HAAGA-HELIA
ammattikorkeakoulu

# Zeus-pankkihaittaohjelman rakenne ja toiminta

Jussi Leskinen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2014

HAAGA-HELIA
ammattikorkeakoulu

Tietojenkäsittelyn koulutusohjelma

**Tiivistelmä**

3.5.2014

| **Tekijä tai tekijät**<br>Jussi Leskinen | **Ryhmä tai aloitusvuosi**<br>TIKO 2010 |
|---|---|
| **Opinnäytetyön nimi**<br>Zeus-pankkihaittaohjelman rakenne ja toiminta | **Sivu- ja liitesivumäärä**<br>25 + 6 |
| **Ohjaaja tai ohjaajat**<br>Ahti Kare | |


Tässä tutkimuksessa perehdytään Zeus-pankkihaittaohjelman rakenteeseen ja toimintaan. Tutkimuksen tarkoituksena on syventää tietoturva-alalla työskentelevien tai alaan muuten perehtyneiden tietämystä Zeuksesta ja pankkihaittaohjelmien toiminnasta yleensä.

Työ koostuu kolmesta osasta, joista ensimmäisessä käydään läpi pankkihaittaohjelmien toimintaa yleisellä tasolla sekä Zeuksen historiaa ja nykytilaa. Toisessa osassa käydään läpi varsinaisen haittaohjelman luontivaihe ja sen tarvitseman infrastruktuurin osat. Kolmannessa osassa käsitellään Zeuksen version 2.1.0.1 toiminnallisuutta.

Zeusta tutkittiin asentamalla se virtuaaliympäristöön. Työn tuotoksena syntyi teoriamateriaalia, jonka avulla Zeuksen ja pankkihaittaohjelmien toimintaa on helpompi esittää asiasta kiinnostuneille. Tutkimiseen käytettyä virtuaaliympäristöä pystytään käyttämään myös muiden vastaavien haittaohjelmien tutkimiseen sekä sen avulla teoriamateriaalin oppeja pystytään syventämään ja havainnollistamaan paremmin.

Materiaalista käy ilmi Zeus-tartunnan havaitsemisen vaikeus. Edes suojatusta yhteydestä kertova lukon kuva nettiselaimen osoitepalkissa ei ole tae pankkitunnusten turvallisesta käytöstä.



**Asiasanat**
Haittaohjelmat, verkkohyökkäykset, verkkourkinta, verkkopankit

HAAGA-HELIA
University of Applied Sciences
Degree Programme in Information Technology

**Abstract**

3 May 2014

| **Author(s)**<br>Jussi Leskinen | **Group or year of entry**<br>2010 |
|---|---|
| **The title of thesis**<br>The anatomy and functions of Zeus banking malware | **Number of report pages and attachment pages**<br>25 + 6 |
| **Advisor(s)**<br>Ahti Kare | |


This Bachelor's thesis looks at the functions and anatomy of the world's most notorious banking Trojan Zeus.

The primary objective of this study was to deepen the knowledge of Zeus of those who work in the field of information security or who have basic understanding about banking malware generally.

The thesis consists of a theory section and an empirical section. The theory section is divided in two parts of which the first deals with banking malware generally and the history and present situation of Zeus. The second part describes the infrastructure and primary parts of Zeus.

The empirical section of this thesis deals with the functionality of Zeus, which was demonstrated by installing version 2.1.0.1 in virtual environment. The same environment can be used for testing other Zeus variants and for educational purposes. With slight modification the virtual environment serves for testing purposes of other malware.

The material shows the difficulty of detecting Zeus infection. Not even the lock symbol in the Internet browser address bar is a guarantee of secure use of online banking credentials.



**Key words**
Malware, online banking, information security

# Sisällys

# 1 Johdanto

Tietoturvallisuus on aina ollut ajankohtainen asia tietotekniikan maailmassa. Toisen hallussa olevaa tietoa on pyritty anastamaan, hävittämään ja vääristelemään niin kauan, kuin jollakin on ollut toiselle arvokasta tietoa. Tämä asia ei ole muuttunut mihinkään ihmiskunnan tärkeiden toimintojen siirtyessä yhä enenemissä määrin verkkoon. Internetin myötä tiedon käytettävyys on saanut aivan toisenlaisen käsityksen. Ihmiset siirtävät henkilökohtaisia tietojaan pilveen, vaikka eivät näin välttämättä ymmärrä tekevänsä. Googlen, Facebookin ja Microsoftin tarjoamien palveluiden käyttö on lisääntynyt räjähdyksenomaisesti viimeisenä vuosikymmenenä.

Tietojen käytettävyys on ollut varmasti yksi eteenpäin ajava voima, kun pankkipalveluita alettiin siirtämään verkkoon yhdeksänkymmentäluvun alkupuolella. Samaan aikaan tietokonevirusten, troijalaisten ja matojen kirjoittajat kehittivät tuotteitaan niin, että niillä voitiin hyökätä verkkopankkien asiakkaita vastaan. Tämä hyökkäysvektori on toiminut viimeiset vuosikymmenet niin hyvin, että verkkopankit ovat saaneet olla hyökkäyksiltä rauhassa. Pankkien ja viranomaisten työtä vaikeuttaa se, että verkkopankkien käyttäjiltä anastetuilla tunnuksilla tehtyä tunkeutumista on hyvin vaikeaa estää. Pankkitunnuksia pyritään anastamaan kalastelemalla (Eng. phishing) ja tietoa anastavien haittaohjelmien avulla.

Jotta haittaohjelmia ja yleensä tietoverkkorikollisuutta vastaan pystytään toimimaan tehokkaasti on tietoturva-alan eri toimijoiden välisen tiedonvaihdon oltava tehokasta. Tietoturvayhtiöt tekevät jatkuvasti töitä analysoidakseen uusia verkossa liikkuvia haittaohjelmia ja muita uhkia. Tämän tiedon jakaminen kaikkien toimijoiden kesken on parantanut valmiuksia torjua nykyisiä ja varautua tuleviin uhkiin. Lisäksi on myös erittäin tärkeää ottaa oppia jo aiemmin tutkituista ja analysoiduista haittaohjelmista. Tämä on ollut helpoin tapa tutustua haittaohjelmiin ja niiden toiminnallisuuksiin. Tietoturvayhtiöiden tekemät analyysit ovat usein erittäin teknisiä, jolloin vähemmän teknisesti orientoituneen on hyvin vaikea päästä asiaan käsiksi. Aloitteleville tietoturvan kanssa tekemisissä oleville ammattilaisille suunnatusta materiaalista on pula. Muun muassa poliisilla ja pankeilla on töissä henkilöitä, jotka työnsä puolesta joutuvat tekemisiin haittaohjelmien

avulla tehtyjen rikosten kanssa. Monesti näiden henkilöiden tekniset valmiudet eivät riitä ymmärtämään ammattilaisten tekemiä haittaohjelma-analyysejä.

Tässä opinnäytetyössä käydään läpi yhden maailman tunnetuimman haittaohjelman, Zeuksen, rakennetta ja toiminnallisuutta. Työn lähdemateriaalina on käytetty tietoturvayritysten analyyseja ja tarkoitusta varten asennetussa virtuaaliympäristössä haittaohjelmalla suoritettuja testejä.

## 1.1 Tavoitteet ja rajaus

Työn tarkoituksena on tuottaa tietoturvakoulutusta varten käytännön materiaalia pankkihaittaohjelmista. Internetissä esiintyvistä pankkihaittaohjelmista Zeus valikoitui kohteeksi sen yleisyyden vuoksi ja koska sen tutkimisesta on Suomessa paljon kokemusta. Opinnäytetyön materiaali pohjautuu tietoturvayhtiöiden tekemiin analyyseihin, käytännön testeihin ja kirjoittajan omiin kokemuksiin Zeuksen avulla toteutettujen rikosten tutkimisesta. Tuotetun materiaalin kohderyhmänä ovat tietoturva- tai muulla alalla työskentelevät henkilöt, joiden arkeen pankkihaittaohjelmat tavalla tai toisella kuuluvat. Näihin ammattilaisiin lukeutuvat muun muassa verkkorikoksia tutkivat poliisit ja pankkien tietoturvan kanssa tekemisissä olevat henkilöt. Opinnäytetyön pohjalta valmistuu tulevaisuudessa laajempi opintokokonaisuus, jonka yhdeksi tärkeäksi osaksi työtä varten rakennettu virtuaaliympäristö jää.

Työssä ei analysoida Zeuksen lähdekoodia, eikä suoriteta haittaohjelman takaisinmallinnusta. Työhön tutustuvan on kuitenkin tunnettava tietotekniikkaa ainakin käsitetasolla. Lisäksi verkkoliikenteen ja Windows-käyttöjärjestelmän tunteminen helpottavat Zeuksen toiminnan ymmärtämistä.

## 1.2 Käsiteanalyysi

**Haittaohjelma,** Eng. malware, on yleinen termi haitalliselle tietokoneohjelmalle. Haittaohjelmia ovat esimerkiksi virukset, troijalaiset ja madot.

**Pankkihaittaohjelma**, Eng. banking malware, on haittaohjelma, joka on suunniteltu erityisesti verkkopankkitunnusten ja muiden verkkomaksuvälineiden (muun muassa luottokorttien) tunnisteiden anastamiseen.

**Botti**, Eng. bot, on yleisempi nimitys haittaohjelmalle, jonka yksi tehtävä on ottaa uhrin tietokone haltuun, niin että hyökkääjä voi käyttää sitä omiin tarkoituksiinsa. Yleensä botteja käytetään rikollisiin tarkoituksiin, kuten tietojen varastamiseen, roskapostittamiseen tai muiden haittaohjelmien levittämiseen.

**Bottiverkko**, Eng. botnet, on useiden bottien hallitsemien koneiden muodostama verkko. Tällaisen verkon avulla verkkorikollinen voi suorittaa esimerkiksi massiivisia palvelunestohyökkäyksiä tai roskapostikampanjoita.

