Esa Aikio

# Bot-verkot pahantahtoisissa käyttötarkoituksissa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

26.2.2014

Metropolia

| | |
|---|---|
| Tekijä<br>Otsikko<br><br>Sivumäärä<br>Aika | Esa Aikio<br>Bot-verkot pahantahtoisissa käyttötarkoituksissa<br><br>46 sivua<br>26.2.2014 |
| Tutkinto | insinööri (AMK) |
| Koulutusohjelma | tietotekniikka |
| Suuntautumisvaihtoehto | ohjelmistotekniikka |
| Ohjaaja | lehtori Kimmo Sauren |

Insinöörityön tavoitteena oli tutustua bot-verkkojen teoriaan, niiden teknisiin toteutuksiin sekä käytännössä rakentaa bot-verkko. Työssä keskityttiin bot-verkkojen haitallisiin käyttötarkoituksiin vaikka bot-verkkoja voidaan käyttää myös hyödyllisiin tarkoituksiin.

Työn teoriaosassa selvitetään bot-verkkojen eri rakenteet sekä tyypillisimmät käyttökohteet. Käytännön testaus toteutettiin rakentamalla bot-verkko asiakaskoneina olleiden Windows XP -käyttöjärjestelmällä olevien tietokoneiden sekä Linux-käyttöjärjestelmällä toimivan bot-verkon hallintapalvelimen välille. Työssä asiakaskoneille jaettiin Zeus-haittaohjelma, jonka suorituksen jälkeen asiakaskoneet liittyivät bot-verkon jäseniksi. Tämän jälkeen seurattiin asiakaskoneiden toimintaa, kommunikointia hallintapalvelimen kanssa sekä koneiden välittämiä tietoja hallintapalvelimelle.

Työn tuloksena selvisi, että mikäli tietokoneessa ei ole erillistä ajan tasalla olevaa virustorjuntasovellusta, työssä esitelty haittaohjelma tartuttaa tietokoneen lähes huomaamattomasti. Tartunnan jälkeen tietokoneella olevat kaikki käyttäjän tiedot sekä hänen internetiin syöttämät tiedot ovat vaarassa joutua bot-verkon ylläpitäjän haltuun. Internetiin syötetyt kirjautumis- sekä muut tiedot välittyvät selkokielisenä bot-verkon ylläpitäjälle huolimatta siitä, että käyttäjällä olisi suojattu yhteys palveluntarjoajaan.

Työssä testattiin myös online-virustorjuntapalveluiden ajamista asiakaskoneissa haittaohjelman tartunnan jälkeen. Tarkistuksen tuloksena selvisi että F-Securen online-tarkistus ei löytänyt haittaohjelmaa asiakaskoneesta, muiden testattujen palveluiden tunnistettua haittaohjelman onnistuneesti.

Yleisenä tuloksena myös tämän työn perusteella voidaan todeta, että on tärkeää pitää tietokoneiden tietoturvasta vastaavat käyttöjärjestelmäpäivitykset sekä sovellukset ajan tasalla. Työssä ilmeni myös se, että erillisen virustorjuntasovelluksen asentaminen tietokoneisiin on suositeltavaa.

| | |
|---|---|
| Avainsanat | Bot-verkko, bot, Zeus, haittaohjelma |

| | |
|---|---|
| Author<br>Title<br><br>Number of Pages<br>Date | Esa Aikio<br>Malicious uses of botnets<br><br>46 pages<br>26 February 2014 |
| Degree | Bachelor of Engineering |
| Degree Programme | Information Technology |
| Specialisation option | Software Engineering |
| Instructor | Kimmo Sauren, Senior Lecturer |

The objective of the project described in this thesis was to study botnets in theory, their technical implementations and to build a botnet in practice. This thesis concentrates on malicious uses of botnets although botnets can be used also for beneficial purposes.

The theoretical section of this thesis introduces different technical implementations and typical malicious uses of botnets. In practice, a botnet was built using client workstations with the Windows XP operating system and the botnet's command and control server with the Linux operating system. Malware called Zeus was distributed to workstations, and after it was executed, workstations became members of the botnet. After the infection of the workstations, their operations, communication between the command and control server and data workstations provided were monitored.

As a result it was noticed that if a workstation does not have antivirus software installed, the malware introduced in this thesis infects the workstation almost without noticing. After infection all of the data stored on the user's workstation and the information the user provides via the internet is in danger of being delivered to the botnet administrator. The user's login and other information provided via the internet are forwarded to the botnet administrator despite the user having a secure connection to the service provider.

In the project described in this thesis also online antivirus tools were tested after the client workstations were infected. Scanning results indicated that the online antivirus tool of F-Secure did not find malware while other tested online tools found malware successfully.

Based on this thesis it can be said that it is important to keep the operating system and other software up to date and to install security updates. Installing standalone antivirus software is also recommended.

| | |
|---|---|
| Keywords | botnet, bot, Zeus, malware |

## Sisällys

## Lyhenteet

| | |
|---|---|
| BOT | Lyhenne sanasta robot. Tässä työssä tarkoittaa bot-verkon asiakaskonetta. |
| C&C | *Command & Control*. Bot-verkon hallintapalvelin. |
| DHCP | *Dynamic host configuration protocol*. Verkkoprotokolla, jonka tehtävä on jakaa verkko-osoite verkkoon kytkeytyville päätelaitteille. |
| DDOS | *Distributed denial of service*. Hajautettu palvelunestohyökkäys, jossa palveluun kohdistetaan useasta lähteestä suuri määrä liikennettä palvelun toiminnan lamauttamiseksi. |
| DNS | *Domain name system*. Nimipalvelujärjestelmä, jonka tehtävä on muuttaa selkokieliset internet osoitteet IP osoitteiksi. |
| FTP | *File transfer protocol*. Asiakas-palvelinperiaatteella toimiva tiedonsiirtoprotokolla. |
| HTML | *Hypertext markup language*. Kuvauskieli, jolla voidaan rakentaa hyperlinkkejä sisältävää tekstiä. Tunnetaan erityisesti internet-sivujen kuvauskielenä. |
| HTTP | *Hypertext transfer protocol*. Tiedonsiirtoprotokolla, jonka yleisin käyttökohde on internetin selaimen (asiakas) ja palvelimen (palvelin) välisessä liikenteessä. |
| HTTPS | *Hypertext transfer protocol secure*. HTTP-protokollan suojattu versio, jossa käytetään HTTP- ja SSL-protokollan yhdistelmää. |
| IP | *Internet protocol*. Tietoliikenneprotokolla, jonka tehtävä on ip-tietoliikennepakettien toimittaminen päätelaitteille annettujen ip-osoitteiden perusteella. |
| IRC | *Internet relay chat*. Pikaviestipalvelu, joka mahdollistaa reaaliaikaisen keskustelun internetin välityksellä. |

| | |
|---|---|
| JAVA | Ohjelmistoalusta, johon kuuluu mm. laitteistoriippumaton ohjelmointikieli. |
| MYSQL | Relaatiotietokantaohjelmisto. Avoimeen lähdekoodiin perustuva tietokantaohjelmisto. |
| NAT | *Network address translation*. Osoitteenmuunnostekniikka, joka mahdollistaa usean laitteen käyttämisen yhdellä ulkoisella ip-osoitteella. |
| P2P | *Peer to peer*. Vertaisverkko, jossa toimiva päätelaite toimii sekä palvelimena että asiakkaana verkon muille päätelaitteille. |
| PDF | *Portable document format*. Adoben kehittämä ohjelmistoriippumaton tiedostomuoto, jota käytetään yleisimmin sähköisissä julkaisuissa. |
| PHP | *Php: Hypertext Preprocessor*. Ohjelmointikieli, joka yleisimmin tunnetaan palvelinpohjaisten dynaamisten internet-sivujen luomisesta. |
| RC4 | *Ron's code 4, Rivest cipher 4*. Symmetrinen salausalgoritmi, joka salaa tiedon tavu kerrallaan. |
| SOCKS | *Socket secure*. Internetprotokolla, jota käytetään asiakas-palvelin yhteyksissä pakettien reitittämiseen välityspalvelimen kautta. |
| SSL | *Secure sockets layer*. Salausprotokolla, jota käytetään mm. internet -liikenteen salaukseen http-protokollan kanssa. |
| UPNP | *Universal plug and play*. Ryhmä verkkoprotokollia, jotka sallivat verkossa olevien päätelaitteiden havaita toisensa sekä muodostaa yhteyksiä toisiinsa. |
| XAMPP | Avoimen lähdekoodin ohjelmistopaketti, joka sisältää Apache http-palvelimen, MySQL-tietokantaohjelmiston sekä tuen PHP ja PERL-ohjelmointikielille. |

# 1 Johdanto

Internet luo rikollisille houkuttelevan mahdollisuuden rikosten suorittamiseen palveluiden siirryttyä ja yhä siirtyessä enenevissä määrin tietoverkkojen avulla suoritettaviksi. Tietoverkkojen avulla rikolliset tavoittavat helposti ja pienin kustannuksin moninkertaisen määrän mahdollisia rikoksen kohteita verrattuna perinteiseen rikollisuuteen. Tyypillisiä tietoverkoissa esiintyviä, taloudellista hyötyä tavoittelevia, rikoksia ovat erilaiset huijaukset, käyttäjien henkilökohtaisten tietojen kaappaaminen sekä rikokset suoraan käyttäjää ja käyttäjän verkkopankkia kohtaan. Tietoverkkojen käytön laajentuessa koskemaan suurta osaa väestöä, ei maantieteellisiä rajoja rikosten kohteille myöskään ole. Osaavalle tietoverkkojen käyttäjälle myös rikoksen jälkien peittely tai jälkien väärentäminen on suhteellisen helppoa.

Huolimatta siitä, että käyttäjien tietoisuus mahdollisista tietoverkkojen riskeistä on lisääntynyt, MTV uutisoi 28.11.2013 verkkosivuillaan, että vuonna 2012 suomalaisilta tileiltä varastettiin onnistuneesti noin 800 000 euroa verkkorikosten avulla [1]. Haittaohjelmat kehittyvät yhä monimutkaisemmiksi ja vaikeammiksi havaita, sekä tavallisille käyttäjille että myös tietoturvapalveluita tarjoaville yrityksille ja heidän sovelluksilleen.

Bot-verkot ovat laajoja etähallittavia tietokoneiden verkostoja. Termi bot on lyhenne sanasta robot. Haittaohjelmalla saastutettua konetta kutsutaan bot-asiakaskoneeksi, muita käytettyjä termejä ovat mm. zombie-kone. Bot-verkon haltija käyttää tällaista konetta erilaisten automaattisten tehtävien suorittamiseen ilman tietokoneen todellisen käyttäjän tietoa tai suostumusta.

Bot-verkkoja voidaan käyttää sekä hyväntahtoisiin että haitallisiin ja rikollisiin käyttötarkoituksiin. Kuten monet muutkin keksinnöt, myös bot-sovellukset olivat alun perin hyödyllisiin tarkoitusperiin kehitettyjä. Ensimmäisenä bot-sovelluksena pidetään 1980 -luvun loppupuolella IRC-istuntoihin kehitettyjä bot-sovelluksia, jotka emuloivat todellisia käyttäjiä ylläpitääkseen IRC-kanavaa ja IRC-istuntoja käyttäjien poissa ollessa.

Julkisuudessa bot-verkot yhdistetään yleensä rikollisiin käyttötarkoituksiin, joihin myös tässä työssä keskityn. Bot -verkkojen toiminnassa verkon ylläpitäjän päätavoite on yleensä taloudellisen hyödyn tavoittelu, tosin bot-verkko mahdollistaa myös muunlaiset rikokset kuten esimerkiksi laittoman materiaalin jakamisen, mutta tässä työssä keskityn

taloudelliseen puoleen. Viime aikoina julkisuudessa ovatkin olleet bot-verkot, joilla pyritään kaappaamaan käyttäjien henkilökohtaisia tietoja sekä vaikuttamaan käyttäjien verkkopankki-istuntoihin taloudellisen hyödyn saavuttamiseksi.

Tämän työn tarkoituksena tutkia bot-verkkojen teoriaa, esitellä niiden käyttötapoja ja käyttökohteita erityisesti haitallisiin käyttötarkoituksiin liittyen. Lisäksi tarkoituksena on käytännössä perustaa bot-verkko ja testata sen toimintaa hallintapalvelimen ja asiakaskoneiden näkökulmasta.

# 2 Bot-verkkojen tekniset ratkaisut

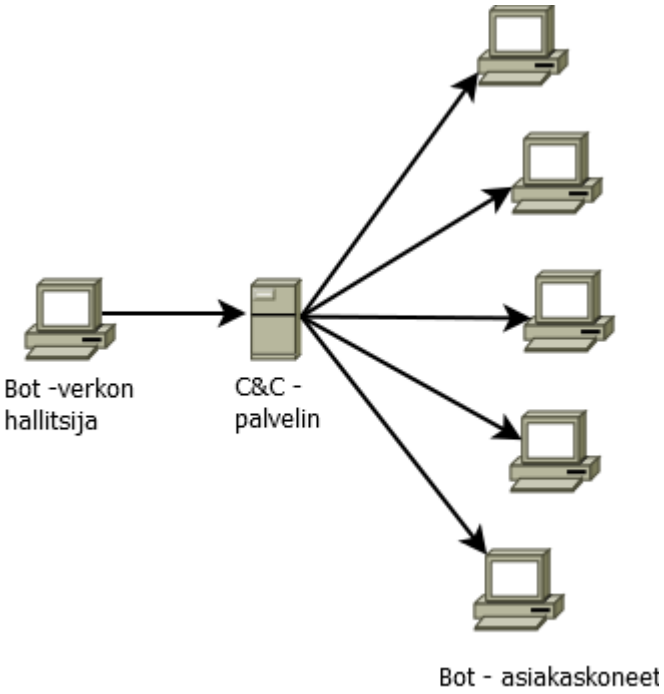
## 2.1 Bot-verkon rakenne

Perinteiset bot-verkot koostuvat asiakaskoneista (bot) sekä yhdestä tai useammasta Command and Control (C&C) -palvelimesta, joilla bot-koneita hallitaan ja ylläpidetään. Bot-verkot jaotellaan yleisesti keskitetyksi tai hajautetuksi verkoksi, tosin bot-verkkoja voidaan jaotella myös yhteysprotokollan mukaan. Hajautetuissa bot-verkoissa asiakaskoneet voivat toimia sekä hallintapalvelimina että asiakaskoneina.

### 2.1.1 Keskitetty bot-verkko

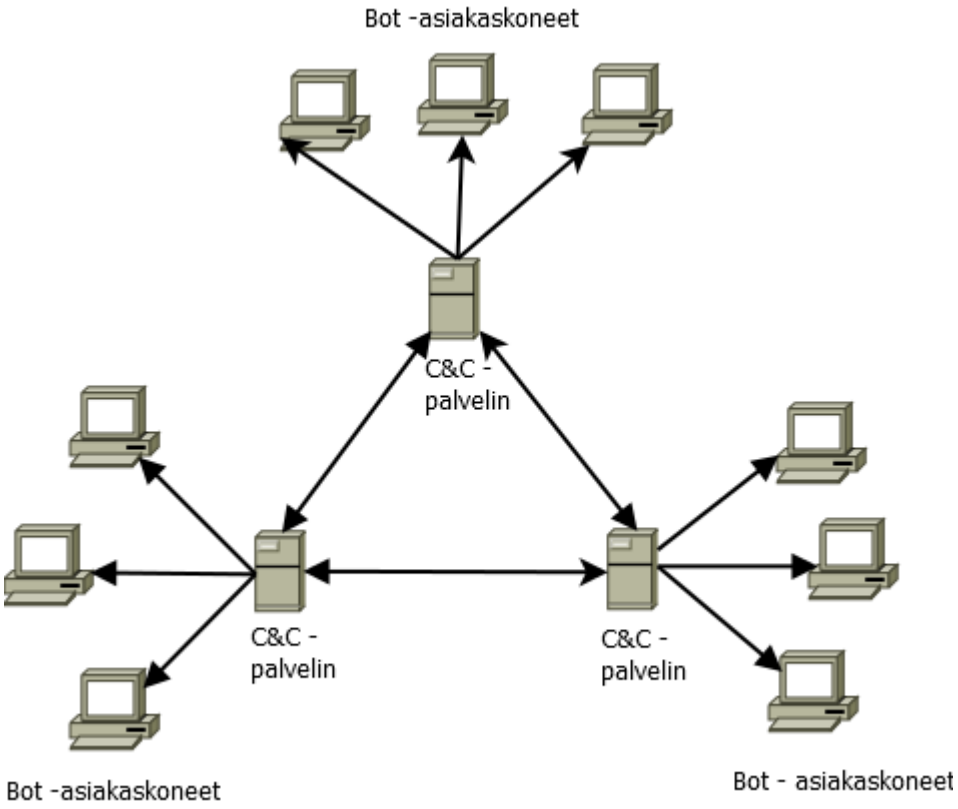
Keskitetyt bot-verkot ovat yleisimmin tunnettuja ja myös eniten tutkittuja. Monet ensimmäisistä ja yleisimmistä bot-verkoista käyttivät IRC-palvelimia keskitettyinä hallintapalvelimina, mutta nykyään yleisemmin on käytössä muita yhteysprotokollia kuten normaalin internet liikenteen käytössä oleva HTTP-protokolla, sen salattu versio HTTPS-protokolla sekä myös vertaisverkkoliikenteestä tunnettu P2P (peer-to-peer)-protokolla. Keskitetyn bot-verkon heikkous on sen perustuminen yhteen keskitettyyn hallintapalvelimeen. Hallintapalvelimen löytyminen ja verkosta poistaminen riittää estämään kyseisen verkon toiminnan. Palvelimen poistaminen ei kuitenkaan poista asiakaskoneilla siellä olevia haittaohjelmia mutta mikäli haittaohjelmissa on ohjelmoituna yksi tietty hallintapalvelin ja sen osoite, estyy verkon toiminta poistamalla palvelin verkosta. [2.]

Tämän estämiseksi bot-verkon ylläpitäjä voi myös käyttää tiettyjä DNS-palveluita, joissa palvelimen ip-osoite saadaan nopeasti vaihdettua ja yhteys asiakaskoneisiin palautettua, mikäli yksi palvelin putoaa verkosta pois. Kuvassa 1 on esitetty perinteinen yhden hallintapalvelimen (C&C-palvelin) piirissä toimiva bot-verkko.



