74
00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00
2E 00 74 00 78 00 74 00 00 00 1C 00 DC 00 00 00 02 00 00 00 56 00 32 00 0B
00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 31 2E 4D 50 33 00 00 3A 00

03 00 04 00 EF BE 5B 44 99 86 5B 44 99 86 14 00 00 00 74 00 65 00 73 00 74
00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 6D 00 70 00
33 00 00 00 1C 00 02 00 00 00 3A 00 00 00 56 00 32 00 0B 00 00 00 5B 44 95
86 20 00 54 45 53 54 49 54 7E 31 2E 44 4F 43 00 00 3A 00 03 00 04 00 EF BE
5B 44 A8 86 5B 44 A9 86 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69
00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 64 00 6F 00 6

3 00 00 00 1C 00 DC 00 00 00 3A 00 00 00 56 00 32 00 0B 00 00 00 5B 44 95
86 20 00 54 45 53 54 49 54 7E 31 2E 50 44 46 00 00 3A 00 03 00 04 00 EF BE
5B 44 AE 86 5B 44 AF 86 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69
00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 70 00 64 00 66 00 00 00 1C 00
02 00 00 00 72 00 00 00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53
54 49 54 7E 31 2E 58 4C 53 00 00 3A 00 03 00 04 00 EF BE 5B 44 BB 86 5B
44 BB 86 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00
6F 00 73 00 74 00 6F 00 2E 00 78 00 6C 00 73 00 00 00 1C 00 DC 00 00 00 72
00 00 00 58 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 32
2E 44 4F 43 00 00 3C 00 03 00 04 00 EF BE 5B 44 C4 86 5B 44 C4 86 14 00
00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74
00 6F 00 2E 00 64 00 6F 00 63 00 78 00 00 00 1C 00 02 00 00 00 AA 00 00 00
56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 31 2E 50 50
54 00 00 3A 00 03 00 04 00 EF BE

5B 44 FC 86 5B 44 FC 86 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69
00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 70 00 70 00 74 00 00 00 1C 00
DC 00 00 00 AA 00 00 00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53
54 49 54 7E 31 2E 4A 50 47 00 00 3A 00 03 00 04 00 EF BE 5B 44 00 87 5B
44 00 87 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00
6F 00 73 00 74 00 6F 00 2E 00 6A 00 70 00 67 00 00 00 1C 00 02 00 00 00 E2
00 00 00 58 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 31
2E 4A 50 45 00 00 3C 00 03 00 04 00 EF BE 5B 44 02 87 5B 44 02 87 14 00
00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74
00 6F 00 2E 00 6A 00 70 00 65 00 67 00 00 00 1C 00 DC 00 00 00 E2 00 00 00
56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 31 2E 47 49

46 00 00 3A 00 03 00 04 00 EF BE 5B 44 03 87 5B 44 03 87 14 00 00 00 74 00
65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E
00 67 00 69 00 66 00 00 00 1C

00 02 00 00 00 1A 01 00 00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45
53 54 49 54 7E 31 2E 52 54 46 00 00 3A 00 03 00 04 00 EF BE 5B 44 0C 87
5B 44 0C 87 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64
00 6F 00 73 00 74 00 6F 00 2E 00 72 00 74 00 66 00 00 00 1C 00 02 00 00 00
1A 01 00 00 00 00 00 00

HKU\S-1-5-21-299502267-1004336348-682003330-

1003\Software\Microsoft\Windows\ShellNoRoam\Bags\15\Shell\ItemPos1024x7
68(1): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 3A 00 00
00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 31 2E 44
4F 43 00 00 3A 00 03 00 04 00 EF BE 5B 44 A8 86 5B 44 A9 86 14 00 00 00
74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F
00 2E 00 64 00 6F 00 63 00 00 00 1C 00 DC 00 00 00 72 00 00 00 58 00 32 00
0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 32 2E 44 4F 43 00 00 3C
00 03 00 04 00 EF BE 5B 44 C4 86 5B 44 C4 86 14 00 00 00 74 00 65 00 73 00
74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 64 00 6F
00 63 00 78 00 00 00 1C 00 DC 00 00 00 E2 00 00 00 56 00 32 00 0B 00 00 00
5B 44 95 86 20 00 54 45 53 54 49 54 7E 31 2E 47 49 46 00 00 3A 00 03 00 04
00 EF BE 5B 44 03 87 5B 44 03 87 14 00 00 00 74 00 65 00 73 00 74 00 69 00
74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 67 00 6

9 00 66 00 00 00 1C 00 02 00 00 00 E2 00 00 00 58 00 32 00 0B 00 00 00 5B
44 95 86 20 00 54 45 53 54 49 54 7E 31 2E 4A 50 45 00 00 3C 00 03 00 04 00
EF BE 5B 44 02 87 5B 44 02 87 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74
00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 6A 00 70 00 65 00 67 00
00 00 1C 00 DC 00 00 00 AA 00 00 00 56 00 32 00 0B 00 00 00 5B 44 95 86 20
00 54 45 53 54 49 54 7E 31 2E 4A 50 47 00 00 3A 00 03 00 04 00 EF BE 5B 44
00 87 5B 44 00 87 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65
00 64 00 6F 00 73 00 74 00 6F 00 2E 00 6A 00 70 00 67 00 00 00 1C 00 DC 00
00 00 02 00 00 00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49