**Troijalainen**, Eng. trojan, on haittaohjelma, joka uhrin koneelle päästyään suorittaa järjestelmälle haitallisia ohjelmia. Troijalainen nimi juontaa juurensa antiikin tarusta, jossa Troijan valtakunnan viholliselleen lahjana antamaa puuhevosta käytettiin salakuljettamaan sotilaita vihollisen linnoitukseen. Samalla tavalla haittaohjelma tuotetaan uhrin koneeseen esimerkiksi luotettavan oloisen ohjelman sisällä.

**Kalastelu,** joskus myös khalastelu, Eng. phishing, on yleinen termi verkkorikosten toimintamallille, jolla pyritään saamaan uhrilta arkaluontoista tietoa haltuun. Phishing tapahtuu pääosin sähköpostin välityksellä, mutta sitä tehdään myös Internetissä erilaisilla lomakkeilla ja myös puhelimitse.

**XMPP** on yleinen pikaviestimissä käytetty protokolla. Sitä käytetään muun muassa Facebook Chat ja Google Talk -palveluissa. XMPP on lyhenne sanoista Extensive Messaging and Presence Protocol.

# 2 Pankkihaittaohjelmat

Verkossa on tarjottu pankkipalveluita jo vuodesta 1994 saakka. Alusta lähtien rikolliset ovat kehittäneet haittaohjelmia kiertääkseen niiden turvajärjestelmiä saadakseen taloudellista hyötyä. Vuonna 2003 verkossa oli havaittu jo noin 20 erilaista haittaohjelmaa, jotka olivat suunnattu nimenomaan verkkopankkipalveluita vastaan. (Doherty, Krysiuk & Wueest 2013.)

Pankkihaittaohjelmien avulla tehdyt petokset ovat tällä hetkellä taloudellisilla mittareilla mitattuina ylivoimaisesti eniten vahinkoa aiheuttavia verkkorikoksia maailmalla. Vuoden 2012 alussa julkaistujen lukujen mukaan niiden aiheuttamat vahingot edellisen viiden vuoden ajalta olivat noin miljardi dollaria. Tuolloin Zeus vastasi noin 80 % maailman pankkihaittaohjelmien avulla tehdyistä rikoksista. (RSA 2012.)

Suomen osalta lukuja ei ole julkaistu vaikka Zeusta on käytetty verkkopankkipetosten tekemiseen täälläkin useita vuosia. Tämän opinnäytetyön tekijä on työskennellyt Keskusrikospoliisissa verkkorikoksia tutkivassa yksikössä tutkijana vuodesta 2011 saakka. Yksikössä on tutkittu muun muassa vuoden 2011 marraskuussa alkanutta suurta rikoskokonaisuutta, jossa Zeuksen avulla on useiden eri pankkien asiakkaiden tileiltä siirretty onnistuneesti rahaa. Taloudellisiin tappioihin ei sisälly pelkästään anastetut varat. Kun uhreilta varastettujen varojen lisäksi kustannuksiin lasketaan mukaan muut välilliset kulut, kuten viranomaisten ja kohteena olevien pankkien asiaan liittyvät selvittelykustannukset, ovat Zeuksen aiheuttamat taloudelliset menetykset varsin suuria. Valitettavasti näitä lukuja harvoin nähdään missään yhteenlaskettuna ja artikkeleihin sekä oikeussaliin päätyy vain anastettujen varojen yhteissumma.

## 2.1 Pankkihaittaohjelmien ominaisuudet

Verkossa käytettäviä maksuvälineitä ja niiden käyttäjiä vastaan suunnatut nykyaikaiset haittaohjelmat kykenevät manipuloimaan uhrin ja kohdepalvelun välistä liikennettä ja sieppaamaan sieltä esimerkiksi luottokorttitietoja tai verkkopankkitunnuksia. Tämän lisäksi uhrin konetta voidaan käyttää välityspalvelimena peittämään rikollisten omaa

verkkoliikennettä tai uhrin omaa verkkoliikennettä voidaan ohjata uudestaan rikollisten haluamille sivustoille. Haittaohjelmien avulla rikolliset pystyvät myös käyttämään uhrin konetta etätyöpöytäyhteyden avulla. Haittaohjelmissa on myös ominaisuuksia, joiden avulla uhrien tietokoneen käytöstä ja verkkoyhteyksien avaamisesta viestitään haittaohjelmaa hallitseville rikoksille muun muassa pikaviestiohjelmien avulla. (Donohue 2013.)

Nykyaikaiset pankkihaittaohjelmat käyttävät uhrin verkkoliikenteen sieppaamiseen ja manipuloimiseen niin kutsuttua man-in-the-browser-tekniikkaa. Tämä tarkoittaa sitä, että haittaohjelma sieppaa verkkoliikenteen nettiselaimen ja käyttöjärjestelmän rajapinnasta. Verkkoliikenteestä haittaohjelma pystyy anastamaan salasanoja ja muokkaamaan uhrin internet-selaimen näkymää rikollisen toivomalla tavalla. (Trusteer 2013.)

## 2.2 Zeuksen historia ja nykytila

Zeus tuli myyntiin ja kenen tahansa ostettavaksi vuonna 2007 (Falliere & Chien 2009). Alkuaikoina Zeuksen täysi versio maksoi 10 000 dollaria internetin pimeillä markkinoilla. Kaksi vuotta myöhemmin se sai vastaansa varteenotettavan kilpailijan: troijalaisen nimeltä Spyeye. Spyeyen kirjoittaja yritti horjuttaa Zeuksen markkina-asemaa selkeästi halvemmalla hinnalla. Kahden suuren haittaohjelman kamppailu ei kestänyt montaa vuotta. Vuonna 2011 Zeuksen lähdekoodi tuli vapaasti ladattavaksi verkkoon, minkä johdosta Zeuksen käyttöaste lisääntyi huomattavasti. Lähdekoodin vapautuminen oli yksi syy, miksi Zeuksesta tuli maailman suosituin pankkihaittaohjelma. Zeuksen kehittäjän sanottiin itse laittaneen koodin saataville ja vetäytyneen julkisuudesta, mutta tietoturvatutkijat väittävät, että tämä olisi jatkanut Zeuksen kehittämistä taustalla. (RSA 2013.)

Zeuksen lähdekoodin tultua yleiseen jakoon on haittaohjelma kehittynyt koko ajan toimivampaan suuntaan ja vaikeammin havaittavaksi. Kaksi ensimmäistä, ja tällä hetkellä tunnetuinta, lähdekoodin julkaisun jälkeen valmistettua Zeuksen versiota ovat nimeltään ICE IX ja Citadel. Versioissa on muun muassa vaihdettu käytettyä salausalgoritmia, jolloin sen tutkimista takaisinmallinnusta hyväksikäyttäen on vaikeutettu. (RSA 2013, 3.)

Myöhemmissä Zeuksen versioissa verkkoliikenteen jäljittämistä on vaikeutettu entisestään. Zeuksesta on nykyään olemassa versio, joka käyttää tiedon liikuttamiseen vertaisverkkoa, mikä tekee haittaohjelman verkkoliikenteen seuraamisen lähes mahdottomaksi (Gallagher 2012). Toinen Zeuksen moderni versio siirtää botin ja sen komentopalvelimen välisen liikenteen kokonaan Tor-verkkoon (Tarakanov 2013). Tor-verkossa verkkoliikenne kulkee salattuna useiden ympäri maailmaa ylläpidettyjen palvelimien kautta (Torproject).

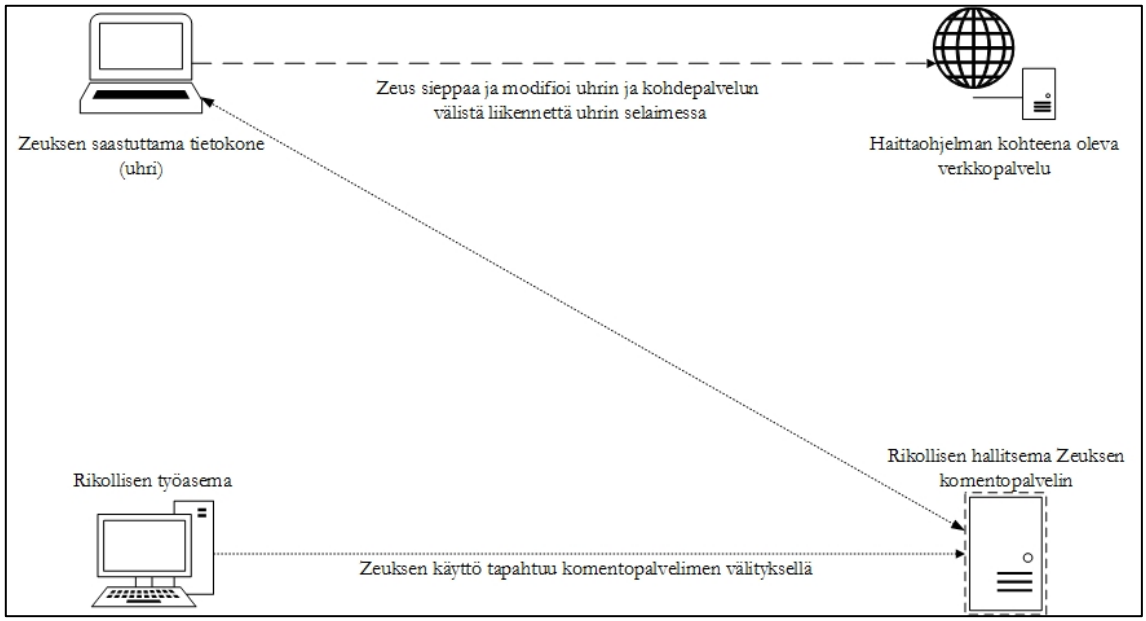
Tietoturvayhtiö Symantec (2013) listasi tutkimuksessaan The State of Financial Trojans seitsemän levinneintä troijalaista, jotka olivat saastuttaneet yhteensä useita miljoonia koneita ympäri maailman (Taulukko 1). Taulukosta voi nähdä, että vielä seitsemän vuotta rikollisille markkinoille tulon jälkeen Zeus on edelleen selvästi levinnein troijalainen, mitä verkosta löytyy.