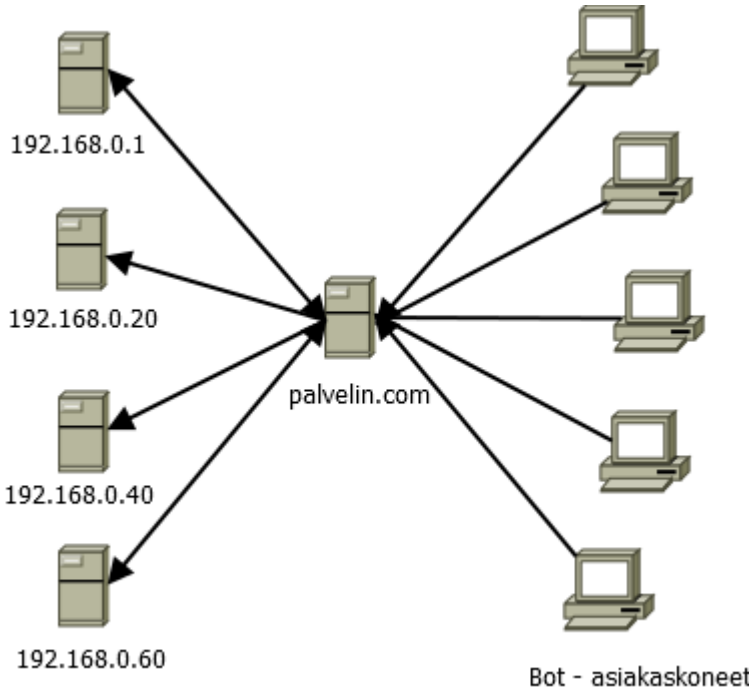

**Kuva 1. Keskitetty bot-verkko.**

Bot-verkko voidaan rakentaa myös niin että hallintapalvelimia on useita. Tällöin yhden palvelimen putoaminen verkosta pois ei lamauta koko verkkoa. Tällaisen verkon rakentaminen on kuitenkin haastavampaa ja vaatii enemmän suunnitelmallisuutta kuin yhteen palvelimeen perustuva bot-verkko. Mikäli bot-verkko jakaantuu usealle eri mantereelle, voi hallintapalvelimet myös jakaa maantieteellisesti lähemmäs asiakaskoneita, jolloin yhteydetkin palvelimen ja asiakaskoneen välillä ovat nopeammat. [3.] Kuvassa 2 on esitetty periaatekuva useamman hallintapalvelimen bot-verkosta.




**Kuva 2. Usean hallintapalvelimen bot-verkko**

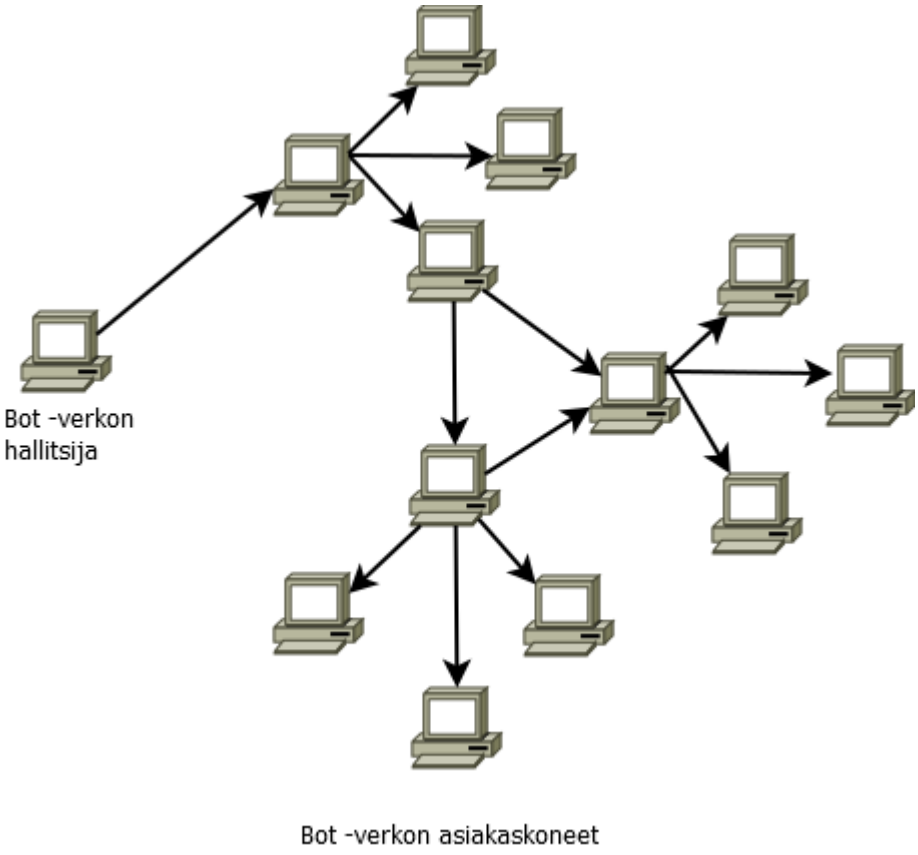
Useampaan hallintapalvelimeen perustuu myös bot-verkoissa yleisesti käytössä oleva ns. fast flux-tekniikka, jossa yhteen domain-nimeen on liitetty useita eri ip-osoitteita. Tekniikkaa käytetään siten, että DNS-palvelussa vaihdellaan nopeasti nimeen liitettyä ip-osoitetta. Bot-verkon asiakaskoneilla on tieto pelkästään domain-nimestä, johon koneet ottavat yhteyttä. Tällöin yhden ip-osoitteen perusteella poistetun palvelimen verkosta poistuminen ei lamauta koko verkkoa, vaan domain-nimeen liitetyn ip-osoitteen muututtua toimivaan palvelimeen, on verkko taas toimintakykyinen. Kuvassa 3 esitetään, miten bot-verkon asiakaskoneet ottavat yhteyttä hallintapalvelimeen palvelin.com osoitteella, joka voi ohjautua mihin tahansa domain-nimen takana olevasta useasta ip-osoitteesta.




**Kuva 3. Fast flux periaate.**

### 2.1.2 Hajautettu bot-verkko

Hajautetussa bot-verkossa käytetään yleisesti vertaisverkoista tunnettua P2P (peer-to-peer)-protokollaa. Hajautetuissa verkoissa bot-verkon asiakaskoneet kommunikoivat keskenään vertaisverkon tavoin yhden keskitetyn hallintapalvelimen sijaan. Voidaankin sanoa, että asiakaskoneet vertaisverkossa toimivat sekä hallintapalvelimina että asiakaskoneina. Verkko toimii siten, että asiakaskoneet lähettävät toisilleen verkon hallitsijan välittämät komennot, joten verkon hallitsijalla tulee olla pääsy ainoastaan yhdelle bot-verkon koneelle hallitakseen koko verkkoa. Komentojen jakaminen on toteutettu siten, että jokaisella asiakaskoneella on lista kyseisen koneen bot-verkkoon kuuluvista naapurikoneista, joille asiakaskone välittää saamansa komennot. Nämä asiakaskoneet taas välittävät vastaanottamansa komennot omille naapureilleen jne., kunnes uudet komennot ovat välitetty kaikille verkon koneille. Kuvassa 4 on esitetty hajautun P2P-verkossa toimivan bot-verkon periaate.[4.]




**Kuva 4. Hajautettu bot-verkko.**

Hajautetun bot-verkon perustaminen alkaa asiakaskoneiden hankkimisella. Asiakaskoneiden hankkiminen tapahtuu kuten muissa bot-verkoissa, haittaohjelman jakamisella asiakaskoneille. Mikäli asiakaskoneet hankitaan jo olemassa olevasta P2P-verkosta, asiakaskoneet voivat kommunikoivat bot-verkossa käyttäen kyseistä P2P-protokollaa. Mikäli taas asiakaskoneet ovat hankittu P2P-verkon ulkopuolelta, täytyy asiakaskoneelle välittää tieto P2P-verkon protokollasta sekä verkossa jo olevista asiakaskoneista. Tieto näistä asiakaskoneista voidaan välittää joko ohjelmoituna haittaohjelman koodiin tai välittämällä haittaohjelmassa verkko-osoite, josta asiakaskone noutaa muiden bot-verkon asiakaskoneiden tiedot. Yleisesti käytössä olevien P2P-protokollien käyttö on bot-verkon hallinnassa on varmempaa, koska nämä protokollat ovat yleensä jo testattu toimiviksi.

P2P-verkossa käskyjen jakaminen bot-koneille voi tapahtua joko pull- tai push mekanismin avulla. Pull mekanismi viittaa perinteiseen bot-verkkoon, jossa asiakaskoneet kysyvät tietyin aikavälein verkon muilta koneilta suoritettavia komentoja. Perinteisessä bot-verkossa tämä tapahtuu kysymällä tietoja hallintapalvelimelta.

Pull-mekanismi voi tapahtua vertaisverkossa normaalistikin tapahtuvan tiedostohaun mukana. Asiakaskoneille jaetussa haittaohjelmassa on bot-verkon ylläpitäjän sisällyttämä hakuparametri, jota asiakaskoneet hakevat ylläpitäjän määrittämin aikavälein kyseisestä vertaisverkosta. Verrattuna normaaliin vertaisverkkojen tiedostojen jakamiseen, ylläpitäjä jakaa tiedostojen sijaan suoritettavia komentoja ja tehtäviä asiakaskoneille. Tiedostot voivat sijaita millä tahansa bot-verkon ylläpitäjän hallitsemalla asiakaskoneella, joten keskitettyä hallintapalvelinta ei tarvita. Hakuparametrit voivat olla ylläpitäjän määrittämiä tiedostonimiä tai esimerkiksi hash arvoja, jotka lasketaan bot-verkon ylläpitäjän määrittämän algoritmin avulla. Näin ylläpitäjä saa salattua haettavat komennot.

Push-mekanismissa asiakaskone taas välittää itse komentoja eteenpäin. P2P-verkoissa asiakaskoneet ovat tietoisia toisista saman verkon koneista, mutta ongelmana voi olla se, että bot-verkon asiakaskonetta lähellä olevat koneet eivät kuulukaan kyseiseen bot-verkkoon eivätkä välitä saamiaan komentoja enää eteenpäin. Tätä ongelmaa on bot-verkoissa kierretty mm. siten, että bot-verkon asiakaskoneet ilmoittavat vertaisverkkoon että heillä on jaettavana suosittuja tiedostoja, jotka kuitenkin sisältävät myös tai pelkästään bot-verkon ylläpitäjän asiakaskoneille määrittämiä komentoja. Suositut tiedostot tulevat useammin ladatuiksi ja näin todennäköisyys komentojen leviämiselle asiakaskoneille kasvaa.

Toinen push-mekanismiin liittyvä komentojen välitystapa liittyy siihen mikäli asiakaskone on tietoinen että vertaisverkon lähellä olevissa koneissa on samaan bot-verkkoon kuuluvia koneita. Tällöin asiakaskone voi liittää vertaisverkkoon lähetettävään kyselyyn komentoja, jotka vain toinen samaan verkkoon kuuluva asiakaskone osaa tulkita oikein ja välittää taas komentoja eteenpäin. [5.]

### 2.1.3 Yhteysprotokollaan perustuva jaottelu

Toinen tapa jaotella bot-verkkoja on C&C-palvelimen ja bot-asiakaskoneiden yhteysprotokollaan perustuva jaottelu. Bot-verkoissa tavattuja yhteysprotokollia ovat mm. seuraavat:

- IRC-protokollaan perustuva, jossa asiakaskoneet ilmoittautuvat tietylle IRC-palvelimelle ja tietylle IRC-kanavalle, jonka kautta asiakaskoneita ohjataan.

IRC-protokollan kautta muodostettu bot-verkko oli yksi ensimmäisistä ja aiemmin yleisin käytössä ollut protokolla.

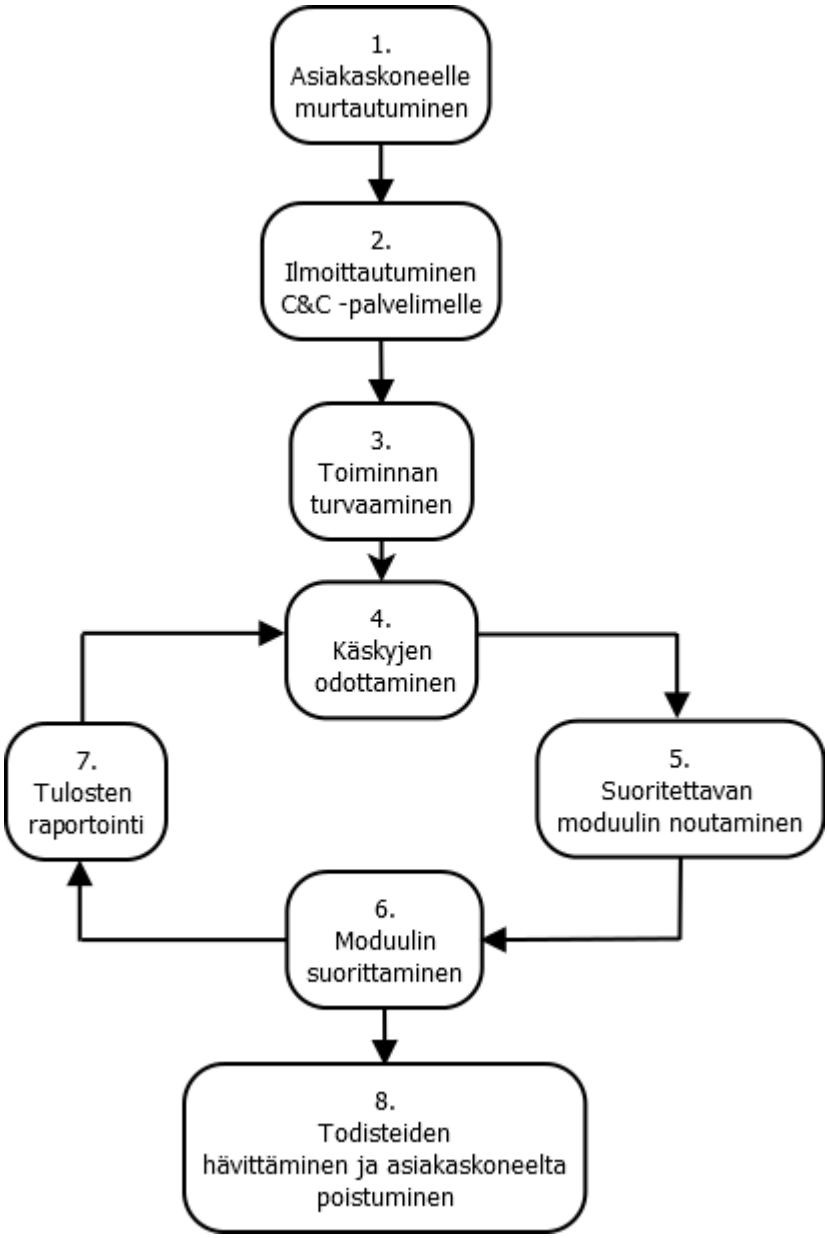
- Internet pohjainen bot-verkko, jossa asiakaskoneet ilmoittautuvat HTTP- tai HTTPS-protokollan avulla C&C-palvelimelle. HTTPS-protokollan avulla saavutetaan salattu liikenne asiakaskoneen ja palvelimen välille. Internetiin perustuvat bot-verkot ovat nykyään suosittuja, koska ne ovat yleensä suhteellisen helppo perustaa ja asiakaskoneiden hallinta web-käyttöliittymän avulla on helppoa.

- Pikaviestipalveluihin perustuvat bot-verkot. Periaate on sama kuin IRC-pohjaisissa bot-verkoissa, joissa yhteys muodostetaan tietylle palvelimelle ja tietylle kanavalle. Käytettyjä pikaviestipalveluita ovat olleet mm. Microsoftin MSN, ICQ ja America Onlinen AOL palvelu. Pikaviestipalveluihin perustuvissa bot-verkoissa vaikeutena on se, että jokaisella asiakaskoneella tulee olla oma erillinen tunnus pikaviestipalveluun liittyäkseen. Tämän ovat palveluntarjoajat ottaneet huomioon siten, että automaattinen rekisteröityminen palveluun on estetty tai tehty mahdollisimman vaikeaksi.

- Bot-verkon oma protokolla. Osalla bot-verkoilla on kehitetty täysin oma yhteysprotokolla, jonka kautta asiakaskoneet ja hallintapalvelin pitävät yhteyttä. [4.]

## 2.2 Bot-asiakaskoneen elinkaari

Bot-verkkojen kehittyminen ja synty noudattaa yleistä kehityskaarta. Kuvassa 5 esitellään tämä kehityskaari.




**Kuva 5. Bot -asiakaskoneen elinkaari. [6.]**

1. Asiakaskoneelle murtautuminen

Bot-verkon ja bot-asiakaskoneen synty alkaa asiakaskoneen hyväksikäytöllä, jolloin koneen käyttäjä saadaan suorittamaan haitallista koodia sisältävä tiedosto tai sovellus. Yleisimmin käytetyt keinot ovat hyökkäys paikkaamattomia tietoturvahaavoittuvuuksia vastaan, suora yritys murtaa käyttäjän salasana joko bruteforce tekniikalla tai salasanaa arvailemalla. Useasti tähän vaiheeseen liittyy myös sosiaalisen hakkeroinnin tekniikat, joilla käyttäjä suostutellaan haitallisen koodin suorittamiseen.

Hyökkäys paikkaamattomia tietoturvahaavoittuvuuksia vastaan voidaan suorittaa esimerkiksi lähettämällä käyttäjälle sähköpostin välityksellä liitetiedosto, joka sisältää hyväksikäyttökoodin. Liitetiedosto voi olla esimerkiksi tavalliselta pdf-dokumentilta näyttävä tiedosto, jota avatessa haittaohjelma asentuu käyttäjän koneelle. Sähköpostin lähettäjätiedot voidaan väärentää käyttäjän luottamuksen saavuttamiseksi tai mikäli botverkko on jo syntynyt, haittaohjelma voidaan välittää aiemmin murretusta asiakaskoneesta ja sähköposti näyttää tulevan kyseisen koneen käyttäjältä. Mitä luotettavammalta taholta sähköposti näyttää tulevan, sitä varmemmin käyttäjä avaa sähköpostin mukana tulleen liitetiedoston. Viime aikoina suuren suosion ovat saavuttaneet varsinkin java teknologiaan liittyvät haavoittuvuudet, joihin on myös julkaistu monia hyväksikäyttökoodeja.

Toinen yleinen tapa hyökätä tietoturva-aukkoja vastaan on välittää käyttäjälle internet osoite, jossa vieraillessaan käyttäjä saa tietokoneelleen haittaohjelman. Tämä voi tapahtua joko käyttäjän itse sivuilla suorittamana sovelluksena tai sivuston pyytämänä lisäosan asennuksena tai huomaamattomana ns. drive-by-tartuntana, jolloin tartunta tapahtuu ilman, että käyttäjän tarvitsee itse suorittaa tai asentaa mitään.