54 7E 31 2E 4D 50 33 00 00 3A 00 03 00 04 00 EF BE 5B 44 99 86 5B 44 99
86 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00
73 00 74 00 6F 00 2E 00 6D 00 70 00 33 00 00 00 1C 00 DC 00 00 00 3A 00 00
00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 31 2E 50
44 46 00 00 3A 00 03 00 04 00

EF BE 5B 44 AE 86 5B 44 AF 86 14 00 00 00 74 00 65 00 73 00 74 00 69 00
74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00 2E 00 70 00 64 00 66 00 00
00 1C 00 02 00 00 00 AA 00 00 00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00
54 45 53 54 49 54 7E 31 2E 50 50 54 00 00 3A 00 03 00 04 00 EF BE 5B 44
FC 86 5B 44 FC 86 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65
00 64 00 6F 00 73 00 74 00 6F 00 2E 00 70 00 70 00 74 00 00 00 1C 00 02 00
00 00 1A 01 00 00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49
54 7E 31 2E 52 54 46 00 00 3A 00 03 00 04 00 EF BE 5B 44 0C 87 5B 44 0C
87 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00
73 00 74 00 6F 00 2E 00 72 00 74 00 66 00 00 00 1C 00 02 00 00 00 02 00 00
00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45 53 54 49 54 7E 31 2E 54
58 54 00 00 3A 00 03 00 04 00 EF BE 5B 44 85 86 5B 44 95 86 14 00 00 00 74
00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64 00 6F 00 73 00 74 00 6F 00
2E 00 74 00 78 00 74 00 00 00 1C

00 02 00 00 00 72 00 00 00 56 00 32 00 0B 00 00 00 5B 44 95 86 20 00 54 45
53 54 49 54 7E 31 2E 58 4C 53 00 00 3A 00 03 00 04 00 EF BE 5B 44 BB 86
5B 44 BB 86 14 00 00 00 74 00 65 00 73 00 74 00 69 00 74 00 69 00 65 00 64
00 6F 00 73 00 74 00 6F 00 2E 00 78 00 6C 00 73 00 00 00 1C 00 02 00 00 00
72 00 00 00 00 00 00 00

HKU\S-1-5-21-299502267-1004336348-682003330-
1003\SessionInformation\ProgramCount: 0x00000002

HKU\S-1-5-21-299502267-1004336348-682003330-
1003\SessionInformation\ProgramCount: 0x00000004

Files added: 7

C:\Documents and Settings\User\Application Data\Process Hacker
2\usernotesdb.xml

C:\Documents and Settings\User\Local Settings\Application Data\lodcjajf

C:\Documents and Settings\User\Local Settings\Application Data\zaflshfd.exe

C:\Program Files\Capture\logs\deleted_files\C\Documents and Set-
tings\User\Desktop\44217C15F30538A1FBDF614C9785C9B7.exe

C:\Program Files\Capture\cryptolocker.txt

C:\WINDOWS\Prefetch\44217C15F30538A1FBDF614C9785C-11763CAF.pf

C:\WINDOWS\Prefetch\ZAFLSHFD.EXE-11B8E079.pf

Files deleted: 1

C:\Documents and Set-
tings\User\Desktop\44217C15F30538A1FBDF614C9785C9B7.exe

Files [attributes?] modified: 17

C:\Documents and Settings\User\Cookies\index.dat

C:\Documents and Settings\User\Local Settings\History\History.IE5\index.dat

C:\Documents and Settings\User\Local Settings\Temporary Internet Files\Content.IE5\index.dat

C:\Documents and Settings\User\NTUSER.DAT.LOG

C:\Documents and Settings\User\Recent\Testaustiedostot.Ink

C:\Documents and Settings\User\Recent\testitiedosto.txt.Ink

C:\Program Files\Capture\logs\192.168.222.129.pcap

C:\WINDOWS\Prefetch\CAPTUREBAT.EXE-056A1A48.pf

C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

C:\WINDOWS\Prefetch\notepad.exe-336351A9.pf

C:\WINDOWS\Prefetch\PROCESSHACKER.EXE-1467EA23.pf

C:\WINDOWS\system32\CatRoot2\edb.chk

C:\WINDOWS\system32\CatRoot2\edb.log

C:\WINDOWS\system32\CatRoot2\tmp.edb

C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb

C:\WINDOWS\system32\config\software.LOG

C:\WINDOWS\system32\config\system.LOG

Folders added: 2

C:\Documents and Settings\User\Application Data\Process Hacker 2

C:\Program Files\Capture\logs\deleted_files\C\Documents and Settings\User\Desktop

Total changes: 88