Taulukko 1. Seitsemän levinneimmän troijalaisen tartuttamat koneet vuonna 2013 (Symantec 2013.)

| Troijalainen | Saastutetut tietokoneet |
|---|---|
| Zeus (Zbot+Gameover) | > 2 000 000 kpl |
| Cridex | > 125 000 kpl |
| Shylock | > 33 000 kpl |
| Spyeye | > 26 000 kpl |
| Bebloh | > 21 000 kpl |
| Mebroot | > 9 000 kpl |
| Tilon (Tylon) | > 2 000 kpl |

# 3 Zeuksen rakenne

Haittaohjelmana Zeus edustaa troijalaisten ryhmää. Varsinainen troijalainen on ajettava ohjelmatiedosto, joka uhrin koneella toimiessaan aiheuttaa konkreettiset vahingot ja sieppaa hyökkääjän haluamia tietoja. Tämä ei kuitenkaan riitä rikoksen tekemiseen vaan rikollinen tarvitsee troijalaisen ympärille oman infrastruktuurin (Kuvio 1).



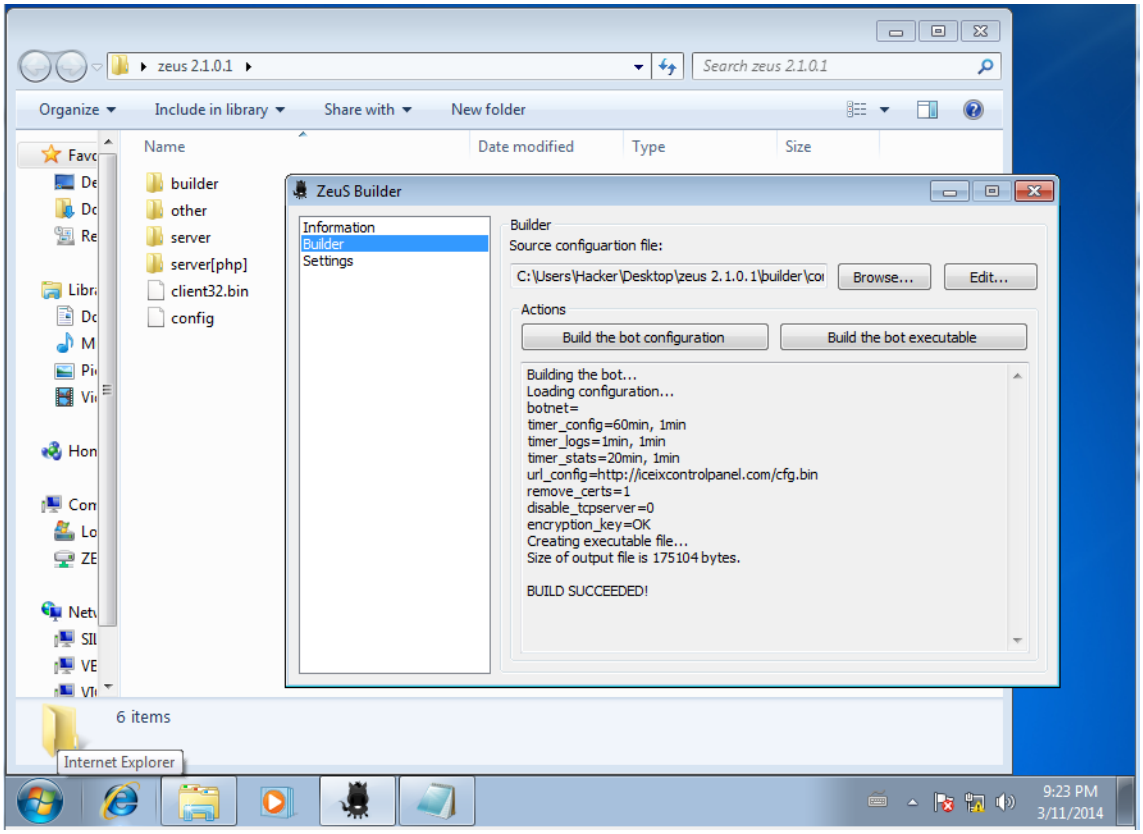

Kuvio 1. Zeuksen infrastruktuuri

Saadakseen varsinaisen haittaohjelman ja sen tarvitseman infrastruktuurin rikollisen on saatava Zeuksen asennuspaketti haltuunsa. Asennuspaketti hankitaan yleensä ostamalla se joltakin internetissä sijaitsevalta rikollisten käyttämältä foorumilta. Zeusta ja siihen liittyviä osia ostaessaan rikollinen on jo suunnitellut, mihinkä hän sitä aikoo käyttää. Mahdollisuuksia on monia: hän voi suunnitella sieppaavansa luottokorttitietoja tai verkkopankkien asiakkaiden tunnuksia. Näiden lisäksi hänen määriteltävä minkä maiden ja yritysten asiakkaiden tietoja haittaohjelma kerää. Asennuspaketti antaa rikolliselle tarvittavat työkalut haittaohjelman uhrin koneelle asentavan ohjelman luomiseen. Lisäksi paketti sisältää haittaohjelman hallintaan käytettävän komentopalvelimen asentamiseen tarvittavat ohjelmatiedostot. Asennuspaketin ja haittaohjelman kohdentamiseen tarvittavien tiedostojen, eli injektioiden lisäksi rikollisen tarvitsee hankkia käyttöönsä palvelin, jonne komentopalvelimen tarvitsemat tiedostot asennetaan. Rikollisten on mahdollista käyttää murrettuja palvelimia tai vuokrata oma palvelin tätä käyttöä varten.

Asennuspaketin oston ja palvelimen hankkimisen jälkeen rikollisen on luotava Zeuksen lataamiseen ja asentamiseen tarvittava ohjelma sekä asentaa palvelin valmiiksi ottamaan vastaan botilta tulevia yhteydenottoja. (Falliere & Chien 2009.)

### 3.1 Botin luonti ja komentopalvelimen asennus

Asennustyökalu on muodoltaan Windows-käyttöjärjestelmässä ajettava exe–ohjelmatiedosto (Kuvio 2). Asennustyökalun avulla Zeuksen ostanut henkilö pystyy luomaan varsinaisen haittaohjelman ja sen tarvitseman konfiguraatiotiedoston. Muokkaamaton konfiguraatiotiedosto on asennustyökalun mukana tavallisena tekstitiedostona. Erikseen hankittava verkkoliikenteen sieppaamiseen tarkoitettu webinjektio sijoitetaan myös samaan hakemistopolkuun konfiguraation kanssa, jotta ohjelma pystyy luomaan toimivan botin. Ohjelma luo haittaohjelman levittäjän valitsemilla nimillä kaksi tiedostoa, joista toinen on haittaohjelman suoritettava asennustiedosto ja toinen salattu konfiguraatiotiedosto. Konfiguraatiotiedosto sijoitetaan Zeuksen tarvitsemalle komentopalvelimelle odottamaan haittaohjelman yhteydenottoa. (Wyke 2011, 3–4; Zeus User Guide 2012.) Komentopalvelin tarvitsee toimiakseen web- ja MySql-tietokantapalvelimen sekä PHP-tulkin asennuksen. Asennuspaketissa on mukana tarvittavat tiedostot komentopalvelimen asentamiseksi joko Windows- tai Linux-palvelinympäristöön. (Zeus User Guide 2012, 5.)




Kuvio 2. Zeuksen asennustyökalu (Kuvankaappaus testiympäristöstä.)

## 3.2 Konfiguraatiotiedosto

Zeuksen asennuspaketin mukana on tekstitiedosto, joka sisältää konfiguraatiotiedoston pohjan. Tähän tiedostoon syötetään niiden nettisivujen osoitteet, joita halutaan valvoa, eli joiden käyttäjätunnukset ja salasanat botti kerää talteen ja lähettää komentopalvelimelle (Kuvio 3). Tärkeimmät syötettävät osoitteet konfiguraatiossa ovat url_config, url_loader ja url_server kohdissa. Näille riveille syötetään konfiguraation ja botin päivitystiedostojen sekä komentopalvelimen tarkat osoitteet tiedostonimineen. (Wyke 2011, 4; Zeus User Guide 2012.)

```
;Build time:   10:13:05 01.07.2011 GMT
;Version:      2.1.0.1

entry "StaticConfig"
  ;botnet "btn1"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "http://iceixcontrolpanel.com/cfg.bin"
  remove_certs 1
  disable_tcpserver 0
  encryption_key "jNBF43098092jojf209u402jf2polaa"
end

entry "DynamicConfig"
  url_loader "http://iceixcontrolpanel.com/file.exe"
  url_server "http://iceixcontrolpanel.com/tyt.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs"
    ;"http://advdomain/cfg1.bin"
  end
  entry "WebFilters"
  end
  entry "WebDataFilters"
  end
  entry "WebFakes"
  end
end
```

Kuvio 3. Esimerkki konfiguraatiotiedostosta (kuvankaappaus testiympäristöstä.)

### 3.3 Webinjektio

Tärkein osa Zeuksen toiminnallisuutta on webinjektio (Eng. webinject). Webinjektio rakennetaan muusta botista erillään ja sen kehittäminen on verkkorikollisten keskuudessa oma toimintonsa. Injektioita koodaavat henkilöt myyvät tuotteitaan Internetin alamaailmassa yleensä tilauksesta. Tehdäkseen toimivan injektion on koodaajan tutustuttava kohteena olevan verkkopankin toimintaan. Toimiva injektio hämää uhria saaden tämän uskomaan selaimen näkymän olevan autenttinen verkkopankin sivusto, eikä tämä osaa epäillä osan tietokentistä olevan tekaistuja. Injektion avulla haittaohjelmalla voidaan kiertää verkkopankkien tietoturvan kohottamiseksi tehdyt JavaScript-ohjelmat ja muokata uhrin selaimen näkymää. Käytännössä haittaohjelmalla voidaan luoda kokonaan uusi html-sivu, korvata alkuperäiset lomakkeen kohdat uusilla, tai pelkästään lisätä aitojen tietokenttien lisäksi sivulle uusia tiedonsyöttöruutuja. Esimerkiksi verkkopankin kirjautumissivulle voidaan käyttäjätunnusta ja salasanaa kysyvien tietoruutujen alle sijoittaa kohdat, jotka kysyvät luottokortin numeroa ja turvakoodia. Oleellista injektiossa on se, että uhri ei missään vaiheessa siirry pois pankin sivustolta, vaan koodi injektoidaan samaan istuntoon suoraan uhrin selaimeen. Näin suojatusta verkkoyhteydestä kertovat lukon tms. kuvat eivät paljasta haittaohjelman sieppaavan uhrin lomakkeelle tekemiä syötteitä. (Smith 2013.)