2. Asiakaskoneen ilmoittautuminen C&C-palvelimelle

Asiakaskoneelle pääsyn jälkeen bot-asiakaskone ilmoittautuu hallintapalvelimelle. Yhteys palvelimelle voi olla salattu tai vaatia erillisiä tunnistetietoja. Ensimmäisellä yhteyskerralla asiakaskone voi myös ladata palvelimelta erilaisia päivityksiä, kuten esimerkiksi muita haitta- ja vakoiluohjelmia sekä päivitettyjä hallintapalvelimen tai hallintapalvelimien tietoja.

3. Bot-ohjelmiston toiminnan turvaaminen asiakaskoneella

Yksi ensimmäisistä ja yleisistä toimenpiteistä minkä bot-ohjelmisto tekee, on virustorjunnalta piiloutuminen. Tähän on monia eri käytäntöjä, osa bot-ohjelmistoista yrittää sulkea koko virustorjuntaohjelmiston, mutta nykyiset käyttöjärjestelmät osaavat tästä varoittaa mikäli virustorjunta puuttuu tai se suljetaan. Osa haittaohjelmista voi yrittää ajaa erityistä dll-tiedostoa, joka rajoittaa virustorjuntaohjelmiston toimintaa. Tällöin virustorjunta näyttää ulospäin olevan käynnissä mutta se ei reagoi bot-ohjelmistoon liittyviin tiedostoihin. Yksi yleisistä tavoista on myös muuttaa työaseman hosts-tiedostoa

siten, että virustorjuntasovelluksen päivittäminen ei onnistu tai päivitysyritys ohjaa pyynnön hyökkääjän hallitsemaan verkkopalvelimeen.

Yhä useammin bot-ohjelmisto pyrkii piiloutumaan käyttämällä rootkit-tekniikka, joka vaikeuttaa haittaohjelman löytämistä entisestään. Rootkit-tekniikassa haittaohjelma voi sulautua ja piiloutua esimerkiksi käynnissä olevaan sovellukseen tai prosessiin, jolloin sen havaitseminen on vaikeaa. Jotkin bot-ohjelmistot myös tarkistavat asiakaskoneen ettei koneelle ole jo asentunut jokin muu haittaohjelma.

Tässä vaiheessa on myös tavallista että asiakaskoneen laitteistotiedot lähetetään C&C -palvelimelle. Näitä tietoja ovat mm. levyasemien koko, prosessori ja sen nopeus, muistin määrä, käyttäjätiedot sekä asiakaskoneen käyttämän verkkoyhteyden nopeus. Näiden tietojen avulla verkon haltija voi jaotella asiakaskoneet tarpeidensa mukaan sekä koneilla suoritettavia tehtäviä silmällä pitäen. [6.]

4., 5., 6. Käskyjen odottaminen C&C-palvelimelta, moduulien noutaminen ja niiden suorittaminen

Kun bot-ohjelmiston toiminta on saatu turvattua ja yhteys C&C-palvelimelle on käytössä asiakaskone jää odottamaan suoritettavia tehtäviä. Bot-verkoilla suoritettavia tehtäviä käsitellään tarkemmin luvussa 3.

7. Tulosten raportointi C&C-palvelimelle suorituksen jälkeen

Annettujen tehtävien suorituksen jälkeen asiakaskoneet raportoivat hallintapalvelimelle onko tehtävät suoritettu onnistuneesti sekä mahdollisesti muita määritettyjä tietoja, joiden avulla verkon haltija saa tiedon miten onnistunut tehtävä on ollut. Raportoinnin jälkeen asiakaskoneet palautuvat odottamaan seuraavia ohjeita, mikäli tehtävää suorittaessaan ne eivät ole paljastuneet ja haittaohjelmaa saatu koneelta poistettua tai konetta ei ole kytketty verkosta irti.

8. Todisteiden hävittäminen asiakaskoneelta ja koneelta poistuminen

Mikäli asiakaskone käy bot-verkolle ja verkon ylläpitäjälle tarpeettomaksi, voi asiakaskoneen poistaa bot-verkosta poistamalla koneella olevan bot- sekä muut koneelle asennetut haittaohjelmistot. Asiakaskone voi käydä tarpeettomaksi, mikäli esimerkiksi

sen resurssit eivät riitä enää toimintojen suorittamiseen tai bot-verkon ylläpitäjä huomaa että asiakaskoneella oleva haittaohjelmisto on paljastunut käyttäjälle. Ohjelmistojen ja todisteiden poistamiseen bot-verkkojen ylläpitäjillä on yleensä valmiit työkalut, joiden avulla tarvittavat toiminnot voidaan suorittaa nopeasti. Todisteiden poistaminen koneelta tarkoittaa tarvittavien lokitiedostojen poistamista esimerkiksi bot-ohjelmiston toiminta-ajalta tai pelkästään tiettyjen toimintojen poistamista lokitiedostoista. [6.]

# 3 Bot-verkkojen käyttökohteet

Bot-verkkoja voidaan käyttää sekä hyväntahtoisiin että pahantahtoisiin käyttötarkoituksiin. Sanalla bot tarkoitetaankin tässä yhteydessä yleensä sovellusta, joka suorittaa automaattisesti ja itsenäisesti erilaisia tehtäviä. Yksi esimerkki hyväntahtoisista bot-tehtävistä on hakukoneiden internet-botit, jotka indeksoivat internet-sivuja hakukoneiden toiminnan parantamiseksi ja haluttujen internet-sivujen löytämiseksi. Toinen yleinen esimerkki hyväntahtoisesta bot-verkosta on SETI@HOME-projekti, jossa käyttäjät asentavat vapaaehtoisesti tietokoneelleen botin, joka analysoi radioteleskooppidataa maapallon ulkopuolisen älykkään elämän löytämiseksi. Tässä työssä keskityn tarkemmin bot-verkkojen pahantahtoisiin käyttötarkoituksiin, joista esitellään seuraavaksi olennaisimmat. [6.]

Roskapostitus

Roskapostilla tarkoitetaan sähköpostin yhtä aikaista lähettämistä suurelle ryhmälle sähköpostin käyttäjiä. Roskapostin avulla suoritettuja yleisiä rikoksia ovat mm. erilaiset petokset, jotka voivat liittyä esimerkiksi väärennettyjen lääkkeiden myyntiin tai erilaisiin keksittyihin pyyntöihin, joihin yleensä liittyy uhrin houkuttelu pikaiseen rikastumiseen. Tällaisia ovat mm. perinteiset nigerialaiskirjeet, joissa käyttäjää pyydetään auttamaan esimerkiksi suuren rahasumman siirtämisessä. Näihin liittyy yleensä käyttäjältä vaadittava maksu erilaisiin kuluihin, mm. pankkikuluihin, todistusten hankkimiseen, virkamiehien lahjomiseen jne. Rikollisten kannalta roskapostituksen tekee houkuttelevaksi se, että postitus on halpaa, sitä on vaikea jäljittää ja sillä tavoittaa hyvin suuren määrän käyttäjiä. [7.]

Bot-verkoissa roskapostitukseen käytetään yleensä SOCKS-protokollaa. Hyökkääjä asentaa uhrikoneelle SOCKS-välityspalvelimen, jonka kautta voidaan välittää SMTP-

komentoja sähköpostipalvelimelle. Mikäli uhrikoneen ip-osoite vaihtuu säännöllisesti, esimerkiksi aina uudelleen käynnistyksen yhteydessä tai muuten DHCP-määritysten mukaan, on palveluntarjoajan vaikea estää roskapostin lähetys tällaiselta koneelta.

Toinen yleinen vaihtoehto bot-verkoissa käytettävälle roskapostitukselle on käänteinen versio edellisestä, jossa uhrikone ensin ilmoittautuu ja muodostaa C&C-palvelimelle käänteisen SOCKS-välityspalvelin yhteyden. SMTP-komennot välitetään palvelimelta uhrikoneelle tätä muodostettua tunnelia pitkin. Periaate on sama kuin suorassa yhteydessä, mutta käänteinen yhteys mahdollistaa uhrikoneiden tavoittamisen myös NAT-yhdyskäytävän takaa. NAT-yhteyden takana olevat koneet eivät muuten ole yleensä suoraan tavoitettavissa. [8.]

Taulukossa 1 esitellään Washingtonin yliopistossa suoritettua bot-verkkojen tutkimusta, jossa seurattiin verkkojen suorittamaa roskapostitusta [9.]. Kuten taulukosta käy ilmi, välitettyjen viestien määrä on valtava.

**Taulukko 1. Spam-seuranta [9, s.7].**

| Botnet | Aktiiviset päivät seurannan aikana | Spam -viestien kokonaismäärä | Spam -viestin lähetys / min | C&C - protokolla |
|---|---|---|---|---|
| Grum | 8 | 864 316 | 334 | salattu HTTP, portti 80 |
| Kraken | 25 | 5 046 803 | 331 | salattu HTTP, portti 80 |
| Pushdo | 59 | 4 932 340 | 289 | salattu HTTP, portti 80 |
| Rustock | 164 | 7 174 084 | 33 | salattu HTTP, portti 80 |
| MegaD | 113 | 198 799 848 | 1638 | salattu muokattu protokolla, portit 80 ja 443 |
| Srizbi | 51 | 86 003 889 | 1848 | salaamaton HTTP, portti 4099 |
| Storm | 50 | 961 086 | 20 | pakattu TCP |

Tietojen kalastelu

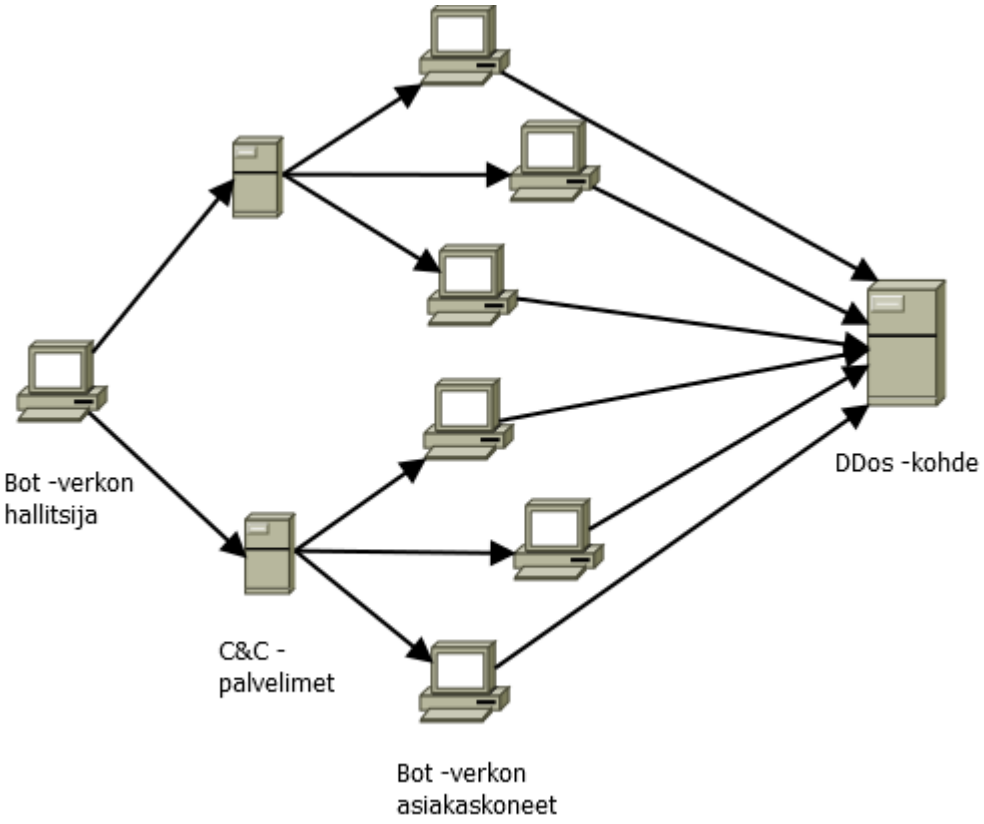
Tietojen kalastelulla pyritään hankkimaan käyttäjien henkilökohtaisia tai taloudellisia tietoja. Tietojen kalasteluun käytetään yleisimmin aidolta näyttäviä sähköposteja, joita välitetään roskapostin tavoin ja jotka ohjaavat käyttäjän hyökkääjän sivustolle. Näillä

sivustoilla pyydetään käyttäjän henkilökohtaisia tietoja, kuten esimerkiksi luottokortin tietoja sekä kirjautumistietoja eri palveluihin.

Bot-verkon hyödyt tietojen kalastelussa liittyvät useiden mahdollisten uhrien tavoittamiseen sekä hyökkääjän jälkien peittämiseen.

Palvelunestohyökkäys

Yksi ensimmäisistä bot-verkkojen käyttötavoista oli palvelunestohyökkäyksien suorittaminen. Palvelunestohyökkäyksellä tarkoitetaan verkossa olevan palvelun toiminnan estämistä niin, ettei se ole palvelun normaaleille käyttäjille saatavilla. Tämä toteutetaan yleensä niin, että palveluun kohdistetaan niin suuri määrä verkkoliikennettä että palvelu lamaantuu. Hajautetussa palvelunestohyökkäyksessä hyökkäykseen ja verkkoliikenteen muodostamiseen osallistuu useampi kuin yksi lähde tietokone. Hajautettujen palvelunestohyökkäyksien suorittaminen onkin bot-verkkojen yleisimpiä käyttötapoja, koska puolustautuminen useasta lähteestä tulevaa haitallista verkkoliikennettä vastaan on vaikeampaa kuin estää yhdestä lähteestä tuleva liikenne. Kuvassa 6 on esitetty hajautettu palvelunestohyökkäys, jossa useasta bot-verkon asiakaskoneesta muodostetaan liikennettä hyökkäyksen kohteeseen.




Kuva 6. Hajautettu palvelunestohyökkäys.

Luottamuksellisten tietojen varastaminen

Bot-verkkojen avulla suoritettava luottamuksellisten tietojen varastaminen tapahtuu yleensä joko suoraan haittaohjelmaan luodulla ohjeistuksella etsiä tietokoneelta luottamuksellisia tietoja tai haittaohjelmaan tehdyllä näppäintallennus funktiolla, joka tallentaa käyttäjän kaikki tai ennalta määritetyillä internetsivustoilla tehtävät näppäimistöpainallukset. Haittaohjelmat etsivät yleensä tietokoneelta pankkitietoja, salasanoja, luottokorttien numeroita, tietokoneen käyttäjä- ja kirjautumistietoja, sovellusten rekisteröintikoodeja sekä muita ennalta määritettyjä tietoja kuten tiettyjä tiedostomuotoja. Tällaisia voivat olla mm. excel taulukot tai pdf dokumentit, joiden hyökkääjä arvioi olevan kiinnostavia.

Yksi esimerkki tällaisesta bot-verkosta on Zeus botverkko, jonka toimintaa esitellään tarkemmin myöhemmin tässä työssä.

Haittaohjelmien asennus ja jakelu

Bot-verkkojen kautta tapahtuva haittaohjelmien asennus ja jakelu mahdollistaa uusien koneiden etsimisen ja liittämisen bot-verkkoon sekä bot-verkossa jo olevien koneiden käyttämisen eri tarkoitusperiin. Yleensä hyökkääjän tarkoituksena on mahdollisimman suuren taloudellisen hyödyn tavoittelu. Yksi esimerkki tällaisesta bot-verkosta on mainossovellukset, joista maksetaan käyttäjälle mainosten napsautusmäärien mukaan eli mitä enemmän napsautuksia, sitä enemmän käyttäjälle maksetaan. Hyökkääjä voi asentaa bot-verkkojen koneille mainossovelluksen, joka automaattisesti hoitaa mainosten napsautukset ja tuottaa hyökkääjälle taloudellista hyötyä.

Haittaohjelmien asennukseen voivat liittyä myös erilaiset lunnasvaatimussovellukset, esimerkiksi bot-verkkoon kuuluville asiakaskoneille asennetaan sovellus, joka lukitsee ja salaa käyttäjän tiedot. Erillistä maksua vastaan käyttäjä saa purkuavaimen, jolla tiedostot saa takaisin käyttöön.

# 4 Zeus toolkit

Zeus haittaohjelma havaittiin ensimmäisen kerran vuonna 2006, jolloin siihen viitattiin tietoturvayhtiöissä tuntemattomana haittaohjelmana nimeltä PRG [10]. Tämän jälkeen Zeus-ohjelmasta on kehitetty ja muokattu lukuisia eri versioita erilaisiin käyttötarkoituksiin. Periaatteena jokaisessa versiossa on kuitenkin ollut käyttäjien henkilökohtaisten ja luottamuksellisten tietojen kaappaaminen. Zeus on alun perin kehitetty Venäjällä ja tarkoituksena on ollut, kuten haittaohjelmissa yleensä, taloudellisen hyödyn saavuttaminen. Zeus on luokiteltu useasti maailman pahamaineisimmaksi haittaohjelmaksi, joka pyrkii varastamaan käyttäjien pankkisovellusten kirjautumis- ja maksutietoja. Heinäkuussa 2009 Zeus haittaohjelmien saastuttamia tietokoneita laskettiin olevan pelkästään Yhdysvalloissa noin 3,6 miljoonaa ja sen on arvioitu tuottaneen yli 100 miljoonan dollarin (USD) vahingot ilmestymisensä jälkeen [11].