Verkkorikollisten alamaailmassa webinjektioista on tullut jo eräänlainen standardi. Zeuksen eri versioiden lisäksi samanlaista injektiota käyttävät muun muassa Zeuksen vanha kilpakumppani Spyeye ja Suomessa harvinaisempi Carberp. (Milletary 2012, 2.)

### 3.4 Salasanojen varastaminen

Zeuksen perusolemukseen kuuluu salasanojen varastaminen. Asennuksen jälkeen botti kerää muun muassa internetselainten ja eri FTP ja POP3 – palvelimien tallennetut salasanat. Käsikirjan mukaan botti kaappaa ainakin seuraavien tunnettujen ohjelmien kirjautumistiedot automaattisesti: FlashFXP, CuteFtp, Total Commander, WsFTP, FileZilla, FAR Manager, WinSCP, FTP Commander, Core FTP ja SmartFTP. (Zeus User Guide 2012, 2.)

Saadakseen myös jo sisäänkirjattujen palveluiden salasanat botti poistaa Internet Explorerin Cookie-tiedostot, jotta uhri olisi pakotettu kirjautumaan kaikkiin verkkopalveluihin uudestaan. Botti pystyy myös importoimaan sertifikaatit Windowsin sertifikaattivarastosta. Zeukseen on myös rakennettu keylogger-toiminnallisuus, jolla uhrin näppäimistön painallukset pystytään tallentamaan. Jos uhri käyttää virtuaalista näppäimistöä keyloggerin pelossa, Zeus kykenee tarvittaessa tallentamaan muutaman neliösentin kokoisen näytönkaappauksen hiiren osoittimen ympäriltä uhrin painaessa hiiren vasenta näppäintä. Botin konfiguraatiotiedostoa luodessaan haittaohjelman levittäjä valitsee botin seuraamat nettiosoitteet. Kun uhri vierailee näillä sivuilla, kerää botti sivustoille syötettävä käyttäjätunnukset ja salasanat. Haittaohjelman levittäjä pystyy merkitsemään muut edellä mainitut toiminnot verkkosivukohtaisesti. Esimerkiksi, jos hyökkääjä tietää jonkin sivuston käyttävän virtuaalinäppäimistöä käyttäjätunnusten ja salasanojen syöttöön, pystyy hän asettamaan botin suorittamaan kuvankaappauksen vain tällä kyseisellä sivustolla. Näin hyökkääjä pystyy kontrolloimaan botin ja komentopalvelimen välisen liikenteen tietomäärää karsimalla turhaa tietoa pois. (Selvaraj 2010.)

# 4 Zeuksen toiminta

Zeuksen toiminnan tutkimista varten asennettiin oma virtuaaliympäristö. Tässä ympäristössä Zeusta pystyttiin käyttämään ilman pelkoa, että se aiheuttaisi vahinkoa aidossa verkkoympäristössä. Virtuaaliympäristön etuna on myös eri työtilojen palauttaminen snapshot–toiminnon avulla. Näin esimerkiksi saastutettu työasema voitiin palauttaa nopeasti aiempaan tilaan, missä se oli ennen saastutusta. Menetelmä on yleinen erityisesti antivirusalalla.

Vaikka rikollinen pystyy asentamaan Zeuksen komentopalvelimen Linux-palvelimelle, niin varsinainen haittaohjelma toimii vain Microsoftin Windows-ympäristössä. Tutkittavana oleva Zeuksen versio 2.1.0.1 tukee Windowsin käyttöjärjestelmistä Vistaa, XP:tä ja 7:ää. Haittaohjelma voidaan asentaa näiden lisäksi myös Windowsin palvelimiin 2003/2003R ja 2008/2008R. Haittaohjelma toimii myös 64-bittisissä käyttöjärjestelmissä, mutta vain sen 32-bittisissä prosesseissa (Zeus User Guide 2012).

Bottiin on rakennettu turvamekanismeja, joiden tehtävänä on haitata sen tutkimista ja poistamista. Asennettua bottia ei esimerkiksi voi siirtää toimimaan muuhun ympäristöön, kuin mihin se on asennettu. Botti luo aina asennettuaan uniikit tiedostonimet ja rekisteriavaimet. Botin päivittäminen ei myöskään vaadi tietokoneen uudelleen käynnistämistä.

## 4.1 Menetelmä ja tavoitteet

Tässä työssä tutkitun Zeuksen version toimintaan tutustuttiin saastuttamalla erillisiä koneita, sekä virtuaalisia että fyysisiä, ja seuraamalla hyökkääjän näkökulmasta tämän infrastruktuurin toimintaa. Asennustyön pohjana käytettiin Zeuksen omaa käyttöohjetta, joka ladattiin internetistä. Käyttöohjeen alkuperää on tällä hetkellä mahdoton jäljittää, koska sen kirjoittajaa ei tunneta. Asentamalla Zeus ja sen tarvitsemat palvelimet voitiin samalla varmistua käyttöohjeen oikeellisuudesta.

Ensisijaisena tavoitteena oli saada ymmärrys Zeuksen ja sen tarvitseman infrastruktuurin toiminnasta. Virtuaaliympäristö rakennettiin sellaiseksi, että se on hyödynnettävissä

myös opetuskäytössä havainnollistavana välineenä. Lisäksi rakennettu ympäristö palvelee myös muiden haittaohjelmien ominaisuuksien selvittämisessä.

### 4.2 Virtuaaliympäristön asennus

Virtuaaliympäristö rakennettiin mahdollisimman paljon ilmaisten ja avoimen lähdekoodin ohjelmistojen pohjalle. Virtuaalisointiin käytettiin VirtualBoxin viimeisintä saatavilla olevaa versiota. Palvelimina käytettiin Ubuntu 12.04 GNU/Linux käyttöjärjestelmää, joita ympäristöön asennettiin kaksi kappaletta, sekä yksi Windows Server 2003. Palvelimien tehtävät oli määritelty niin, että yksi Ubuntu toimi komento- ja hallintapalvelimena, jolla hallittiin bottia ja sen lähettämiä tietoja. Toinen Ubuntu toimi kohdepalvelimena, jonka tehtävänä oli toimia vain webbipalvelimena. Windows Serverin toimi nimipalvelimena, jotta verkko toimisi mahdollisimman paljon oikean internetin tavoin. IP-osoitteita jakavan DHCP-palvelimen roolia hoiti tässä tapauksessa langaton reititin.

Työasemiksi asennettiin virtuaalikoneisiin kaksi 64–bittistä Windows 7 käyttöjärjestelmää toisen toimiessa verkkorikollisen päätteenä ja toisen uhrin työasemana. Kun Zeus oli saatu toimimaan virtuaalikoneilla, testattiin sitä myös erillisellä pöytäkoneella. Tällä pyrittiin varmistamaan, ettei Zeuksen asentaminen virtuaalikoneelle muuttanut sen toimintaa oleellisesti. Asennuskoneena toimi HP:n perustyöasemalle asennettu 32–bittinen Windows 7.

### 4.3 Uhrikoneen saastutus

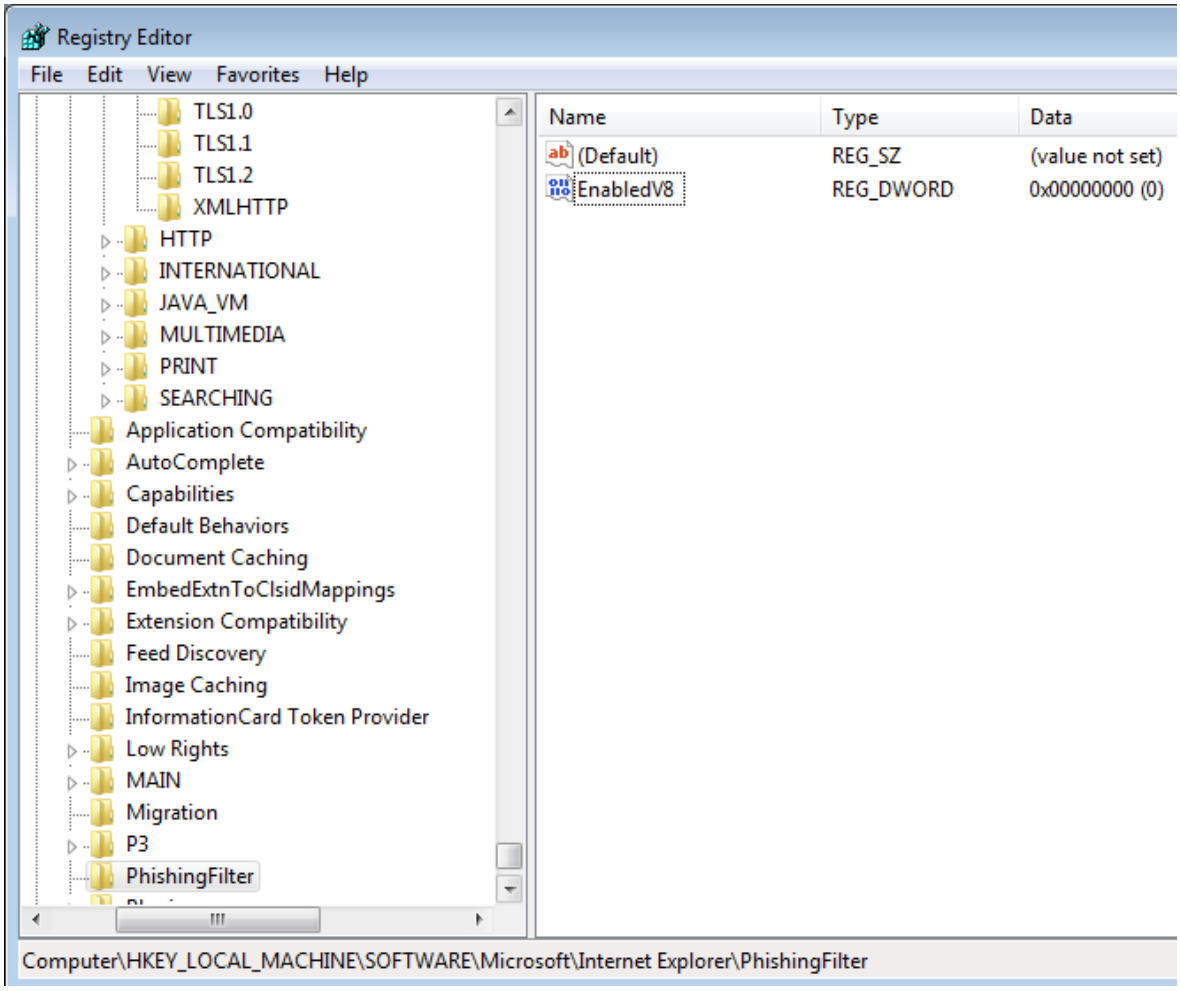
Reaalimaailmassa tyypillinen tapa saastuttaa uhrin kone, on toimittaa asennusohjelma uhrille sähköpostin liitetiedostona, jonka avaamalla uhri saa troijalaisen koneelleen. Uhri voidaan myös ohjata haitalliselle verkkosivulle linkin avulla. Linkki voidaan tarjota joko sähköpostissa, verkkosivulla olevan mainosbannerin kautta tai sosiaalista mediaa hyväksikäyttäen. Esimerkkinä vuonna 2013 raportoitiin Facebook–sivusta, jonka kautta tarjottiin linkkiä Zeusta levittävälle sivustolle (Tom 2013).