Zeus haittaohjelman periaate on kaapata käyttäjän luottamukselliset ja henkilökohtaiset tiedot sekä käyttäjän koneella olevista tiedostoista että käyttäjän vierailemilta internet

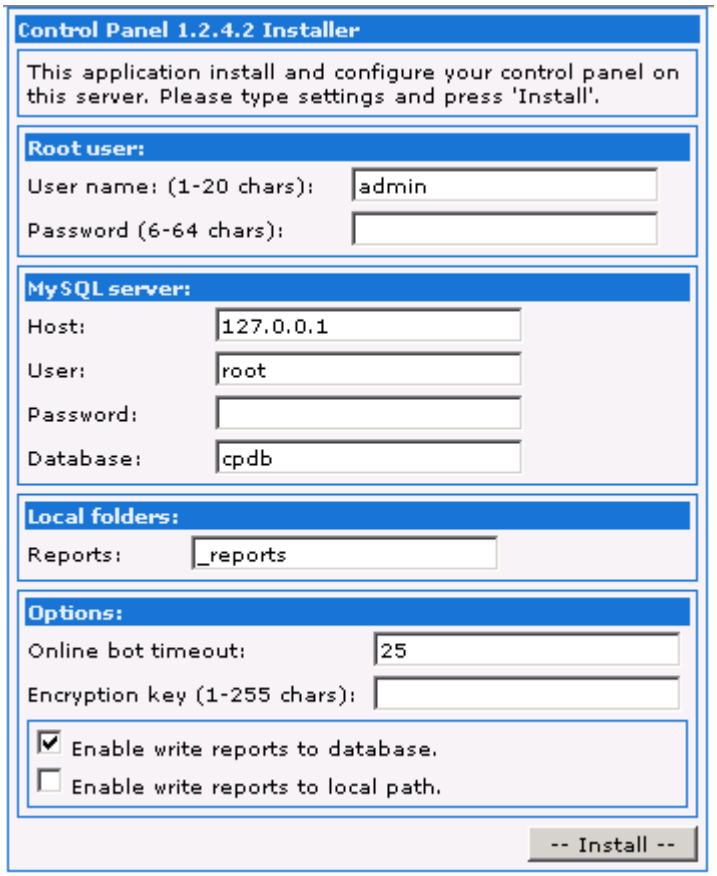
sivuilta, joihin hän syöttää tietojaan. Internetsivuilta tietojen kaappaaminen tapahtuu käyttäjän koneella jo ennen kuin tiedot lähetetään sivustolle, joten vaikka itse yhteys internetpalveluun olisi salattu, haittaohjelma saa tiedot kaapattua selkokielisenä ennen kuin tiedot salataan. Asiakaskoneilta kerättävät tiedot ovat pääasiassa käyttäjien HTML- lomakkeille syöttämiä tietoja, sähköpostin ja FTP-tilien kirjautumistietoja, erilaisten varmenteiden ja evästeiden keräämistä asiakaskoneilta. Zeus Toolkit sovelluksessa on myös ominaisuus, jolla käyttäjälle voidaan näyttää internetsivuilla ylimääräisiä, bot-verkon ylläpitäjän määrittämiä kenttiä, joissa voidaan pyytää käyttäjältä esim. luottokortin tietoja, henkilötunnusta tai pankki- tai luottokortin pin-koodia. Kaapatut tiedot lähetetään bot-verkon ylläpitäjän määrittelemälle hallintapalvelimelle, jossa tiedot tallennetaan MySQL-tietokantaan. Tietokannan hallintaan tulee Zeus Toolkit sovelluksen mukana internetselaimella käytettävä helppokäyttöinen hallintapaneeli, jonka kautta bot-verkon koneita ja niiden tietoja voidaan tarkastella.

Zeus bot-verkko voidaan rakentaa julkisesti saatavilla olevalla Zeus Toolkit-sovelluksella, joka mahdollistaa oman yksilöidyn bot-verkon rakentamisen. Tämä tarkoittaa myös sitä, ettei ole olemassa yhtä laajaa Zeus-bot-verkkoa vaan jokainen voi rakentaa oman ja omilla yksilöidyillä asetuksilla olevan bot-verkon. Zeus Toolkit sovelluksen käyttö esitellään myöhemmin tässä työssä. Zeus Toolkit-sovelluksesta on saatavilla sekä maksullinen että maksuton versio. Maksullinen versio sisältää viimeisimmät funktiot sekä kattavan dokumentoinnin sovelluksen käyttöön. Maksullisen version hinta on tyypillisesti ollut noin 700 dollaria (USD) [12]. Sovelluksen lähdekoodi vuoti julkisuuteen vuoden 2011 maaliskuussa, jonka jälkeen erilaisten Zeus-haittaohjelma muunnosten määrä kasvoi nopeasti.

## 4.1 Asennus

Zeus Toolkitin käyttö vaatii internetpalvelimen sekä MySQL-tietokantapalvelimen. Internet-palvelimessa tulee myös olla tuki PHP-ohjelmointikielelle, koska bot-verkon ohjauspaneeli on ohjelmoitu PHP-kieltä käyttäen ja bot-asiakaskoneiden ohjaus suoritetaan PHP-skriptien avulla. Tässä työssä edellä mainittuja palvelimia ajetaan Kali Linux -jakelun päällä ja palvelinten asennus on suoritettu XAMPP-paketin avulla joka sisältää kaikki tarvittavat sovellukset ja lisäosat.

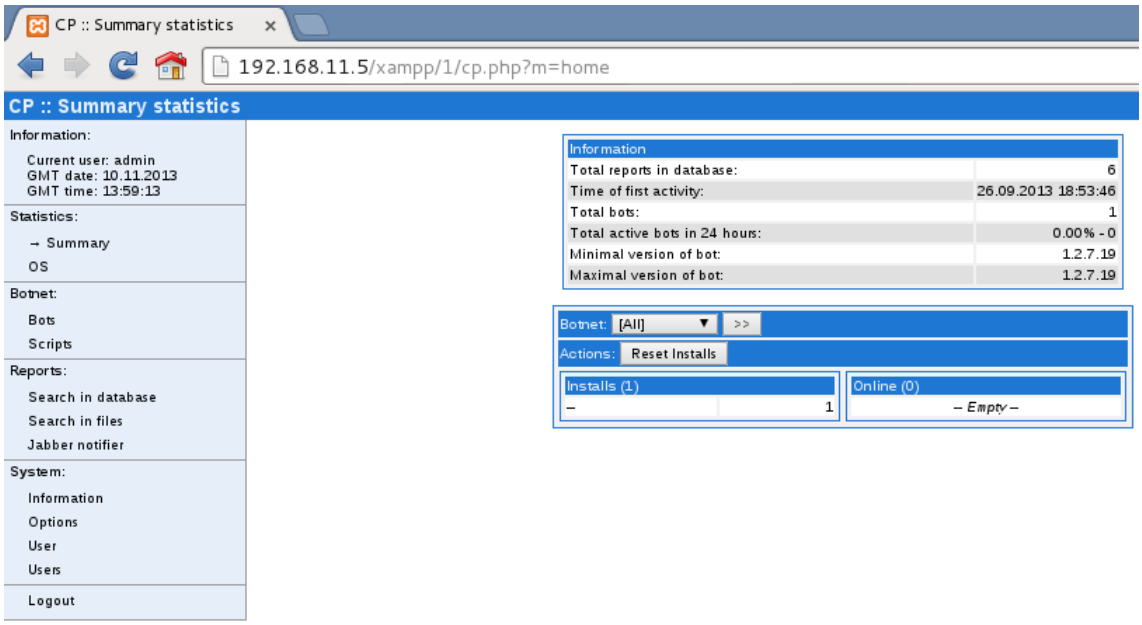
Palvelinten asennuksen jälkeen itse Zeus Toolkitin asennus on suoraviivainen toimenpide. Asennus suoritetaan Zeus Toolkitin mukana tulevalla PHP-skriptillä, joka löytyy /install/index.php polusta. Asennuksen aikana käyttäjältä kysytään käyttäjätunnus sekä salasana itse Zeus Toolkit sovellukseen sekä MySQL-tietokantapalvelimeen tarvittavat tietokanta- ja käyttäjätiedot. Samalla määritetään myös bot-verkon salausavain, jota käytetään tietojen salaamiseen C&C-palvelimen ja bot-verkon asiakaskoneiden välillä. Kuvassa 7 on esitetty valikko, joka avautuu asennuksen tietoja määritettäessä ja - Install -- -painiketta painettaessa asennus käynnistyy.




Kuva 7. Zeus asennus [12].

## 4.2 Bot-verkon ylläpito ohjauspaneelin avulla

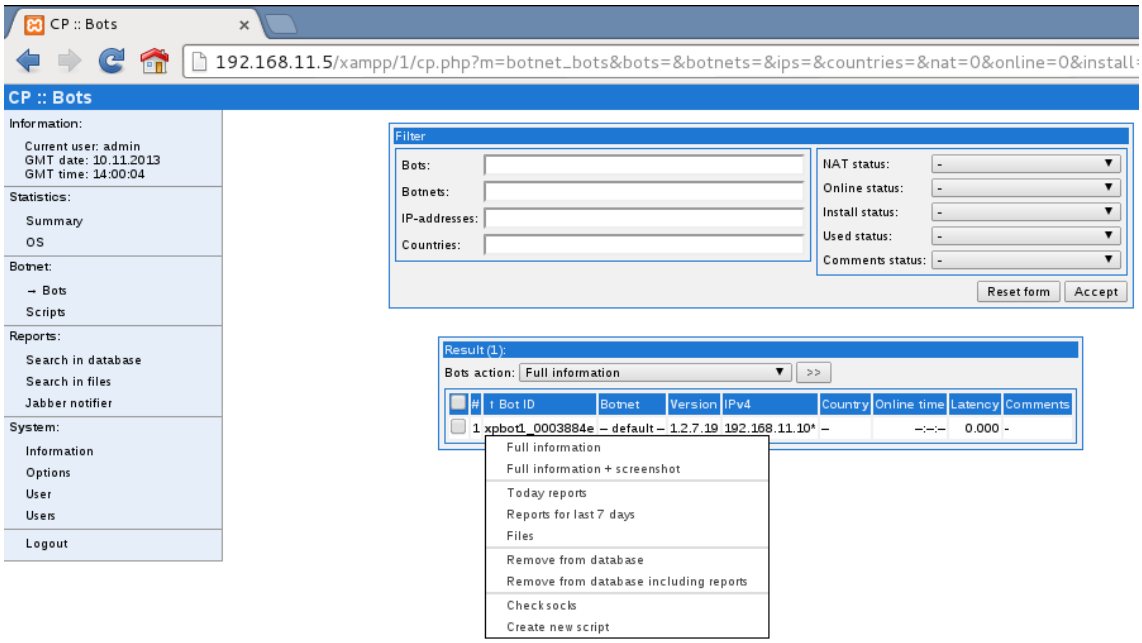
Asennuksen jälkeen ja ohjauspaneelin kirjautumisen jälkeen avautuu kuvassa 8 näkyvä sivu.




**Kuva 8. Ohjauspaneelin etusivu.**

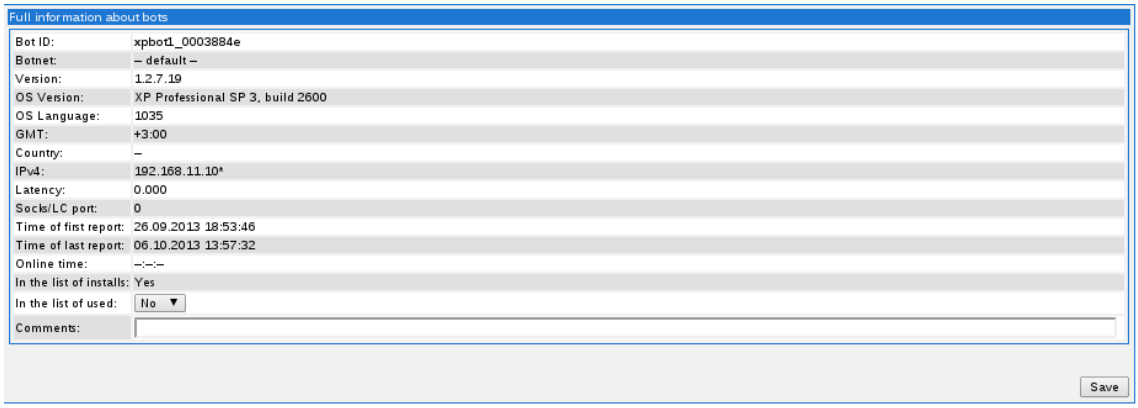
Etusivulta löytyy vasemmasta reunasta valikko, josta pääsee bot-verkon tarkempiin tietoihin sekä oikealla yhteenveto bot-verkosta. Yhteenvedosta näkee mm. tietokannassa olevien raporttien määrän sekä bot-verkkoon kuuluvien asiakaskoneiden lukumäärän. Yhden hallintapalvelimen avulla voi hallita myös useampia bot-verkkoja.

Bot-verkkoon kuuluvia asiakaskoneita ja niistä tulleita tietoja ja raportteja pääsee katsomaan valitsemalla Bots-linkin vasemman reunan valikosta. Kuvassa 9 on esitetty Bots-linkistä avautuva sivu. Bot-verkkoon kuuluvia asiakaskoneita voi luokitella sivulla olevan Filter-valikon avulla. Luokittelun voi tehdä mm. siten kuuluuko asiakaskone NAT-palvelun sisä- vai ulkopuolelle, onko asiakaskone online vai offline tilassa. Kuvassa näkyy bot -verkkoon kuuluva yksi asiakaskone, josta saa avattua useita monipuolisia raportteja.



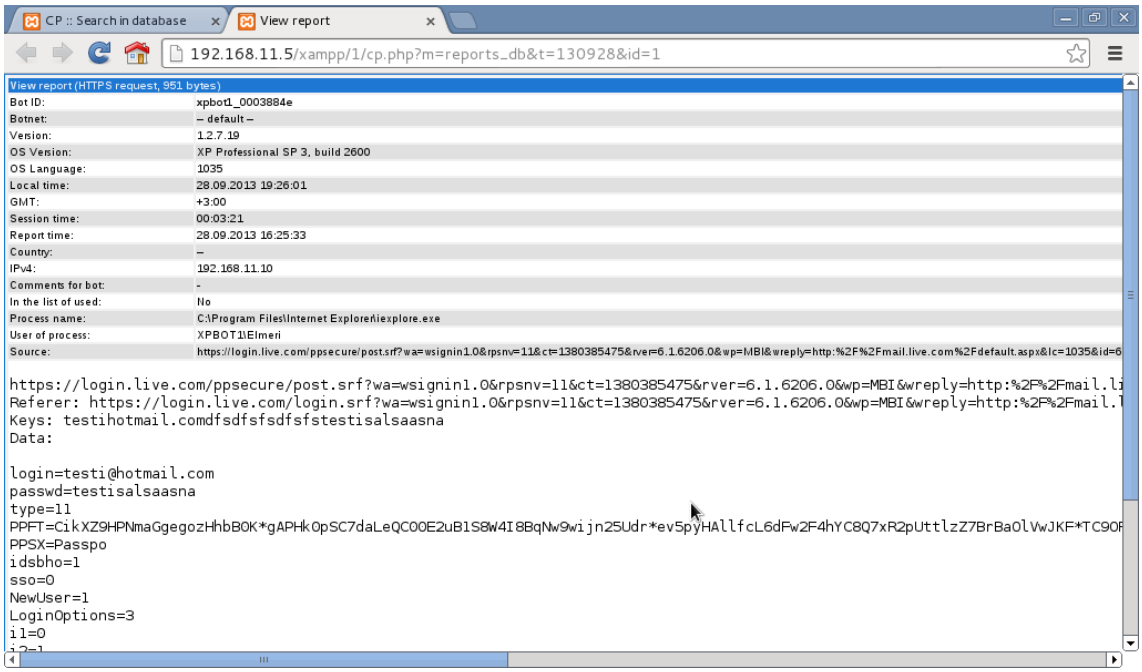

**Kuva 9. Bot-verkkoon kuuluvat asiakaskoneet.**

Kuvassa 10 näkyy Full information valinta bot-asiakaskoneesta. Tiedot sisältävät mm. bot-verkon asiakaskonekohtaisen BotID-tunnuksen, sen mihin bot-verkkoon kyseinen asiakaskone kuuluu, asiakaskoneen käyttöjärjestelmäversion, ip-osoitteen sekä ensimmäisen että viimeisimmän raportoinnin ajankohdan.




**Kuva 10. Bot-asiakaskoneen tiedot.**

Kuvassa 11 näkyy asiakaskoneelta tullut raportti, jossa on kirjauduttu Microsoftin Live-palveluun salatun HTTPS-yhteyden yli. Kuten kuva osoittaa, asiakaskoneelta on välittynyt hallintapalvelimelle login eli käyttäjätunnus sekä passwd eli salasana selkokielisenä.




**Kuva 11. Asiakaskoneen raportti.**

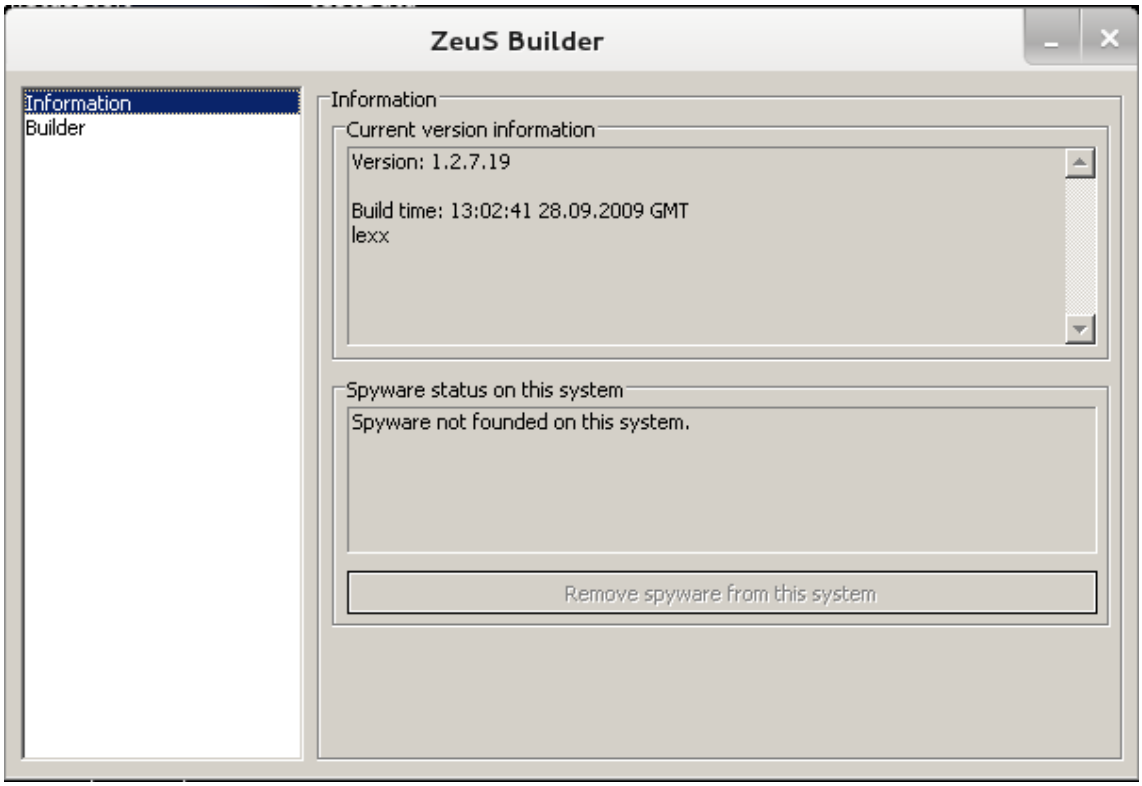
Ohjauspaneelista löytyy myös Scripts-linkki, josta löytyy valmiita komentoja joita voidaan jakaa bot-verkon asiakaskoneille. Komentojen avulla voidaan mm. kerätä lisätietoja asiakaskoneilta sekä tehdä muutoksia bot-verkkoon. Taulukossa 2 on esitetty käytettävissä olevat komennot. Asiakaskoneen ottaessa yhteyttä hallintapalvelimelle asetustiedoston määrittämän aikavälin mukaan hallintapalvelin tarkistaa onko kyseiselle asiakaskoneelle määritetty lähetettäviä komentoja. Mikäli kyseiselle asiakaskoneelle löytyy lähetettäviä komentoja, palvelin välittää asiakaskoneelle komennon tai komennot suoritettavaksi.