Tämän työn tarkoituksena ei ole mennä tietokoneen saastuttamisen yksityiskohtiin, joten Zeusta testatessa koneet saastutettiin yksinkertaisesti toimittamalla Zeuksen latustiedosto koneelle muistitikulla ja ajamalla se käsin. Tätä ennen sammutettiin mah-

dolliset antivirusohjelmat ja Windowsin palomuuri, että ne eivät estäneet testin suorittamista. Testissä käytetty Zeuksen versio oli kaksi vuotta vanha ja sen tunnistetiedot olivat jo kaikkien tunnettujen antivirusohjelmien tiedossa.

Asentaessaan itseään koneelle botti teki muutoksia tietokoneen ja sijoitti itsensä kovalevylle. Asennuksen yhteydessä Zeus tallensi suoritettavan tiedoston seuraavaan kohteeseen C:\Users\"käyttäjänimi"\AppData\Wusoe\esxa.exe. Application Data – kansion alle tulevan kansion ja sen alle tallentuvan ohjelmatiedoston nimet botti muodosti satunnaisesti. Tämän lisäksi Zeus teki Windowsin rekistereihin seuraavan muutoksen: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{B17D99DE-8E6C-D240-A6FA-415363D92966} = C:\Users\"käyttäjänimi"\AppData\Wusoe\esxa.exe. Tällä muutoksella botti varmisti, että se ajetaan uudestaan aina tietokoneen käynnistyksen yhteydessä. Aaltosulkeissa oleva merkkijono on konekohtainen.

Testissä todettiin myös Zeuksen ominaisuus, jolla botti ottaa Internet Explorerin phishing filterin pois päältä. Tämän ominaisuuden avulla selain testaa sivustojen haitallisuutta verkossa olevia haitallisten sivustojen listaa vasten. Alla olevassa kuvassa näkyy, kuinka tietokoneen rekisterissä sijaitseva phishing filterin EnabledV8 -arvon bitti on muutettu botin toimesta nollaksi (Kuvio 4).




Kuvio 4. Internet Explorer 8:n smart screen filtterin kytkeminen pois päältä (kuvankaappaus testiympäristöstä.)

Toisessa Zeuksen avoimeen lähdekoodiin pohjaavassa suositussa versiossa Citadelissa botin ajettava tiedosto tallentuu samaan paikkaan kuin käsiteltävänä olevassa versiossa. Myöskin rekisterimuutokset ovat pysyneet samankaltaisina, toki erilaisia toiminnallisuuksia ja rekisterimuutoksia on Citadelissa enemmän. (Milletary 2012.)

Zeuksen 2.0:aa edeltävässä versiossa botti asentui kahdella eri tavalla riippuen siitä oliko uhri kirjautuneena ylläpitäjän vai tavallisen käyttäjän oikeuksin (Nahorney & Falliere 2009). Vanhemmassa versiossa latauskansiot ja rekisterimuutokset menivät oheisen taulukon mukaisesti (Taulukko 2):

Taulukko 2. Edellisen Zeuksen version (Zbot) tallennuspolut ja rekisterimuutokset (Nahorney & Falliere 2009).

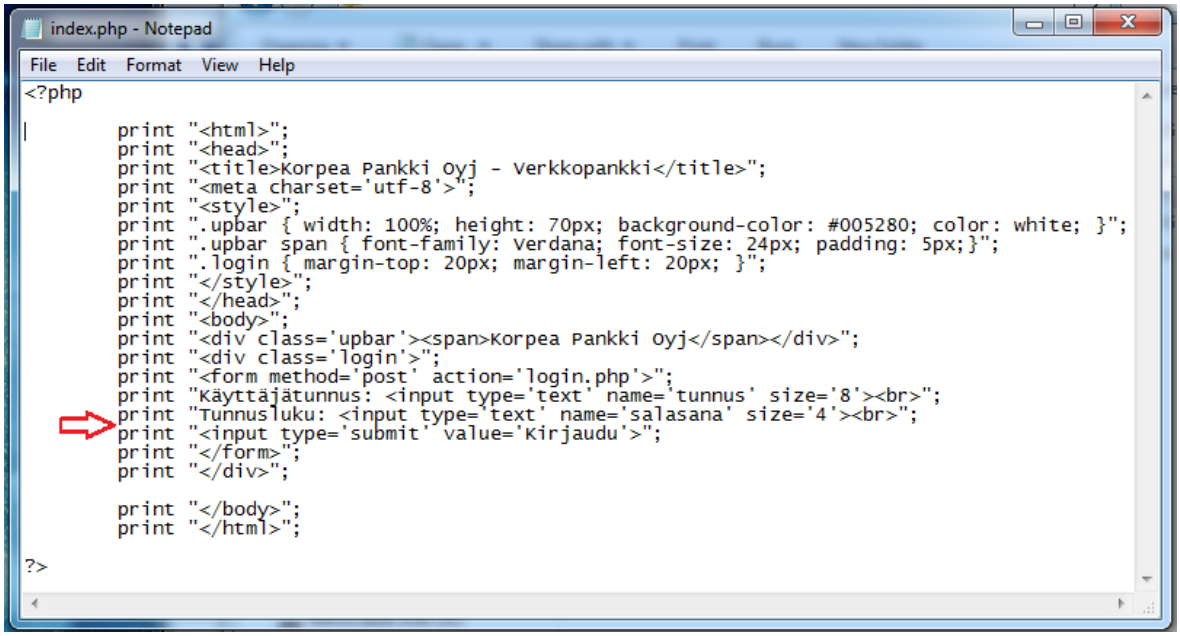
| Käyttäjän rooli | Asennuskansio | Rekisterimuutokset |
|---|---|---|
| Ylläpitäjä | %system32%\sdra64.exe | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Winlogon\"Userinit" = "%System%\userinit.exe, %System%\sdra64.exe" |
| Tavallinen | %UserProfile%\Application Data\sdra64.exe | HKEY_CURRENT_USER\ SOFTWARE \Microsoft\Windows \CurrentVersion\Run\"userinit" = "%UserProfile%\Application Data\sdra64.exe" |

### 4.4 Verkkoliikenteen sieppaaminen

Zeuksen käyttämää man-in-the-browser -tapaa testattiin myös virtuaaliympäristöön asennetulla kohdepalvelimella. Palvelimelle asennetulle webbipalvelimelle luotiin yksinkertainen sisäänkirjautumissivu, jonka näkymää itse tehdyn webinjektion avulla muutettiin. Tällä tavalla voitiin demonstroida Zeuksen tapaa siepata uhrikoneen verkkoliikenne selaimen ja käyttöjärjestelmän rajapinnasta. Reaalimaailmassa webinjektion avulla uhria onnistutaan monesti hämäämään, koska suojatusta yhteydestä kertova lukon kuva ei poistu selaimen osoitepalkista. Testissä ei käytetty suojattua yhteyttä, joten tätä ei voitu testin avulla havainnollistaa. Lomaketietojen sieppaaminen on Zeuksessa toiminnallisesti oletuksena. Tämä voitiin todeta myös testin perusteella. Webinjektiolla ei vaikutettu käyttäjätunnus- ja tunnuslukukenttiin.