**Taulukko 2. Käytettävät komennot. [15]**

| Komennot | |
|---|---|
| reboot | Käynnistää tietokoneen uudelleen |
| kos | Poistaa järjestelmätiedostot ja tuhoaa käyttöjärjestelmän |
| shutdown | Sammuttaa tietokoneen |
| bc_add [palvelu] [ip] [portti] | Lisää takaisinkytkentä [palvelu] palvelimeen [ip]:[portti] |
| bc_del [palvelu] [ip] [portti] | Poistaa takaisinkytkentä [palvelu] joka käyttää [ip]:[portti] |
| block_url [url] | Estää pääsyn [url] |
| unblock_url [url] | Sallii pääsyn [url] |
| block_fake [url] | Ei lisää ylimääräistä HTML -sisältöä [url] -osoitteeseen |
| unblock_fake [url] | Sallii ylimääräisen HTML -sisällön lisäämisen [url] -osoitteeseen |
| rexec [url] [args] | Lataa ja suorita tiedosto |
| rexeci [url] [args] | Lataa ja suorita tiedosto käyttäjän avustamana |
| lexec [url] [args] | Suorita paikallinen tiedosto |
| lexeci [url] [args] | Suorita paikallinen tiedosto käyttäjän avustamana |
| addsf [file_mask...] | Lisää tiedostomaskin paikalliseen tiedostohakuun |
| delsf [file_mask...] | Poistaa tiedostomaskin paikallisesta hausta |
| getfile [path] | Lataa tiedosto tai kansio |
| getcerts | Varastaa tietokoneelta asennetut sertifikaatit |
| resetgrab | Varastaa PSTORE (Protected Storage) -tiedot ja evästeet |
| upcfg [url] | Päivittää asetustiedoston |
| rename_bot [name] | Uudelleen nimeää bot -koneen |
| getmff | Lataa Flash -evästeet |
| delmff | Poistaa Flash -evästeet |
| sethomepage [url] | Vaihtaa Internet Explorerin aloitussivun |

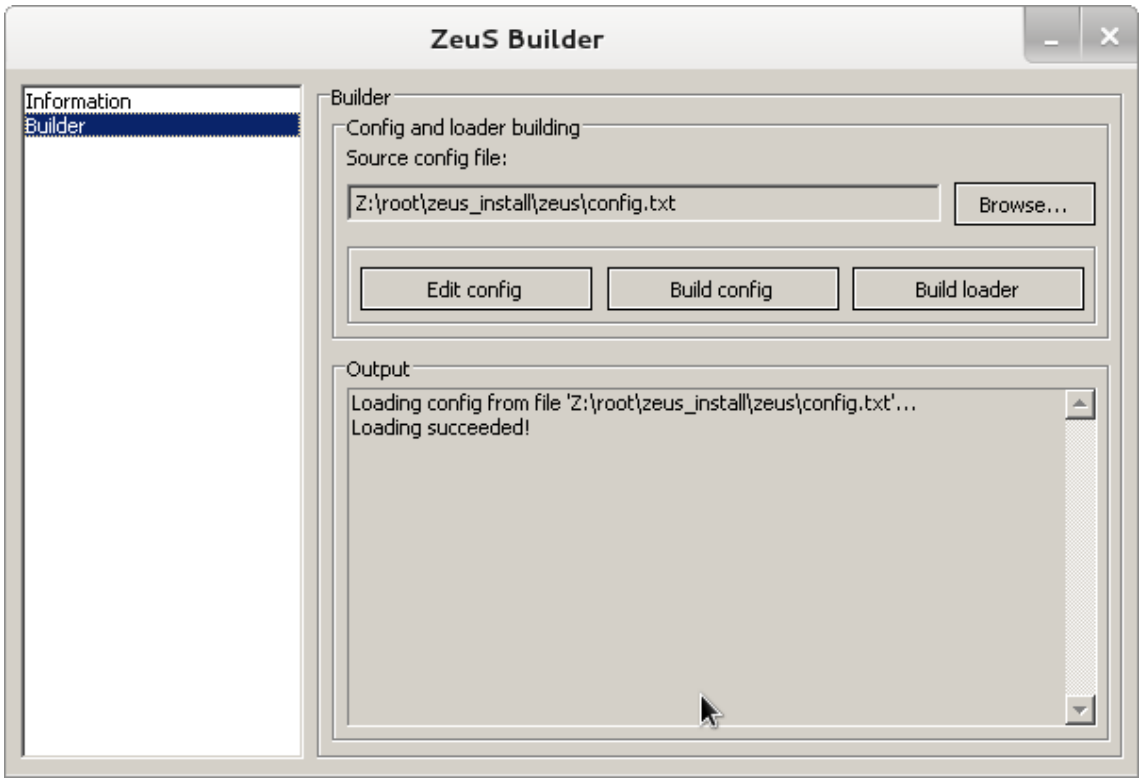
## 4.3 Asiakaskoneille jaettavan haittaohjelman rakentaminen

Asiakaskoneille suoritettavaksi jaettavan haittaohjelman rakentaminen tapahtuu Zeus Toolkit -paketin mukana tulevalla Zeus Builder -sovelluksella. Sovellus käyttää haittaohjelman rakentamisessa apuna bot-verkon ylläpitäjän määrittämiä konfiguraatiotiedostoja, joissa voidaan määritellä bot-verkon yksilöllisiä asetuksia. Yksi mielenkiintoinen yksityiskohta Zeus Builder sovellusta avattaessa on se, että se tarkistaa sitä ajettavassa tietokoneessa eli bot-verkon ylläpitäjän tietokoneessa, ettei siinä ole Zeus-haittaohjelmaa ajettuna. Kuvassa 12 on esitetty Zeus Builder sovelluksen avausikkuna, jossa näkyy, ettei koneessa ole haittaohjelmaa asennettuna.




Kuva 12. ZeuS Builder.

Zeus Builder lataa asetustiedoston config.txt-tiedostosta. Kuvassa 13 asetustiedosto on onnistuneesti ladattu. Asetustiedostoa pääsee muokkaamaan joko tekstieditorin kautta tai Zeus Builder -ikkunassa Edit config -painikkeella.




**Kuva 13. Asetustiedoston lataaminen.**

Seuraavalla sivulla esitettävä esimerkkikoodi 1 on config.txt-tiedoston esimerkki. Tiedosto sisältää sekä staattiset asetukset ”StaticConfig” että dynaamiset asetukset ”DynamicConfig”. Staattisiin asetuksiin kuuluu mm. bot asiakaskoneen ja hallintapalvelimen välisen yhteyden salauksen määrittävä salausavain, kuvassa ”encryption_key”, jonka bot-verkon ylläpitäjä määrittää. Dynaamisin asetuksiin kuuluvat mm. webinjects.txt-tiedoston lataaminen, jossa määritetään minkä sivujen kirjautumistietoja seurataan ja sivuille voidaan haluttaessa lisätä käyttäjältä ylimääräisenä pyydettäviä tietoja, kuten esimerkiksi verkkopankkien sivuilla pyydettäviä maksukorttien pin-koodeja tai muita henkilökohtaisia tietoja. Staattiset asetukset koodataan asiakaskoneille suoritettavaksi lähetettävään haittaohjelmaan, dynaamiset asetukset ovat tarvittaessa bot-verkon ylläpitäjän toimesta muutettavia asetuksia, jotka bot-verkon asiakaskoneet lataavat tietyin aikavälein.

Konfiguraatiotiedostossa määritellään kolme eri ajastinta, joiden mukaan asiakaskoneet suorittavat tehtäviä:

1. Uuden dynaamisen konfiguraatiotiedoston hakeminen hallintapalvelimelta, kuvassa timer_config (oletus 60 minuuttia).
2. Asiakaskoneelta kerätyn ja tallennettujen tietojen lähettäminen hallintapalvelimelle, kuvassa timer_logs (oletus 1 minuutti).
3. Tilastojen lähettäminen asiakaskoneelta hallintapalvelimelle, kuvassa timer_stats (oletus 20 minuuttia).

```
;Build time:    09:48:52 16.01.2010 GMT
;Version:       1.2.7.19

entry "StaticConfig"
  ;botnet "btn4"
  timer_config 10 1
  timer_logs 1 1
  timer_stats 5 1
  url_config "http://192.168.11.5/xampp/1/cfg.bin"
  url_compip "http://192.168.11.5/xampp/1/ip.php" 4096
  encryption_key "asd5asd5asd5asd5asda5sd5asd5asdas5dasd5"
  ;blacklist_languages 1049
end

entry "DynamicConfig"
  url_loader "http://192.168.11.5/xampp/1/bt.exe"
  url_server "http://192.168.11.5/xampp/1/gate.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs"
    ;"http://192.168.11.5/xampp/1/cfg1.bin"
  end
```

Esimerkkikoodi 1. Config.txt tiedoston esimerkki.

Internetsivuille tehtävien muutosten määritys tapahtuu webinjects.txt-tiedostossa. Käyttäjän vieraillessa tiedostossa määritellyllä sivuilla, selain lataa sivun normaalisti palveluntarjoajan palvelimelta mutta sivuille lisätään huomaamatta käyttäjän koneella botverkon ylläpitäjän määrittelemiä tietoja, esim. ylimääräisiä lomakekenttiä. Esimerkkikoodi 2 esittää webinjects.txt-tiedostoon määritettyä koodia, joka näyttää Wellsfargo.com-sivuilla vieraillessa käyttäjälle ylimääräisen ATM PIN-kentän.

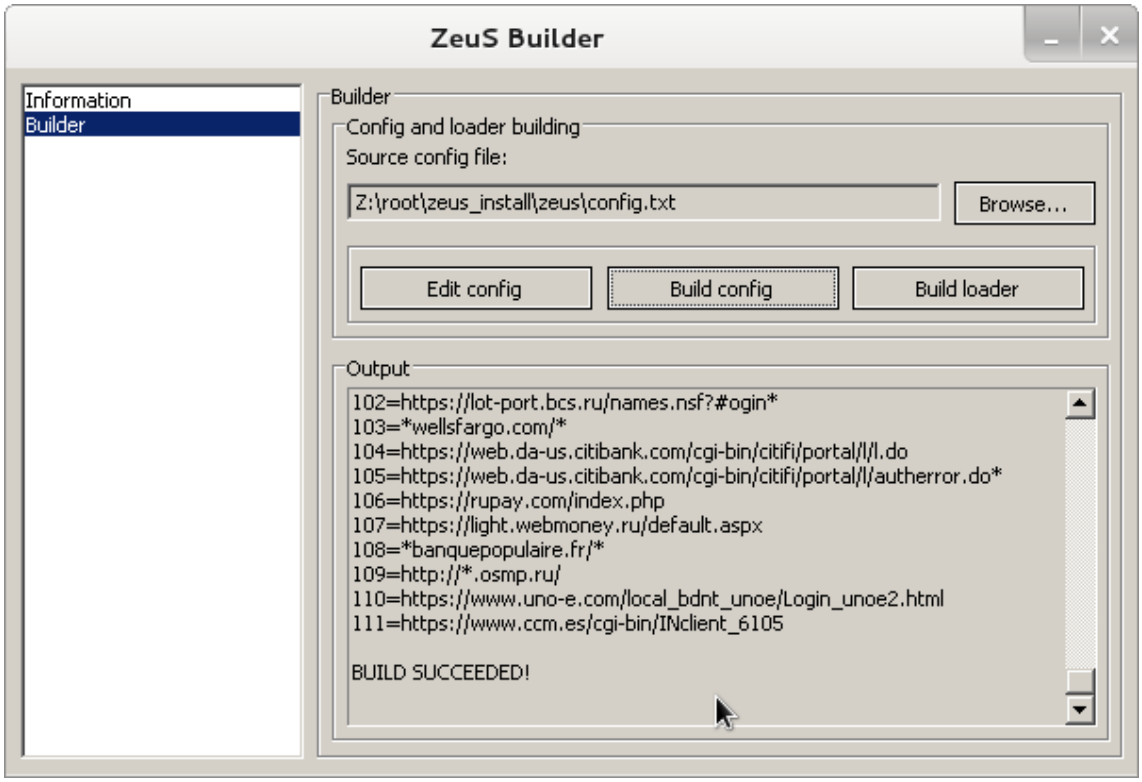
Webinjects.txt-tiedostossa määritellään set_url parametrilla seurattava sivusto, jolle ylimääräistä sisältöä lisätään. Parametri data_before määrittää, mitä kohtaa sivuston lähdekoodista etsitään ja minkä kohdan jälkeen ylimääräinen sisältö lisätään ja parametrin data_inject jälkeen määritetään, mitä sisältöä käyttäjän näkemälle sivustolle lisätään. [13.]

```
set_url https://www.wellsfargo.com/* G
data_before
<span class="mozcloak"><input type="password"*</span>
data_end
data_inject
<br><strong><label for="atmpin">ATM PIN</label>:</strong>
 <br /><span class="mozcloak"><input type="password"
accesskey="A" id="atmpin" name="USpass" size="13" maxlength="14"
style="width:147px" tabindex="2"
/></span>
data_end
data_after
data_end
```

**Esimerkkikoodi 2. Wellsfargo.com-sivuille lisättävä ATM PIN-kenttä.**

Webinjects.txt tiedostossa tulee oletuksena yli sata URL -osoitetta, joilla vieraillessa käyttäjälle esitetään ylimääräisiä tietoja pyytäviä kenttiä.

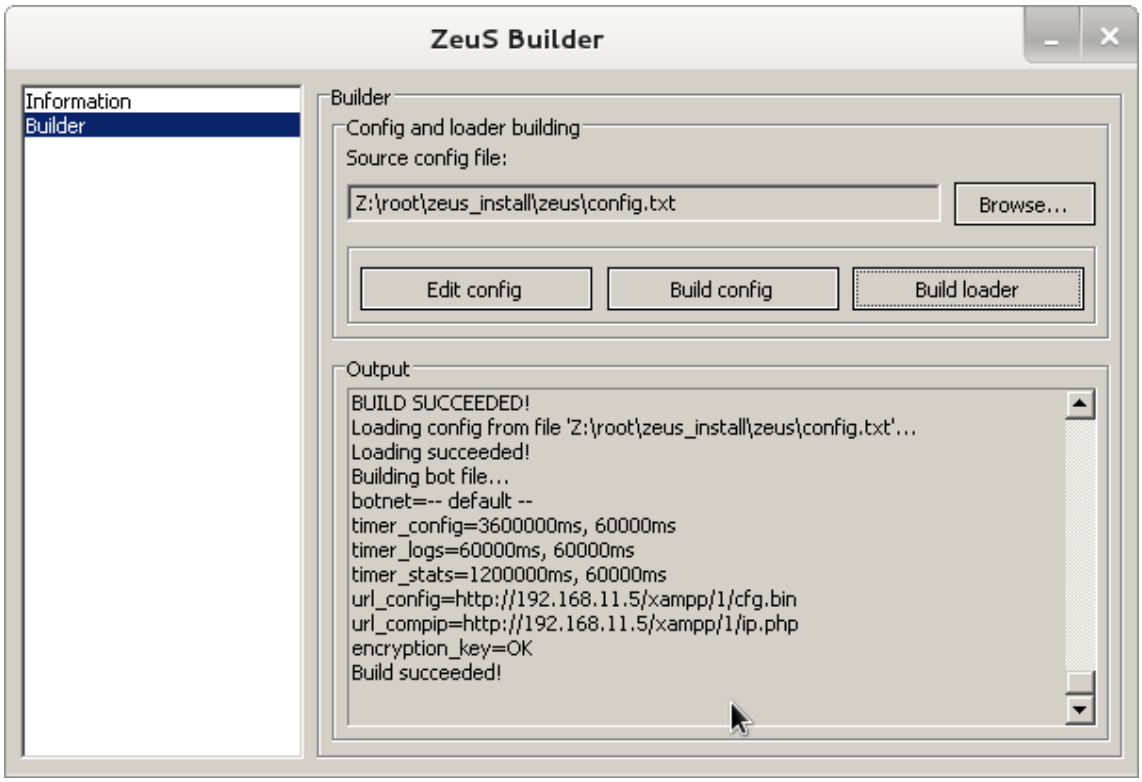
Asetustiedoston määrittämisen jälkeen asetustiedoston rakennus tapahtuu painamalla Build config-painiketta, joka tarkistaa asetustiedoston oikeellisuuden ja ilmoittaa tarvittaessa virheistä. Kuvassa 14 on esitetty asetustiedoston onnistunut valmistuminen. Tässä vaiheessa selkokielinen asetustiedosto muunnetaan haittaohjelman määritettyyn muotoon sekä salataan käyttämällä asetustiedostossa määritettyä salausavainta. Salausalgoritmina käytetään RC4-salausta.




Kuva 14. Asetustiedoston rakentaminen.

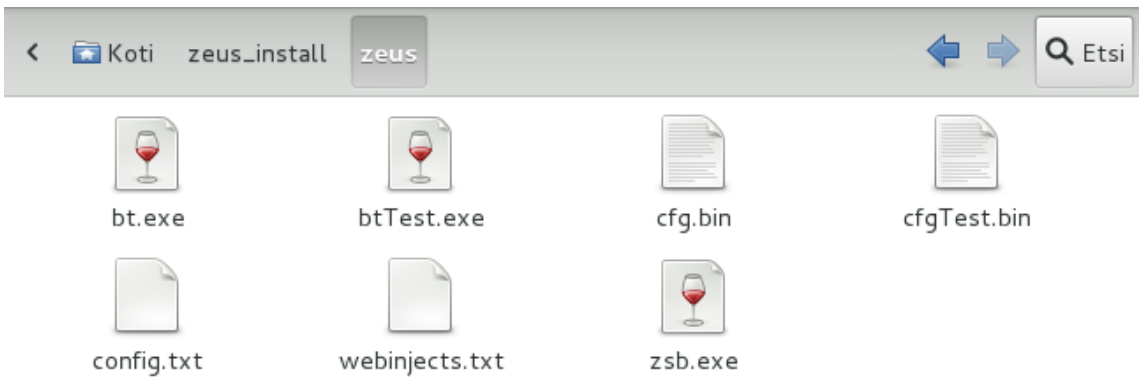
Mikäli bot-verkon ylläpitäjä haluaa muuttaa tai päivittää bot-verkon asiakaskoneilla jo olevaa asetustiedostoa, määrittää esimerkiksi uusia seurattavia ja muokattavia internet-sivuja, ylläpitäjän tulee rakentaa asetustiedosto uudelleen ja asettaa tiedosto palvelimelle saataville. Asiakaskoneet käyvät bot-verkon ylläpitäjän määrittämin aikavälein hakemassa hallintapalvelimelta uusimman version asetustiedostosta ja ottavat uusimmat muutokset käyttöön.