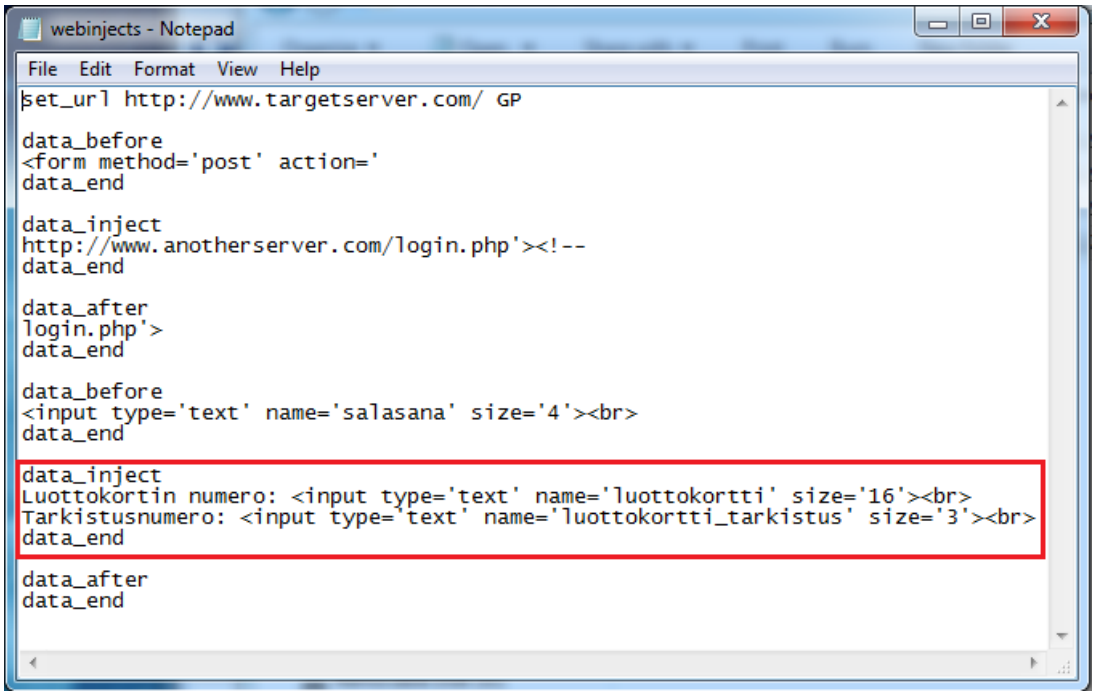
Alla olevissa kuvankaappauksissa esitetään testissä tehty hyvin yksinkertainen webinjektio. Ensimmäisessä kuvassa on esitetty kohdepankin kirjautumissivun lähdekoodi.

Koodiin on merkattu punaisella nuolella kohta, mihin injektoitava koodi tulee (Kuvio 5).



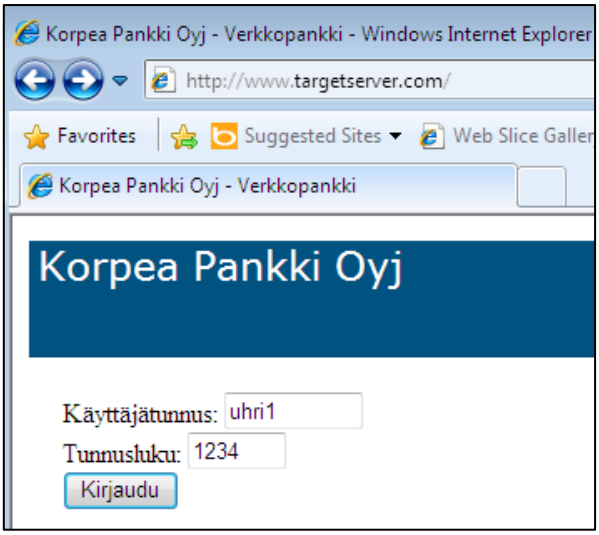

Kuvio 5. Kohdepalvelun nettisivun lähdekoodi (kuvankaappaus testiympäristöstä.)

Seuraavassa kuvassa on testissä käytetty webinjektio. Punaisella laatikolla on koodista merkitty kohta, joka injektoidaan uhrin selaimen näkymään (Kuvio 6).

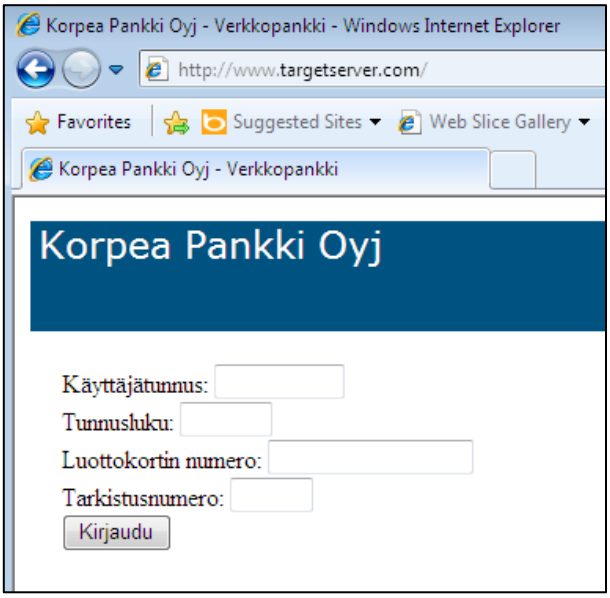



Kuvio 6: Uhrin selaimeen syötettävä koodi (kuvankaappaus testiympäristöstä.)

Botti sieppasi selaimen ja käyttöjärjestelmän välisessä rajapinnassa kohdeosoitteen verkkoliikenteen ja lisäsi siihen itse webinjektioon kirjoitetun koodin. Lopputulos voitiin havaita uhrikoneella, jossa toimivasta injektiosta kertoi kahden luottokorttitietoja kalastelevan syöttöruudun tulostuminen selaimelle. (Kuvio 7 ja Kuvio 8).




Kuvio 7: Kohdesivu ennen saastutusta (kuvankaappaus testiympäristöstä.)




Kuvio 8: Kohdesivu saastutuksen jälkeen (kuvankaappaus testiympäristöstä.)

### 4.5 Päivittäminen ja muut toiminnallisuudet

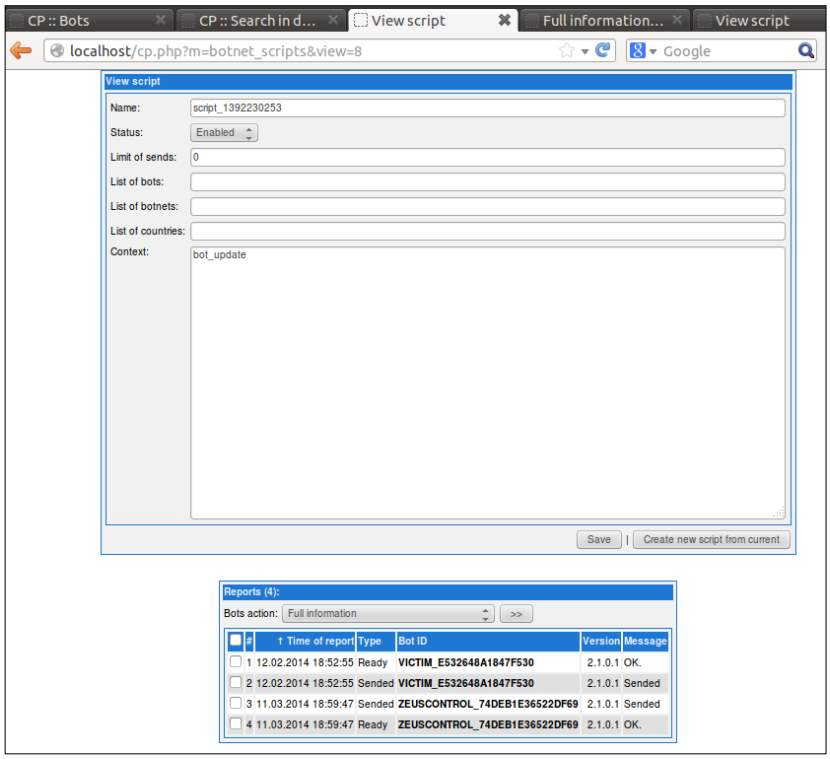
Testiympäristöön luodun komentopalvelimen osoite oli myös annettava botille. Palvelimen osoite syötettiin botin konfiguraatiotiedostoon luontivaiheessa (Kuvio 9). Koh-

dassa timer_config määriteltiin aikaväli, millä botti kävi tarkastamassa päivityksensä edellyttäen, että saastunut kone on verkossa.

```
entry "StaticConfig"
  ;botnet "btn1"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "http://iceixcontrolpanel.com/cfg.bin"
  disable_tcpserver 0
  encryption_key "jNBF43098092jojf209u402jf2polaa"
end
```

Kuvio 9. Osoite, josta botti hakee päivitetyn konfiguraation (kuvankaappaus testiympäristöstä.)

Reaalimaailmassa bottiverkon ylläpitäjä pystyy komentamaan bottia hakemaan uuden päivityksen annetusta osoitteesta komentopalvelimella sijaitsevan hallintapaneelin avulla. Tätä ja muutamaa muuta toiminnallisuutta kokeiltiin testissä asennetun hallintapaneelin avulla. Komennot syötettiin botille paneelissa olevan scripts-toiminteen kautta (Kuvio 10).




Kuvio 10. Hallintapaneelin skriptaus-näkymä (kuvankaappaus testiympäristöstä.)

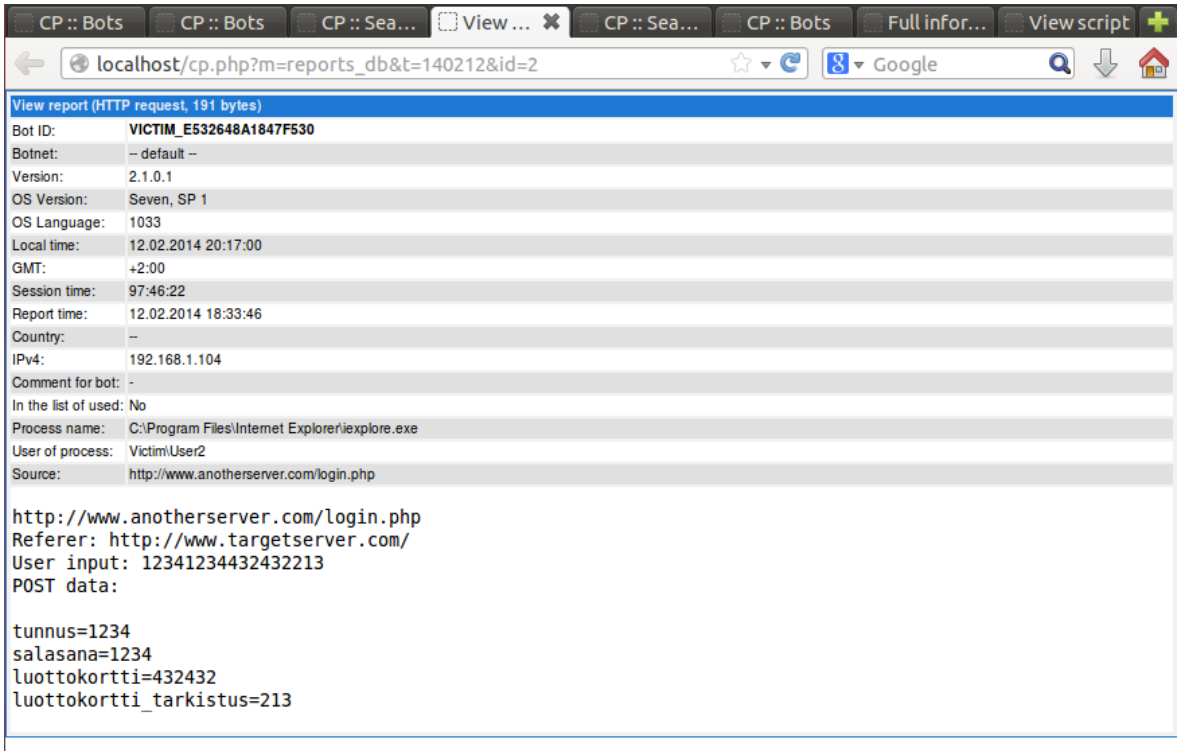
Testiympäristössä suoritetut komennot otettiin Zeuksen ohjekirjasta. Suoritetut komennot on listattu alla näkyvään taulukkoon (Taulukko 3).