Asiakaskoneelle välitettävän haittaohjelman rakennus tapahtuu Build Loader-painikkeesta, jolloin tarkistetaan vielä edellisessä vaiheessa salatun asetustiedoston oikeellisuus ja ilmoitetaan tarvittaessa virheistä. Kuvassa 15 onnistuneen haittaohjelman rakennuksen jälkeinen ilmoitus.




Kuva 15. Haittaohjelma rakennettu onnistuneesti.

Zeus Builder tuottaa asiakaskoneelle suoritettavaksi jaettavan exe tiedoston, joka liittää asiakaskoneen bot-verkon jäseneksi sen suorittamisen jälkeen. Kuvassa 16 bt.exe ja btTest.exe ovat valmiina jaettavaksi asiakaskoneille.




Kuva 16. Valmiit haittaohjelmat.

## 4.4 Muutokset asiakaskoneessa haittaohjelman suorituksen jälkeen

Haittaohjelman suorituksen jälkeen asiakaskoneelta poistetaan käytöstä Windowsin oma palomuuri, mikä onkin ainoa käyttäjän selkeästi huomattavissa oleva tapahtuma. Muut käyttäjälle näkymättömät haittaohjelman suorittamat toimet ovat seuraavat:

1. Ensimmäiseksi haittaohjelma etsii asiakaskoneesta siellä mahdollisesti jo olevaa Zeus tartuntaa hakemalla sdra64.exe-nimistä tiedostoa. Mikäli uusi haittaohjelma löytää asiakaskoneesta kyseisen tiedoston, se poistaa sen. Sama tapahtuu myös, mikäli haittaohjelmaa päivitetään eli uusi versio poistaa asiakaskoneesta vanhan version.

2. Haittaohjelma tekee itsestään kopion ja tallentaa kopion C:/Windows/System32/sdra64.exe-polkuun. Samalla haittaohjelma luo satunnaisia tavuja tiedoston perään estääkseen virustorjuntaa havaitsemasta haittaohjelmaa. Haittaohjelma liittää myös polun C:/Windows/System32/sdra64.exe rekisteriavaimeen HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/Winlogon/Userinit, jolloin haittaohjelma suoritetaan myös aina Windowsin käynnistyessä.

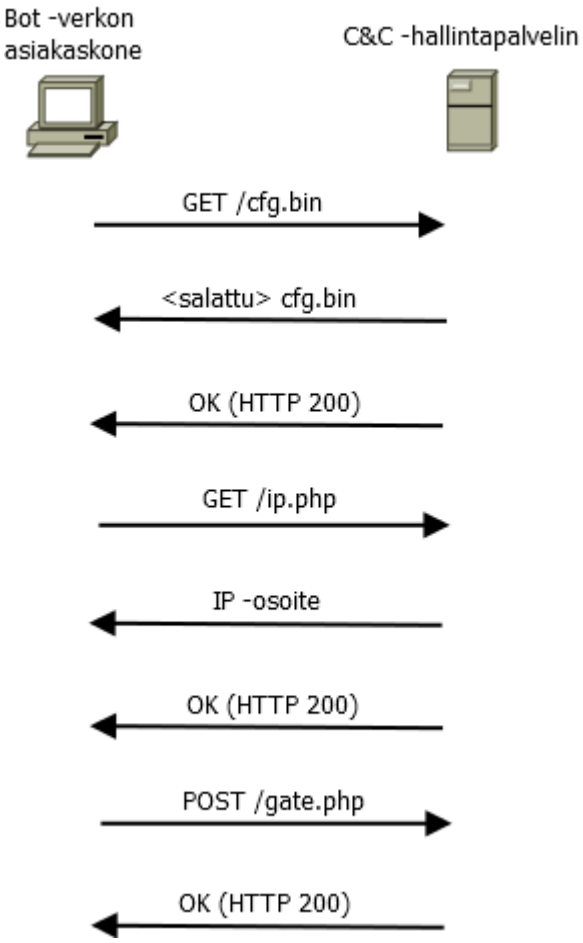
3. Haittaohjelma etsii winlogon.exe-prosessin, johon se tartuttaa oman koodinsa ja luo uuden säikeen, jossa tämä koodi suoritetaan. Lisäksi haittakoodi winlogon-prosessissa lisää haitallista koodia myös svchost.exe-prosessiin. Haittakoodi svchost.exe-prosessissa vastaa verkkoyhteyksistä sekä verkkosivujen sisältöjen muokkaamisesta.

4. Piiloutuakseen paremmin haittaohjelma kopioi Ntdll.dll-tiedoston muokattu-, pääsy- ja luomisajat haittaohjelmaan vastaaviksi tiedoiksi. Tarkoitus on, että haittaohjelma näyttää olleen järjestelmässä jo Windowsin asennuksesta asti. Lisäksi haittaohjelma muokkaa tiedoston sdra64.exe attribuutteja siten, että tiedosto on piilotettu eikä näy normaalissa tiedostolistauksessa. Tiedoston näkeminen vaatii kansioasetusten muuttamisen siten, että piilotetut tiedostot näytetään.

5. Haittaohjelma luo piilotetun C:/Windows/System32/lowsec-kansion, johon se luo local.ds- ja user.ds-tiedostot. Tiedostoista local.ds-tiedosto sisältää viimeisimmän dynaamisen konfiguraatiotiedoston mikä on hallintapalvelimelta ladattu. User.ds-tiedosto sisältää asiakaskoneelta tallennetut tiedot, jotka odottavat toimitusta hallintapalvelimelle seuraavan yhteyden aikana. [14.]

## 4.5 Asiakaskoneen ja hallintapalvelimen välinen kommunikointi

Asiakaskoneen ja bot-verkon hallintapalvelimen välinen kommunikaatio noudattaa kuvassa 17 esitettyjä periaatteita asiakaskoneen saatua haittaohjelma tartunnan. Kommunikaatio koneiden välillä tapahtuu toistuvasti tietyin aikavälein, jotka bot-verkon ylläpitäjä määrittää konfiguraatiotiedostossa.




**Kuva 17. Asiakaskoneen ja hallintapalvelimen välinen kommunikointi. [14]**

1. Haittaohjelman suorituksen jälkeen asiakaskone pyytää hallintapalvelimelta uusimman bot-verkon konfiguraatiotiedoston. Asiakaskone lähettää GET /cfg.bin-pyynnön.

2. Hallintapalvelin vastaa lähettämällä uusimman salatun version cfg.bin-tiedostosta.

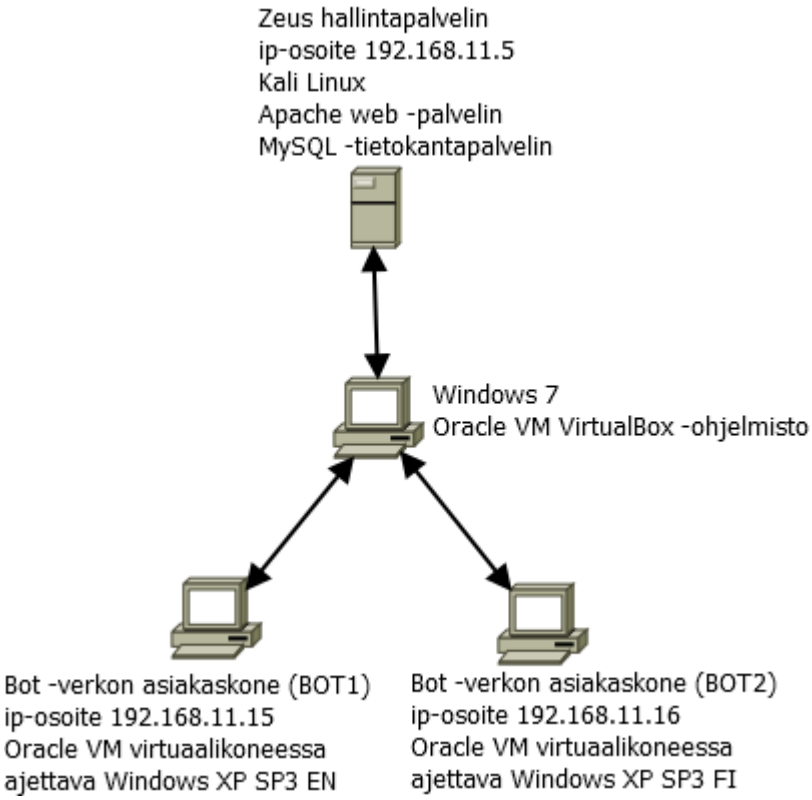
3. Asiakaskone vastaanottaa salatun konfiguraatiotiedoston ja purkaa salauksen käyttäen haittaohjelman mukana jaettua salausavainta.

4. Mikäli bot-verkon ylläpitäjä haluaa liittää asiakaskoneen bot-verkon hallintakoneeksi, tulee asiakaskoneen ilmoittaa hallintapalvelimelle sen ulkoinen ip-osoite sekä mahdollinen NAT (Network Address Translation) -palvelun käyttäminen. Asiakaskoneen ulkoisen ip-osoitteen selvittäminen tapahtuu asiakaskoneelta ottamalla yhteys määritettyyn bot-verkon palvelimeen joka taas ilmoittaa ip-osoitteen takaisin asiakaskoneelle. Palvelinten osoitteet määritellään konfiguraatiotiedoston staattisessa osassa.

5. Asiakaskone raportoi kaappaamansa tiedot sekä omat tilatiedot hallintapalvelimelle lähettämällä POST /gate.php-pyynnön, jotka hallintapalvelin kuittaa saaduksi asiakaskoneelle.

# 5 Zeus toolkit käytännössä

Käytännön testauksen Zeus Toolkit -sovelluksella suoritin kuvassa 18 näkyvässä ympäristössä. Jokaiselle testausympäristön työasemalle oli lisäksi asennettu Wireshark-ohjelmisto, jolla voi kaapata ja analysoida työaseman verkkoliikennettä. Testausympäristön Windows 7-työasema vastaa Oraclen VirtualBox-sovelluksen suorittamisesta. VirtualBox-sovelluksen avulla ajetaan bot-verkon asiakaskoneita omissa virtuaalikoneissaan. Zeus-hallintapalvelinta ajetaan Linux-käyttöjärjestelmässä, jossa on asennettuna Kali Linux jakelu.

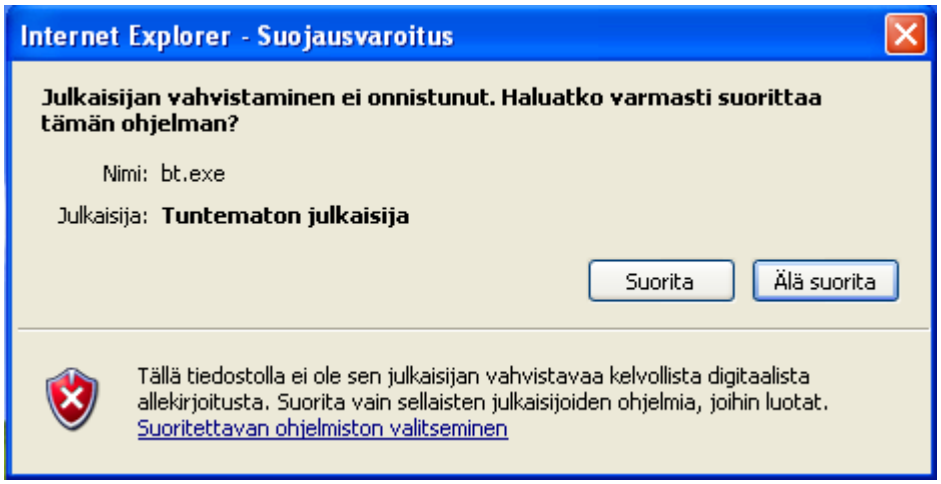



**Kuva 18. Testausympäristö.**

## 5.1 Asiakaskoneen tartuttaminen

Yleisimmät tavat haittaohjelman jakamiseksi käyttäjille ovat haittaohjelman suora lähettäminen esimerkiksi sähköpostin liitetiedostona, suoran haittaohjelmaan viittaavan internet-osoitteen sisältävän linkin lähettäminen käyttäjälle, jossa pyydetään lataamaan ja suorittamaan kyseinen sovellus tai asiakaskoneen tartuttaminen ns. drive-by tartuntana, jolloin haittaohjelma ladataan käyttäjän vieraillessa haittaohjelman sisältävällä sivulla.

bt.exe haittaohjelma on tässä esimerkissä ladattu hallintapalvelimen web-palvelimelta ja suoritettu suoraan selaimessa. Selain antaa varoituksen suoritettavasta sovelluksesta (kuvassa 19), kuten muistakin vastaavista ilman julkaisijatietoa avattavista sovelluksista.

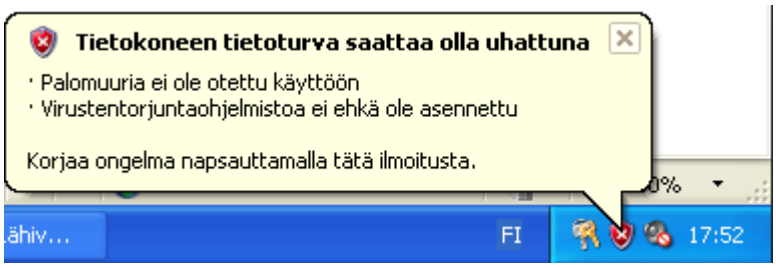



Kuva 19. Selaimen varoitus haittaohjelmaa suoritettaessa.

## 5.2 Asiakaskoneen ja hallintapalvelimen välinen kommunikointi

Käyttäjän valitessa ohjelman suoritettavaksi, haittaohjelma toteuttaa seuraavat toimenpiteet:

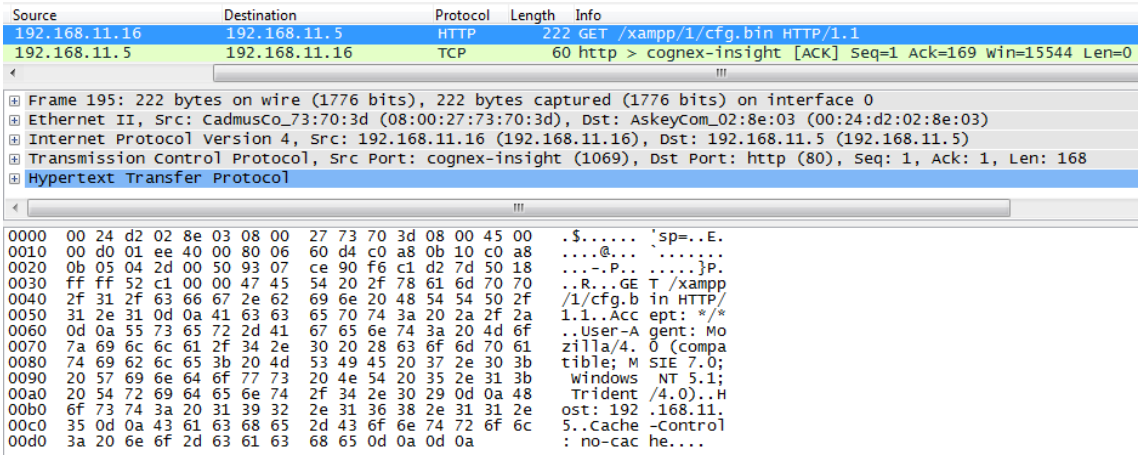
1. Välittömästi suorituksen jälkeen haittaohjelma sulkee Windowsin palomuurin, josta käyttöjärjestelmä antaa kuvassa 20 näkyvän varoituksen. Muita näkyviä merkkejä haittaohjelmatartunnasta käyttäjälle ei tule.




Kuva 20. Windows palomuuri poistettu käytöstä.

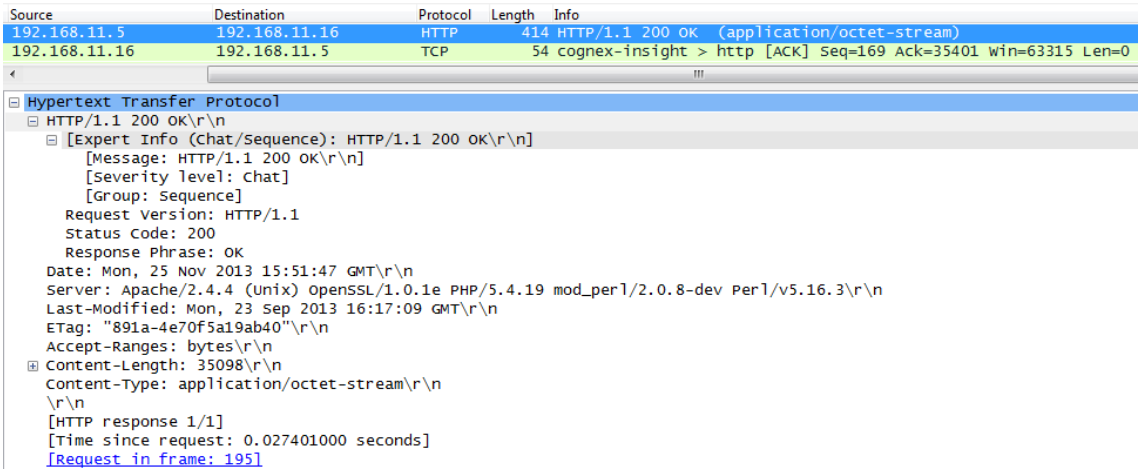
2. Seuraavaksi haittaohjelma lähettää asiakaskoneen verkkoon M-SEARCH -kyselyjä löytääkseen UPnP-protokollalla toimivia laitteita samasta verkosta missä asiakaskone toimii. Kyselyt lähetetään ryhmälähetyksenä (multicast) osoitteeseen 239.255.255.250, UDP-porttiin 1900. Verkossa toimivia UpnP-laitteita ovat mm. reitittimet, joiden välityksellä asiakaskone muodostaa verkkoyhteyden. Näiden tietojen avulla haittaohjelma voi päätellä, mikäli asiakaskone käyttää NAT-palvelua yhteyden muodostamiseksi tai yhteys muodostuu suoraan julkisella ip-osoitteella. [13; 15.]