Taulukko 3. Testissä botille annetut komennot (Zeus User Guide 2012.)

| Komento | Selite |
|---|---|
| bot_update [url] | Lataa ja päivittää botin konfiguraatio – ja asennustiedoston. |
| bot_uninstall | Poistaa botin koneelta täydellisesti. |
| os_reboot | Käynnistää tietokoneen uudelleen. |
| os_shutdown | Sammuttaa tietokoneen. |
| user_logoff | Kirjaa nykyisen käyttäjän ulos. |
| user_execute | Komennolla voidaan suorittaa uhrin koneella haluttu ohjelma. Ohjelma voidaan ladata internetistä ja suorittaa uhrin koneella tai sitten ohjelma voi olla jo koneella oleva resurssi. Testissä komennolla käynnistettiin onnistuneesti uhrin koneella Windows Mediaplayer. |
| user_homepage_set [url] | Asettaa käyttäjä selaimen kotisivuksi hyökkääjän valitseman sivun. Toimii kaikissa tunnetuissa selaimissa. |

Käytännön testauksessa saastuneelta työasemalta otettiin yhteyttä testin kohdepalvelimeen. Kohdepalvelimen etusivulla oleviin tietokenttiin syötettiin niiden kysymät tiedot. Kentistä kaksi ensimmäistä, tunnusta ja salasanaa kysyvät, tulevat kohdepalvelimelta. Selaimessa olevat jälkimmäiset luottokorttitietoja kysyvät kentät ovat botin syöttämiä. Kun tiedot oli syötetty webbilomakkeelle, niiden siirtyminen todettiin komentopalvelimella sijaitsevalta hallintapaneelilta (Kuvio 11). Kuvassa näkyy myös osa muistakin botin komentopalvelimelleen lähettämistä tiedoista, kuin salasanoista. Botti lähetti komentopalvelimelle yksilöllisen tunnistetietonsa, versionumeron ja käynnissäoloajan. Näiden lisäksi komentopalvelimelle tallentui käyttöjärjestelmän versio ja kieli, saastuneen ko-

neen IP-osoite ja sijainti (geolokaatio), koneella käynnissä olevat prosessit sekä viimeisimmän botin komentopalvelimelle lähettämän raportin aika.




Kuvio 11. Botin kaappaamat tunnukset ja luottokortin tiedot hallintapaneelista nähtynä (Kuvankaappaus testipalvelimelta.)

Testissä saastutettiin vain kaksi konetta, jolloin hallintapaneelin hyödyllisyys ei tullut parhaimmillaan esille. Oikeassa maailmassa bottiverkot saattavat koostua suurimmillaan sadoista tuhansista saastuneista koneista. Pienimmissäkin verkoissa on tuhansia koneita. Vasta näissä tapauksissa hallintapaneelin ominaisuudet, joilla botit voidaan jakaa monenlaiseen luokkaan niiden geolokaation, online-tilan tai käyttöjärjestelmän mukaan, tulevat täysin käyttöön.

### 4.6 Testin tulokset

Testi onnistui täysin odotusten mukaan. Kaikki Zeuksen testatut toiminnallisuudet tulivat esille aivan kuten lähdemateriaalien perusteella oli odotettavissakin. Testin rajauksen vuoksi monia mielenkiintoisia toiminnallisuuksia jäi testaamatta, mutta testissä käy-

tetty virtuaaliympäristö jäi tutkimuskäyttöön ja sitä tullaankin tulevaisuudessa kehittämään entistä tehokkaammaksi. Tarkoitus on myös keventää ympäristöä niin, että se olisi paremmin liikuteltavissa erilaisiin luento- ja koulutustilaisuuksiin. Keventämisen yhteydessä ainakin nimipalvelimena toimiva Windows Server 2003 tullaan vaihtamaan huomattavasti kevyempään Linux-pohjaiseen palvelimeen.

# 5 Johtopäätökset

Tietoturvaa opiskelleista moni on päässyt näkemään ja mahdollisesti myös kokeilemaan, kuinka tietomurto tapahtuu. Itselläni vasta käytännön kokeet avasivat silmäni siihen, kuinka paljon vahinkoa aivan yksinkertaisillakin menetelmillä voidaan saada verkossa aikaan. Tämä ei kerro aina menetelmien, ohjelmien tai varsinaisen murtautujan taidoista vaan siitä, kuinka paljon haavoittuvia ohjelmia tai palveluita verkossa tällä hetkellä on. Samalla tavalla silmäni avautuivat, kun pääsin testaamaan pankkitroijalaista käytännössä. Tapa millä se saa haltuunsa uhrin pankkitunnukset on loppujen lopuksi yksinkertainen, mutta valtavan tehokas. Onnistuneiden verkkopankkipetosten määrään vaikuttaa suuresti se, kuinka paljon haavoittuvia käyttäjiä verkossa on. Poliisina rikoksia tutkiessa ja niihin ilmiöinä tutustuessa joutuu miettimään paljon, kuinka näitä rikoksia voitaisiin estää. Helpoin tapa olisi varmasti tiedon jakaminen kaikille tahoille, jotka jollain tavalla liittyvät verkkopankkipalveluiden käyttöön. Jos kykenisimme kertomaan tavalliselle tietokoneenkäyttäjälle, kuinka pankkitroijalainen toimii ja kuinka se hänen koneelleen tarttuu, saattaisi se lisätä tämän kiinnostusta omaa tietoturvaansa kohtaan. Tavallisten tietokoneenkäyttäjien lisäksi tietoa tulisi jakaa myös näiden rikosten tutkintaan liittyville tahoille, kuten poliiseille ja kohteena olevien pankkien henkilökunnalle.

## 5.1 Tutkimuksen hyödyllisyys

Tämän tutkimuksen tekeminen on lisännyt huomattavasti tietämystäni pankkihaittaohjelmista ja etenkin Zeus-haittaohjelmaperheestä. Työn tekeminen on pakottanut minut liikkumaan pois omalta osaamisalueeltani ja haastanut minut oppimaan uutta. Työn tekeminen palvelee myös omaa työyhteisöäni, jossa minulla on rooli uusien työntekijöiden kouluttajana. Tämän materiaalin ja tutkimuksen yhteydessä valmistuneen virtuaaliympäristön avulla kouluttamisesta tulee tehokkaampaa ja laadukkaampaa.

Oman työpaikkani lisäksi kyselyjä tästä työstä on tullut muun muassa verkkorikoksia hoitavalta syyttäjältä ja verkkopankkipetosten kohteeksi joutuneelta pankilta. Molemmat tahot ovat ilmaisseet kaipaavansa enemmän maallikoille tarkoitettua materiaalia, jonka avulla heitä koskevia tapauksia on helpompi ymmärtää. Syyttäjä on vielä siinä erikoisasemassa, että hänen työnsä on esitellä oikeuteen saakka edenneet tapaukset

tuomarille ja lautamiehille. Tuomarilla ja lautamiehillä ei usein ole kovin syvällistä tietoteknistä osaamista, jolloin pankkihaittaohjelmien toiminnan esittely niin sanotusti kansan kielellä on tärkeää jutun menestymisen vuoksi.

## 5.2 Tulevaisuus

Pankkihaittaohjelmat jatkavat kehittymistään. Zeuksesta on jo kehittynyt muutama uusi variantti, jotka vaikeuttavat niiden havaitsemista entisestään. Myös muiden haittaohjelmaperheiden troijalaiset kehittyvät. Vuoden 2013 lopussa maailmalla Suomea myöten tehtiin havaintoja uudesta troijalaisesta nimeltä NeverQuest. Tulevaisuus näyttää, mikä sen kohtaloksi jää.

Troijalaisen koodi ja sen levittämisen eri muodot kehittyvät samaa tahtia kuin antivirustalot kehittävät omia tuotteitaan niiden löytämiseksi. Phishingiin pohjautuvat hyökkäyskampanjat eivät ole menestyneet Suomessa paljolti erittäin haastavan kielen takia. Tälläkin saralla haittaohjelmien kirjoittajatkin ovat kehittyneet. Viimeisimmissä havaituissa pankkihaittaohjelmissa onkin mukana jo varsin laadukasta Suomen kieltä, jolloin hyökkäysten onnistumisprosentinkin voidaan olettaa nousevan.