3. Haittaohjelma lähettää HTTP GET /cfg.bin -komennon hakeakseen hallintapalvelimelta uusimman konfiguraatiotiedoston. Kuvassa 21 on Wireshark-sovelluksella kaapattuna tämä liikenne.




**Kuva 21. Konfiguraatiotiedoston hakupyyntö palvelimelle.**

Hallintapalvelin lähettää salatun cfg.bin-tiedoston ja kuittaa onnistuneen vastauksen asiakaskoneen pyyntöön lähettämällä HTTP/1.1 200 OK -vastauksen (kuva 22).

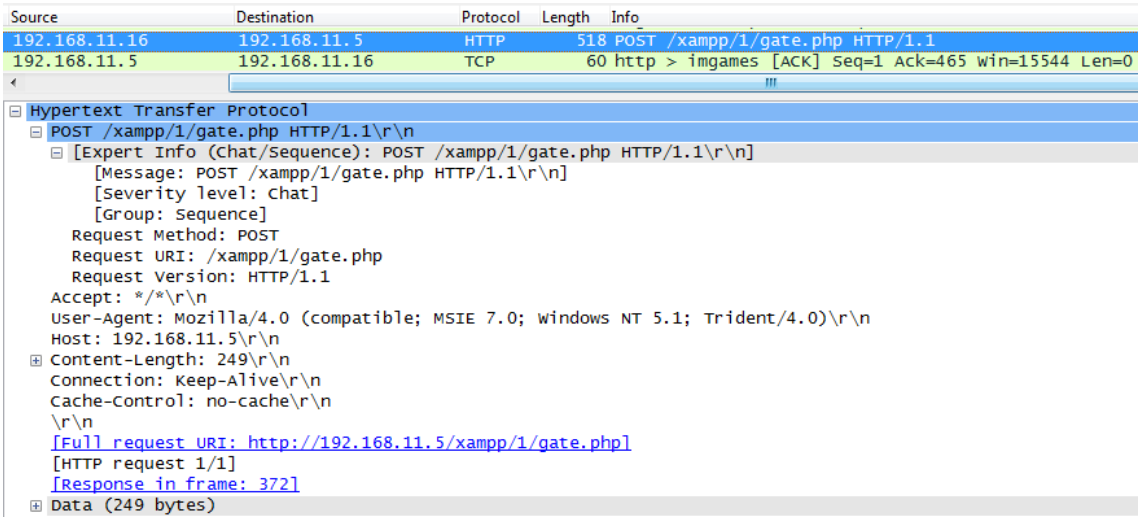



**Kuva 22. Hallintapalvelin lähettää salatun konfiguraatiotiedoston.**

4. Asiakaskone vastaanottaa salatun konfiguraatiotiedoston ja purkaa salauksen käyttämällä haittaohjelmaan sisällytettyä salausavainta.

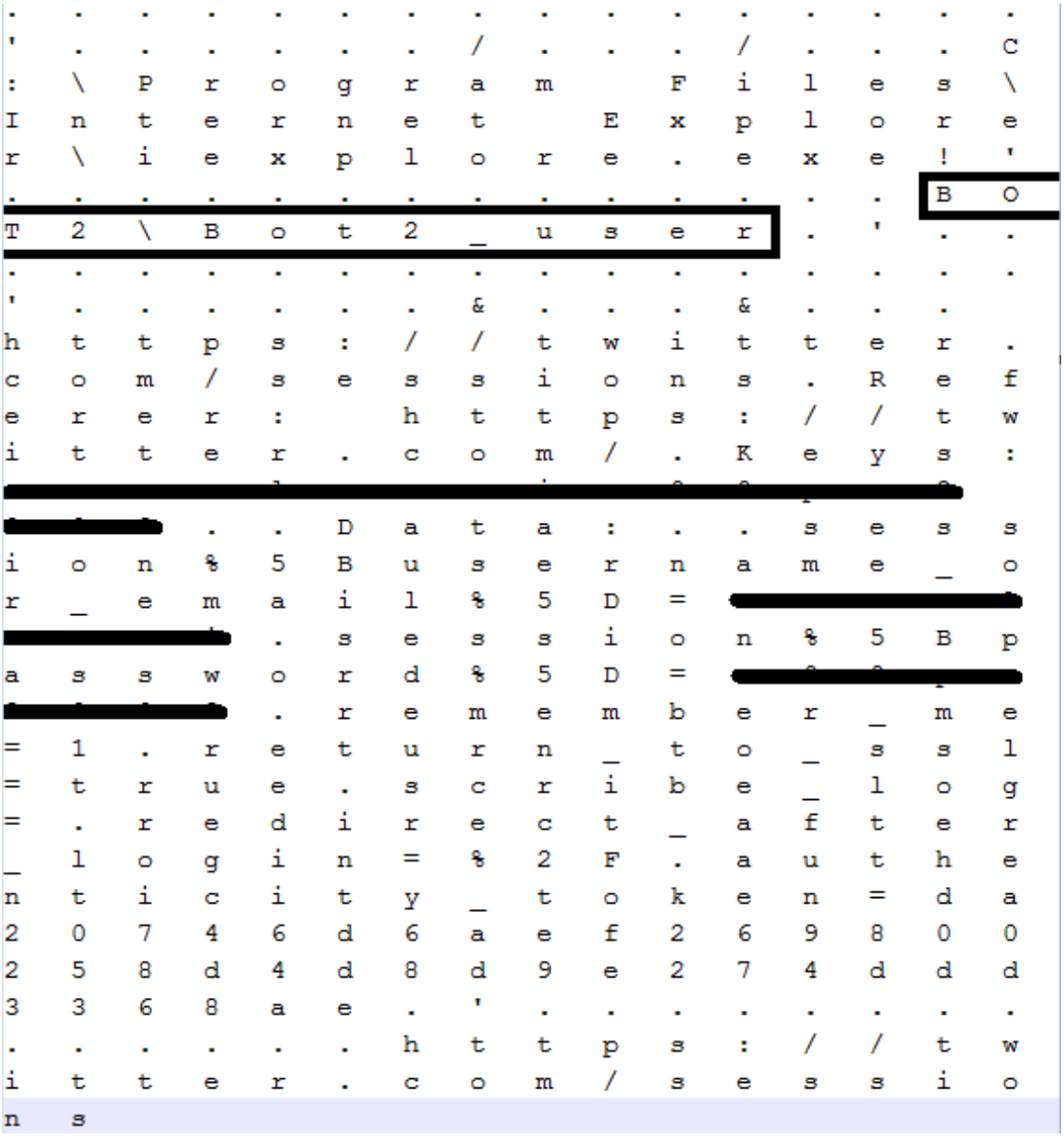
5. Haittaohjelma seuraa ja tallentaa tietoja asiakaskoneelta sekä oletuksena määritetyistä sijainneista että erikseen webinjects.txt-tiedostossa määritettyjen seurattavien internet-sivujen mukaan.

6. Lähettäessään tallentamansa tiedot asiakaskone suorittaa HTTP POST /gate.php -komennon, jolla kerätyt ja tallennetut tiedot lähetetään salattuna hallintapalvelimelle. Kuvassa 23 on kaapattuna kyseinen liikenne.



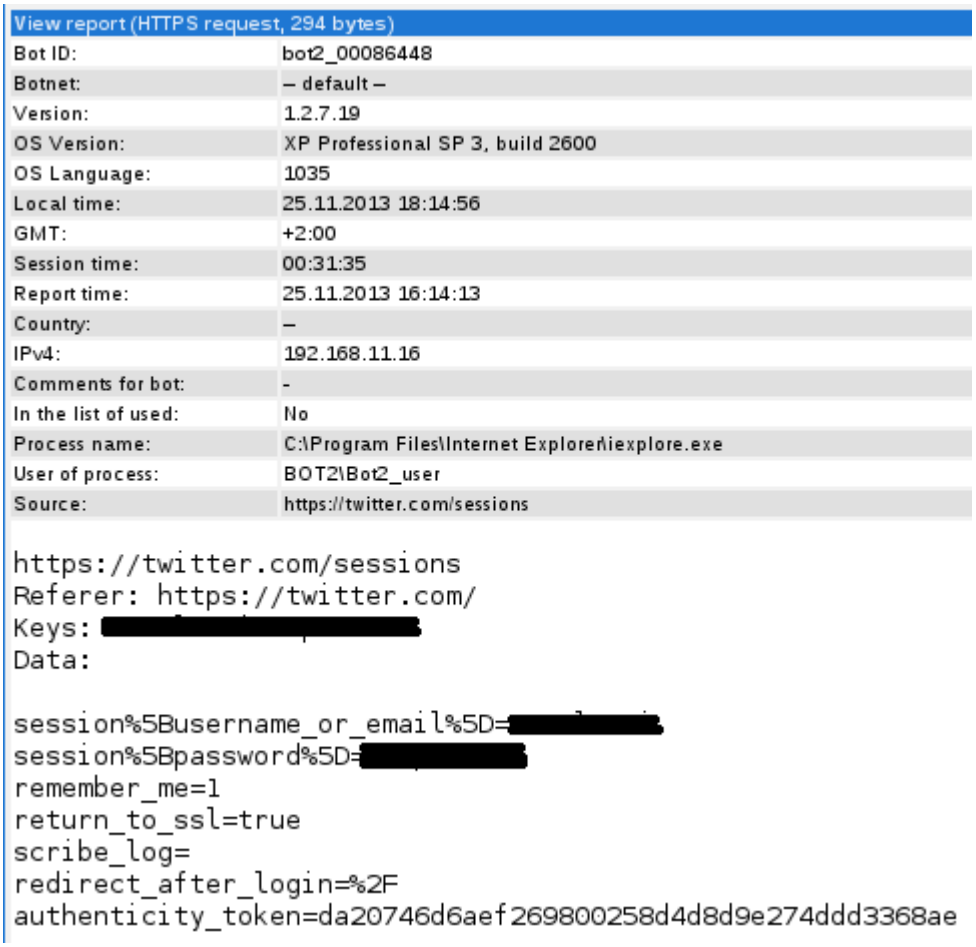

**Kuva 23. Tietojen lähettäminen salattuna hallintapalvelimelle.**

Tiedot salataan RC4-salauksella asiakaskoneen ja palvelimen välillä. Mikäli salausavain on tiedossa, voi lähetyt tiedot purkaa esimerkiksi internetistä löytyvän työkalun tai erillisen sovelluksen avulla. Yksi tällainen työkalu löytyy http://rc4.online-domain-tools.com/ -osoitteesta, jota on käytetty alla olevan salatun viestin purkamisessa. Työkalun avulla kaapatun paketin dataosasta saadaan purettua selkokielisenä hallintapalvelimelle lähetettävät tiedot. Kuvassa 24 on purettuna hallintapalvelimelle lähetetty RC4-paketti dataosaltaan, jossa Twitter palveluun kirjautuminen on lähetetty hallintapalvelimelle. Keys-osassa on välitetty käyttäjänimi ja salasana selkokielisenä. Paketin mukana lähetetään aina myös tietokoneen nimitieto, kuvassa BOT2, ja myös tietokoneelle kirjautunut käyttäjä, kuvassa Bot2_user.




Kuva 24. Datan salaus purettuna.

Hallintapalvelimella oleva gate.php-tiedosto vastaa salauksen purkamisesta sekä tietojen tallentamisesta MySQL-tietokantaan. Kuvassa 25 ovat vastaavat tiedot hallintapalvelimen tietokannasta tarkasteltuna.



View report (HTTPS request, 294 bytes)

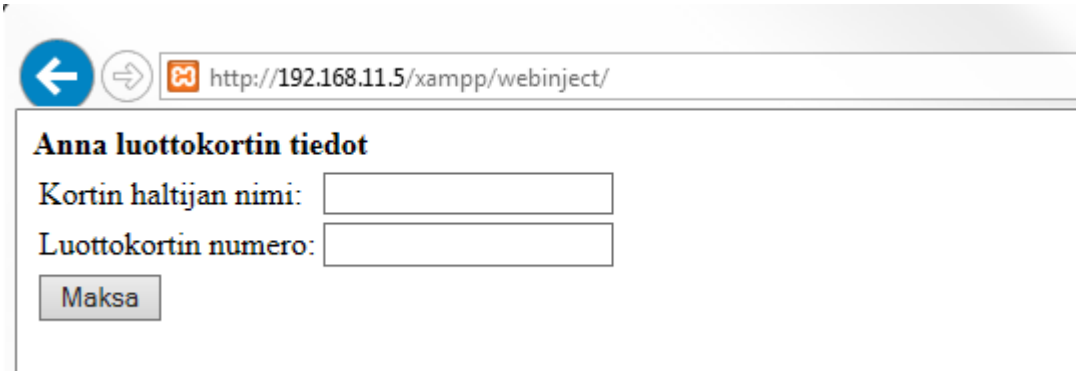
| | |
|---|---|
| Bot ID: | bot2_00086448 |
| Botnet: | – default – |
| Version: | 1.2.7.19 |
| OS Version: | XP Professional SP 3, build 2600 |
| OS Language: | 1035 |
| Local time: | 25.11.2013 18:14:56 |
| GMT: | +2:00 |
| Session time: | 00:31:35 |
| Report time: | 25.11.2013 16:14:13 |
| Country: | – |
| IPv4: | 192.168.11.16 |
| Comments for bot: | - |
| In the list of used: | No |
| Process name: | C:\Program Files\Internet Explorer\iexplore.exe |
| User of process: | BOT2\Bot2_user |
| Source: | https://twitter.com/sessions |



**Kuva 25. Vastaanotetut tiedot hallintapalvelimella.**

6. Mikäli asiakaskoneella avataan internet-sivu, joka on määritetty webinject.txt-konfiguraatiotiedostossa, käyttäjälle näytetään bot-verkon ylläpitäjän määrittämät lisätiedot sivulla. Tällaisia voivat olla mm. erilaiset ylimääräiset kentät joissa käyttäjältä kysytään tietoja, esim. henkilöturvatunnusta, pankki- tai luottokortin numeroa tai sen pin-tunnusta.

Seuraavassa on käytännössä testattu webinject.txt-tiedoston hyödyntämistä. Kuvassa 26 on perussivu mikä näkyy käyttäjille, joilla ei ole bot-verkon ylläpitäjän määrittämää haittaohjelmaa tietokoneellaan.



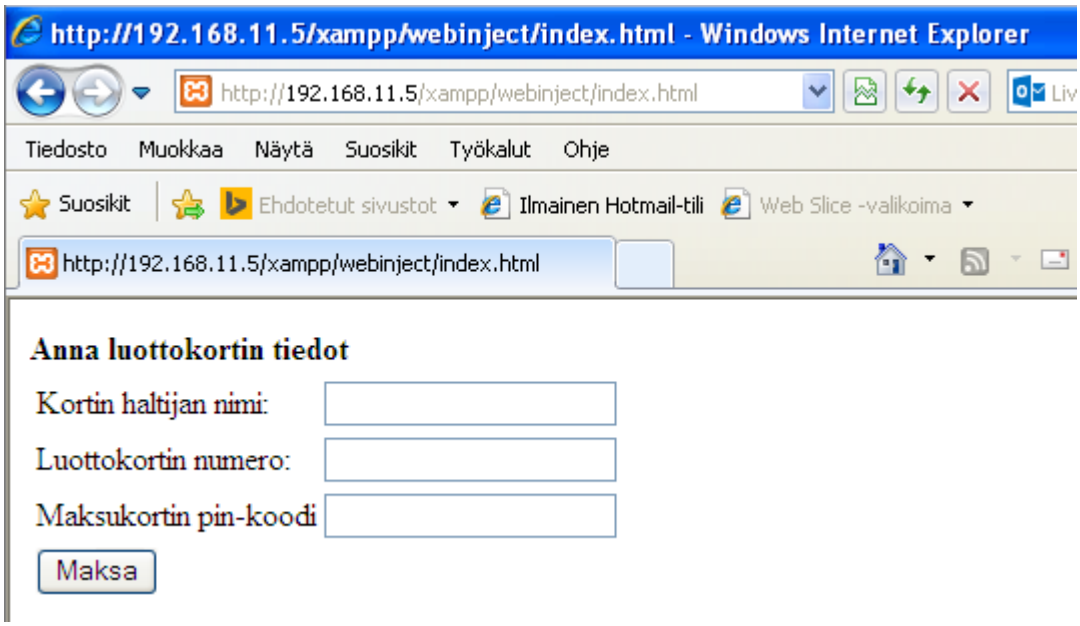

Kuva 26. Sivusto käyttäjälle jolla ei ole haittaohjelmaa asennettuna.

Webinject.txt-tiedostoon määritin esimerkkikoodi 3 listauksessa olevan muutoksen, jossa Kali Linux-testiympäristön Apache-webpalvelimella olevaa sivustoa muutetaan haittaohjelman saaneille koneille.

```
set_url http://192.168.11.5/xampp/webinject/index.html* GP
data_before
<input type="text" name="numero"></td></tr>
data_end
data_inject
<b><tr><td>Maksukortin pin-koodi</td><td><input type="text" name="pin_koodi"></td></tr></b>
data_end
data_after
data_end
```

Esimerkkikoodi 3. Webinject.txt tiedoston muokkaaminen.

Testasin muutosta BOT2-asiakaskoneella. Kun konfiguraatiotiedostoa oli muutettu, seurasin Wireshark-sovelluksella kunnes BOT2-asiakaskone haki uuden cfg.bin-tiedoston ja avasin asiakaskoneen selaimella testisivun, jonka tulos näkyy kuvassa 27.




Kuva 27. Asiakaskoneelle näkyvä sivusto.