Pankkitroijalaisia koodaavien ja niitä käyttöönsä ostavia henkilöitä saattaa motivoida heidän kotimaidensa huono taloudellinen tilanne ja huonot työmarkkinat. Osa nykyaikaisista pankkihaittaohjelmista, on kehitetty entisen Neuvostoliiton alueella. Tuolla alueella elää paljon taitavia ohjelmoijia, joiden on vaikea kieltäytyä heille tehdyistä rahakkaista tarjouksista. Uusia päivitettyjä haittaohjelmia syntyy niin kauan kuin niille on kysyntää Internetin pimeillä markkinoilla. Ainoa keino millä viranomaiset ja yksityinen sektori pystyvät vastaamaan tulevaisuuden uhkiin on tehokas yhteistyö. Yhteistyötä tulisi lisätä ja tehostaa niin ammattitaidon kuin tiedon vaihdon osalta entisestään. Yhteistyötä siviiliorganisaatioiden ja viranomaistahojen kanssa tehdään jo nyt monissa maissa, mutta sen määrän on lisäännyttävä huomattavasti, jotta kaikkein ajantasaisin tieto olisi koko ajan kaikkien toimijoiden saatavilla.

# Lähteet

Doherty, S., Krysiuk, P. & Wueest, C. 2013. The State of Financial Trojans 2013. Luettavissa: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_state_of_financial_trojans_2013.pdf. Luettu: 4.3.2014.

Donohue, B. 2013. The Big Four Banking Trojans. Luettavissa: https://blog.kaspersky.com/the-big-four-banking-trojans/. Luettu: 5.5.2014.

Falliere, N. & Chien, E. 2009. Zeus: King of the Bots. Luettavissa: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf.

Gallagher, S. 2012. New Zeus P2P bots: anonymous cyber-crime ready for mass market. Luettavissa: http://arstechnica.com/business/2012/03/hunt-for-botnets-get-harder-with-new-pure-p2p-zeus-botnet-maker/. Luettu: 2.5.2014.

Mellinger, P. 2011. Crime and malware: A short history of computer fraud. Luettavissa: http://www.computerworlduk.com/in-depth/security/3316463/crime-and-malware-a-short-history-of-computer-fraud/. Luettu: 19.3.2013.

Milletary, J. 2012. Citadel Trojan Malware Analysis. Luettavissa: http://botnetlegalnotice.com/citadel/files/Patel_Decl_Ex20.pdf. Luettu: 13.3.2014.

Nahorney, B. & Falliere, N. 2009. Trojan.Zbot. Luettavissa: http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99&tabid=2. Luettu: 10.3.2014.

RSA. 2012. Cybercrime Trends Report, The Current State of Cybercrime and What to Expect in 2012. Luettavissa: http://www.cs.toronto.edu/~lloyd/TKF/TKF11/11634_CYBRC12_WP_0112.pdf. Luettu 5.5.2014.

RSA. 2013. The Current State of Cybercrime 2013. Luettavissa: http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf. Luettu: 5.5.2014.

Smith, C. 2013. How Malware Attack Web Applications. Luettavissa: https://www.owasp.org/images/1/14/Smith.pdf. Luettu 4.5.2014.

Selvaraj, K. 2010. A brief look at Zeus/Zbot 2.0. Luettavissa: http://www.symantec.com/connect/blogs/brief-look-zeuszbot-20. Luettu: 10.3.2014.

Tarakanov, D. 2013. The inevitable move - 64-bit ZeuS has come enhanced with Tor. Luettavissa: https://www.securelist.com/en/blog/208214171/The_inevitable_move_64_bit_ZeuS_has_come_enhanced_with_Tor. Luettu: 5.5.2014.

Tom, D. 2013. Zeus Trojan returns. Luettavissa: http://www.techspot.com/news/52795-zeus-trojan-returns-facebook-being-used-to-spread-the-infection.html. Luettu: 10.3.2014

Torproject. Tor: Overview. Luettavissa: https://www.torproject.org/about/overview.html.en. Luettu: 5.5.2014.

Trusteer. 2013. Man-in-the-browser (MitB). Luettavissa: http://www.trusteer.com/glossary/man-in-the-browser-mitb. Luettu: 5.5.2014

Wattanajantra, A. 2011. Zeus Trojan is creating an army of young cyber criminals. Luettavissa: http://www.theinquirer.net/inquirer/news/2080163/zeus-trojan-creating-army-cyber-criminals. Luettu: 2.5.2014.

Wyke, J. 2011. What is Zeus? Luettavissa: http://www.sophos.com/medialibrary/PDFs/technical%20papers/Sophos%20what%20is%20zeus%20tp.pdf. Luettu: 5.5.2014.

# Liitteet

## Liite 1: Testiympäristön tekniset tiedot

| Pöytäkoneet (fyysiset) |
| --- |
| Isäntäkone (host)<br>Käyttöjärjestelmä: 64-bit Windows 7 Pro SP1<br>Prosessori ja muisti: Intel Core i7-3770K CPU 3.50GHz 32,0 GB RAM |
| Uhrikone HP Compaq<br>Käyttöjärjestelmä: 32-bit Windows 7 SP1<br>Prosessori ja muisti: CPU 3.00 GHz Intel Pentium 4 RAM 3 GB |

| |
|---|
| Virtualisoidut palvelimet ja työasemat, sekä niiden verkko-osoitteet<br><br>Virtualisointi toteutettiin VirtualBoxilla (versio 4.3.6 r91406) |
| Kohdepalvelin<br>IP: 192.168.1.25<br>Domain: targetservice.com<br>Käyttöjärjestelmä: 64-bit Ubuntu 12.04.3 LTS<br>Kernelin ja tarvittavan palvelinohjelmien versiot:<br>Linux ubuntu 3.8.0-29-generic #42~precise1-Ubuntu SMP Wed Aug 14 16:19:23 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux<br>php5-common 5.3.10-1ubuntu3.9<br>phpmyadmin 4:3.4.10.1-1<br>apache2 2.2.22-1ubuntu1.4<br>mysql-server-5.5 5.5.34-0ubuntu0.12.04.1 |
| Virtualbox data<br>Name: TargetSevice<br>Guest OS: Ubuntu 12.04.3 LTS (64 bit)<br>UUID: e8c54c14-eea5-4633-a12b-092a36abc220<br>Config file: E:\Virtualmachines\TargetSevice\TargetSevice.vbox<br>Snapshot folder: E:\Virtualmachines\TargetSevice\Snapshots<br>Log folder: E:\Virtualmachines\TargetSevice\Logs<br>Hardware UUID: e8c54c14-eea5-4633-a12b-092a36abc220<br>Memory size: 2048MB<br>VRAM size: 32MB<br>CPU exec cap: 100%<br>Firmware: BIOS<br>Number of CPUs: 2 |

| |
|---|
| Zeuksen komentopalvelin<br>IP: 192.168.1.30<br>Domain: iceixcontrolpanel.com<br>Käyttöjärjestelmä: 64-bit Ubuntu 12.04.3 LTS<br>Zeuksen kannalta oleelliset asennetut ohjelmat:<br>Linux ubuntu 3.8.0-29-generic #42~precise1-Ubuntu SMP Wed Aug 14 16:19:23 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux<br>php5-common 5.3.10-1ubuntu3.9<br>phpmyadmin 4:3.4.10.1-1<br>apache2 2.2.22-1ubuntu1.4<br>mysql-server-5.5 5.5.34-0ubuntu0.12.04.1 |
| Virtualbox data<br>Name: IceIXControlPanel<br>Guest OS: Ubuntu 12.04.3 LTS (64 bit)<br>UUID: a02234bb-8632-4021-84d5-74fa2df17530<br>Config file: E:\Virtualmachines\IceIXControlPanel\IceIXControlPanel.vbox<br>Snapshot folder: E:\Virtualmachines\IceIXControlPanel\Snapshots<br>Log folder: E:\Virtualmachines\IceIXControlPanel\Logs<br>Hardware UUID: a02234bb-8632-4021-84d5-74fa2df17530<br>Memory size: 2048MB<br>VRAM size: 32MB<br>CPU exec cap: 100%<br>Firmware: BIOS<br>Number of CPUs: 2 |

| |
|---|
| Nimipalvelin<br>IP: 192.168.1.10<br>Käyttöjärjestelmä: Windows Server 2003 R2 |
| Virtualbox data<br>Name: Win2003srv_dns<br>Guest OS: Other Windows<br>UUID: a6cf63cb-6d38-4949-ad07-096a1e5032e7<br>Config file: E:\Virtualmachines\Win2003srv_dns\Win2003srv_dns.vbox<br>Snapshot folder: E:\Virtualmachines\Win2003srv_dns\Snapshots<br>Log folder: E:\Virtualmachines\Win2003srv_dns\Logs<br>Hardware UUID: a6cf63cb-6d38-4949-ad07-096a1e5032e7<br>Memory size: 2048MB<br>VRAM size: 16MB<br>Firmware: BIOS<br>Number of CPUs: 1 |

| |
|---|
| Hakkerin työasema<br>IP: DHCP<br>Käyttöjärjestelmä: 64-bit Windows 7 Pro SP1 |
| Name: BotHerder-Win7<br>Guest OS: Windows 7 (64 bit)<br>UUID: 1ea15db7-147c-401e-9c1e-676a36f75b95<br>Config file: E:\Virtualmachines\BotHerder-Win7\BotHerder-Win7.vbox<br>Snapshot folder: E:\Virtualmachines\BotHerder-Win7\Snapshots<br>Log folder: E:\Virtualmachines\BotHerder-Win7\Logs<br>Hardware UUID: 1ea15db7-147c-401e-9c1e-676a36f75b95<br>Memory size: 6172MB<br>VRAM size: 32MB<br>Firmware: BIOS<br>Number of CPUs: 2 |

| |
|---|
| Uhrin työasema<br>IP: DHCP<br>Käyttöjärjestelmä: 64-bit Windows  Pro SP1 |
| Virtualbox data<br>Name: Infected<br>Guest OS: Windows 7 (64 bit)<br>UUID: 36f4b0e5-554a-4b74-b1fb-05cab0d1aa53<br>Config file: E:\Virtualmachines\Infected\Infected.vbox<br>Snapshot folder: E:\Virtualmachines\Infected\Snapshots<br>Log folder: E:\Virtualmachines\Infected\Logs<br>Hardware UUID: 36f4b0e5-554a-4b74-b1fb-05cab0d1aa53<br>Memory size: 6172MB<br>VRAM size: 32MB<br>Firmware: BIOS<br>Number of CPUs: 2 |