Kuten kuvasta näkyy, selain lisäsi käyttäjälle määrittelemäni ylimääräisen kentän jossa kysytään maksukortin pin-koodia. Esimerkkikoodi 4 listauksessa näkyy muokatun sivuston lähdekoodi asiakaskoneelta tarkasteltuna.

```
<html>
<body>

<form action="" method="post">
<table>
<tr><b>Anna luottokortin tiedot</b></tr>
<tr><td>Kortin haltijan nimi: </td><td><input type="text"
 name="nimi"></td></tr>
<tr><td>Luottokortin numero: </td><td><input type="text"
 name="numero"></td></tr><b><tr><td>Maksukortin pin-
 koodi</td><td><input type="text"
 name="pin_koodi"></td></tr></b>

<tr><td><input type="submit" value="Maksa"></td></tr>
</table>
</form>
</body>
</html>
```

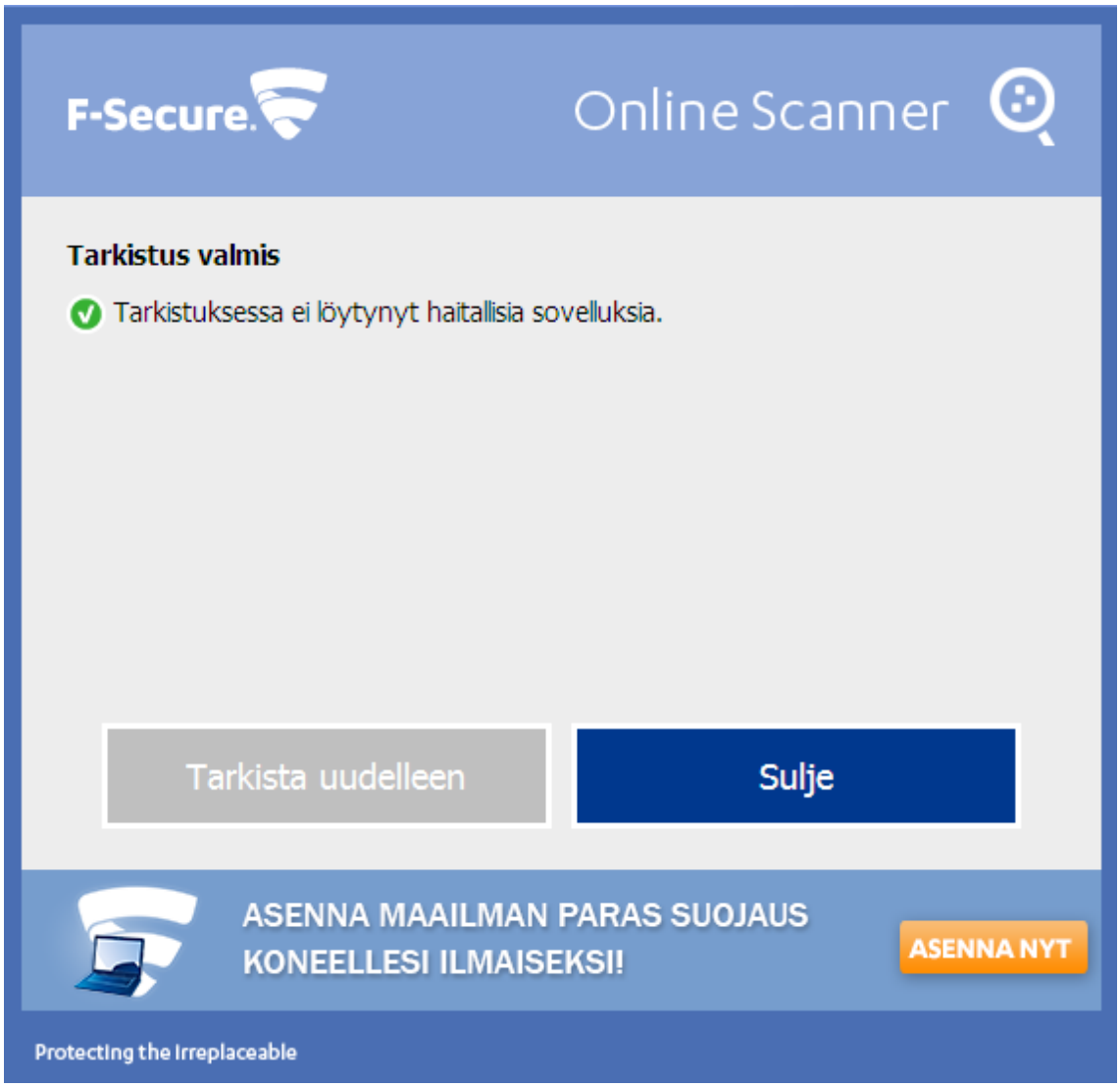
Esimerkkikoodi 4. Muokatun sivuston lähdekoodi asiakaskoneella.

Webinject.txt-tiedostoon voi määritellä asiakaskoneille lisättäväksi myös javascript-koodia, jolla asiakaskoneille voi rakentaa monimutkaisempiakin sovelluksia käyttäjien tietojen kaappaamiseksi.

## 5.3 Virustarkistuksen ajaminen asiakaskoneessa tartunnan jälkeen

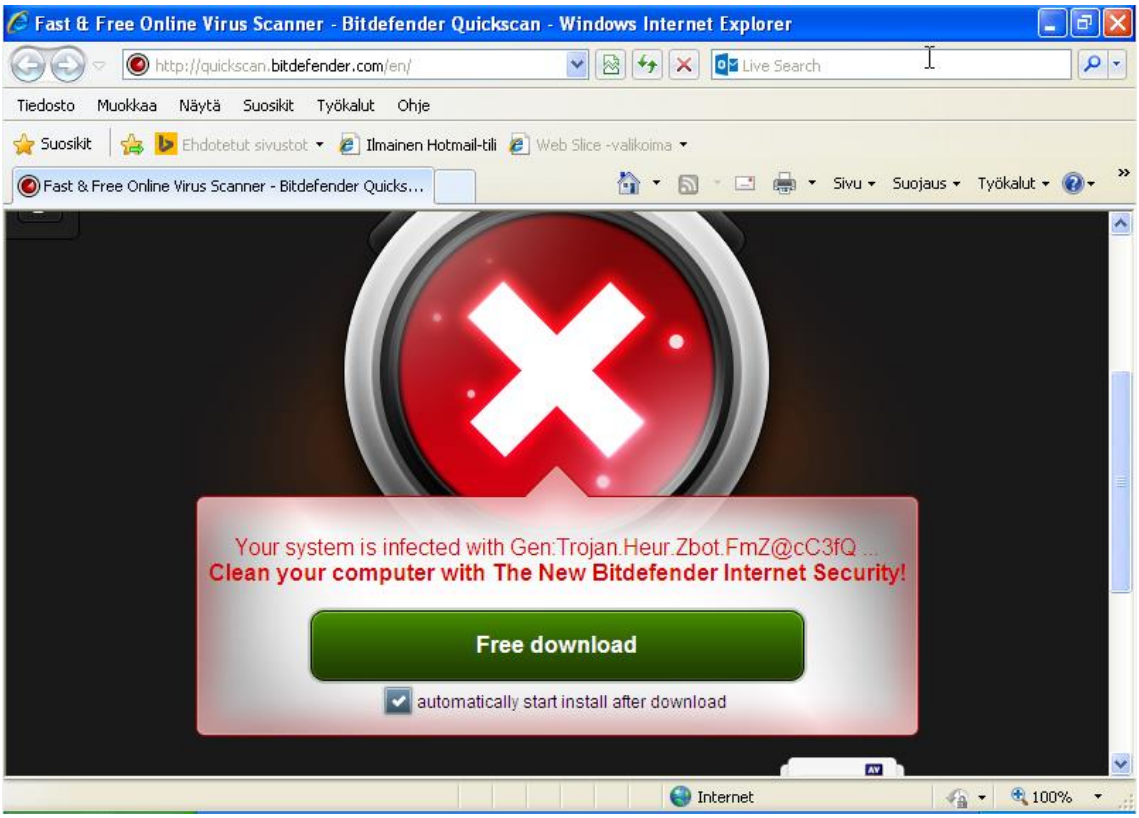
Testaamissani asiakaskoneissa oli asennettuna Windows XP Service Pack 3-käyttöjärjestelmä uusimmilla päivityksillä sekä koneissa oli Windowsin oma palomuuri käytössä. Asiakaskoneissa ei ollut erillistä virustorjuntasovellusta asennettuna. Testasin tartuttamisen jälkeen asiakaskoneita internetistä saatavilla olevilla online-virustarkistussovelluksilla.

Ensimmäisenä testasin F-Securen online-tarkistusta, joka on saatavilla osoitteessa http://www.f-secure.com/fi/web/home_fi/online-scanner. Kuvassa 28 on tarkistuksen tulos BOT2 -asiakaskoneelta eli F-Securen online-tarkistus ei löydä tartuntaa, kun tartunta on jo ehtinyt tapahtua.




Kuva 28. F-Secure Online Scanner tartunnan jälkeen.

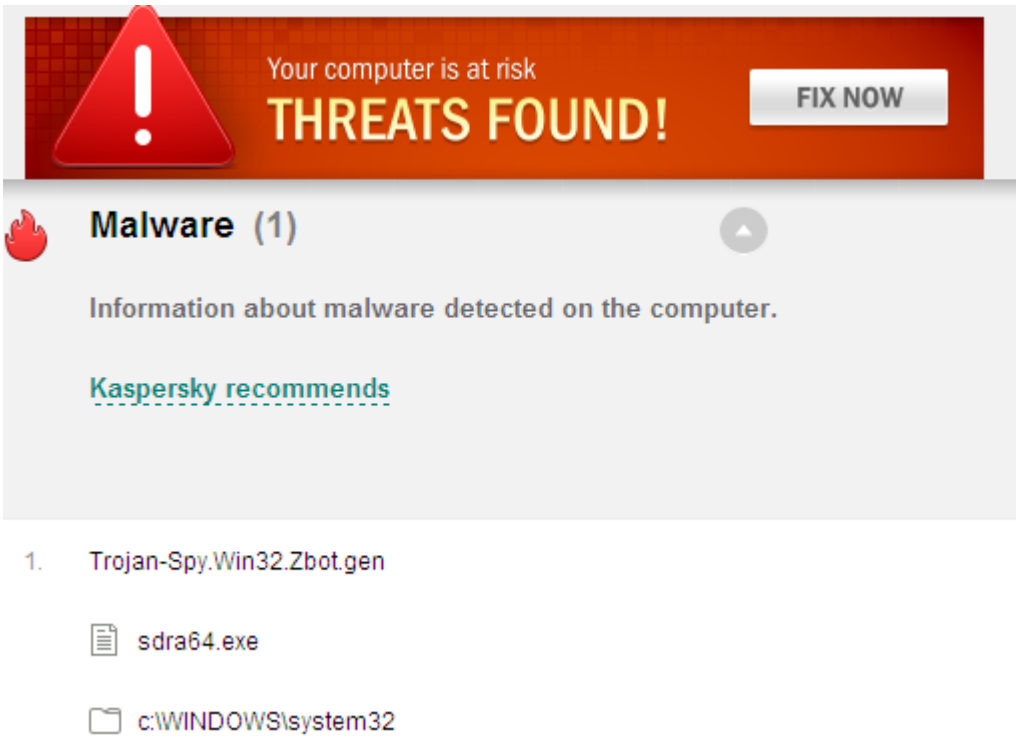
Toinen testaamani palvelu oli Bitdefenderin online-tarkistus, joka on saatavilla osoitteessa http://www.bitdefender.com/scanner/online/free.html. Kuvassa 29 on tarkistuksen tulos eli Bitdefender-palvelu löysi BOT2-asiakaskoneessa ajettuna siihen asennetun haittaohjelman.




**Kuva 29. Bitdefender online-tarkastus.**

Kaspersky-yhtiön online-virustarkistus vaatii erillisen sovelluksen asentamisen tietokoneelle. Kaspersky Security Scan on saatavilla osoitteessa http://www.kaspersky.com/virus-scanner. Sovellus löysi haittaohjelman, kuten kuva 30 osoittaa.

Tämän jälkeen ajoin vielä varmistuksena F-Securen online-tarkistuksen uudelleen ja tulos oli sama: tarkistus ei löytänyt haittaohjelmaa.




Kuva 30. Kaspersky Security Scan.

## 6 Yhteenveto

Bot-verkoista on kirjoitettu viime aikoina paljon mm. erilaisten verkkopankkihyökkäysten myötä ja monet niissä käytetyistä haittaohjelmista perustuu tässä työssä esiteltyyn Zeus-haittaohjelmaan. Tässä mielessä olinkin hieman yllättynyt, että pelkästään bot-verkkoihin liittyvää kirjallisuutta ei tahtonut löytyä, vaikka bot-verkkoja on ollut jo suhteellisen pitkään toiminnassa. Kirjallinen materiaali rajoittui yleensä yleisiin tietoturvakirjoihin, joissa bot-verkot mainittiin yhtenä osana. Suurin osa löytämästäni teoriamateriaalista löytyi internetistä ja oli tutkimus- ja oppilaitosten tutkimusmateriaalia sekä tietoturvayhtiöiden suorittamia aiheen tutkimuksia. Internetistä materiaalia löytyikin paljon yleiskuvauksista aina todella teoreettisiin tutkimuksiin bot-verkkojen liikenteestä ja liikenteen salauksessa käytetyistä algoritmeista.

Käytännön työ ja testaus sujui suunnitelmien mukaan. Asennuksissa ei tullut vastaan suurempia ongelmia. Mielenkiintoista oli seurata Wireshark-sovelluksen avulla asiakaskoneiden sekä hallintapalvelimen välistä liikennettä ja siellä välitettyjä tietoja. Työtä tehdessä tulikin perehdyttyä Wireshark-sovellukseen tarkemmin mm. tietoliikenteen

suodatuksen osalta. Sopivilla suodattimilla asiakaskoneen ja hallintapalvelimen välisen kommunikoinnin sai sujuvasti seurattua. Lisäksi salatun tietoliikenteen purkaminen oli uutta. Toki verrattuna todelliseen tietomurtotilanteeseen, minulla oli tiedossa salausavain, jonka avulla salatun datan sai purettua.

Työn aikana tuli vastaan myös muutama yllätys. Ensimmäinen oli se, miten helposti ilman virustorjuntaa olevat tietokoneet on mahdollista tartuttaa haittaohjelmilla. Käyttäjän tulee olla todella tarkkana mitä liitteitä ja sovelluksia suorittaa. Yksi väärä sovelluksen suorittaminen ja kaikki mitä käyttäjä tietokoneella tekee on mahdollista kaapata. Haittaohjelman saastutettua koneen ei ole väliä sillä, muodostaako käyttäjä salatulla https protokollalla yhteyden eri palveluihin; tunnukset ja salasanat kaapataan jo ennen salausta. Useasti kuulee sanottavan internetpalveluita käytettäessä, että kunhan yhteys on muodostettu https-protokollan avulla, on yhteys turvallinen ja käyttäjän tiedot turvassa. Tällöin jää usein mainitsematta se seikka, että käyttäjän on huolehdittava siitä, ettei hänen koneellaan ole jo asennettuna haittaohjelmaa, joka kaappaa tiedot ennen salausta.

Ongelmaa ei tule helpottamaan se, että Windows XP -käyttöjärjestelmällä olevien tietokoneiden tuki päättyy 8.4.2014. Tämä tarkoittaa sitä, että Microsoft ei enää tarjoa teknistä tukea eikä automaattisia ohjelmisto- ja tietoturvapäivityksiä kyseisen päivän jälkeen. Mikäli käytössä on Windows XP ja Microsoftin oma maksuton virustorjuntasovellus Microsoft Security Essentials, jää käyttöjärjestelmä ja virustorjunta täysin vaille uusia päivityksiä kyseisen päivän jälkeen. Ei ole vaikea ennustaa, että tietoturvaongelmia tulee kevään ja kesän aikana Windows XP -käyttöjärjestelmää edelleen käyttäville. Onkin mielenkiintoista nähdä, tuleeko tuki täysin päättymään kyseiseen päivään vai tuleeko Microsoft ainakin joiltain osin pyörtämään päätöstä mikäli XP tietokoneita on edelleen laajalti käytössä ja niitä vastaan kehitetään tuen päättymisen jälkeen nopeasti ja tehokkaasti leviävä haittaohjelma. Ja sekin lienee turvallista ennustaa, että näin tulee tapahtumaan. Esimerkiksi Atean ja Marketvisionin suorittaman markkinakatsauksen (julkaistu 4.11.2013) mukaan 40 prosenttia suomalaisyrityksistä ja julkishallinnon organisaatiosta käyttää edelleen Windows XP -käyttöjärjestelmää [16]. Netmarketshare palvelun (http://www.netmarketshare.com) mukaan Windows XP -käyttöjärjestelmän osuus koko maailmassa on laskemassa mutta on edelleen noin 31 prosenttia. Luku on säilynyt ennallaan viimeiset kuukaudet. [17.]

Toinen yllätys liittyy virustorjuntasovelluksiin ja ennen kaikkea F-Securen Online-palveluun, joka ei löytänyt koneelta haittaohjelmaa sen sinne asennuttua. Bitdefender-palvelun online-tarkastus taas löysi haittaohjelman, joten olisi mielenkiintoista tietää miten nämä palvelut eroavat toisistaan ja minkä vuoksi F-Securen palvelu ei löydä tätä haittaohjelmaa. Kaspersky Security Scan-virustarkastus, joka myös löysi haittaohjelman, poikkesi edellä mainituista siinä, että sovellus oli normaali asennettava sovellus. Kun myös Kasperskyn sovellus löysi haittaohjelman, halusin vielä varmistua, että F-Securen palvelu ei löydä haittaohjelmaa. Ajoin F-Securen online-tarkastuksen uudelleen ja tulos oli edelleen sama: palvelu ei löytänyt haittaohjelmaa ja ilmoitti tietokoneen olevan puhdas.

Kaikkiaan työn tekeminen teorian lukemisesta alkaen oli mielenkiintoista. Työn alkaessa miettimäni tavoitteet tulivat suurelta osin täytettyä ja olen tyytyväinen lopputulokseen. Yksi kehityskohde tai tulevaisuuden testauskohde on javascriptillä toteutettavat internet-sivujen muokkaukset webinject.txt-tiedostoon, mikä mahdollistaa monimutkaisempienkin toimintojen lisäämisen muokattaville sivuille. Toinen mielenkiintoinen tarkemman tarkastelun kohde liittyy edellä mainittuihin virustarkastussovelluksiin ja ennen kaikkea F-Securen palveluun, joka ei tätä haittaohjelmaa löydä. Kyseessä on kuitenkin yleinen ja pitkään tiedossa ollut haittaohjelma, joten miksi F-Secure ei sitä löydä.

Tietoturvaa koskevat ongelmat ja kysymykset eivät tule lähitulevaisuudessakaan loppumaan, joten aihe tulee pysymään ajankohtaisena vielä jatkossakin. Nykyään tietoturvassa keskitytään monesti tietoverkon ja siellä olevien palveluiden tietoturvaan, kun monesti ongelma tapahtuu jo käyttäjän päätelaitteella, joka nykyään voi olla mikä tahansa matkapuhelimesta perinteiseen tietokoneeseen. Kuluttajalle turvalliselta näyttävä yhteys palveluntarjoajaan voi olla menetetty jo käyttäjän päätelaitteessa. Laitteiden laaja kirjo eri käyttöjärjestelmineen tuo haasteita tulevaisuudessa niin käyttäjille kuin tietoturvapalveluita tarjoaville yrityksille.

## Lähteet


1 Ranta Niko. 28.11.2013. Suomalaistileiltä katosi satojatuhansia euroja verkkohyökkäyksissä. Verkkodokumentti. <http://www.mtv.fi/uutiset/rikos/artikkeli/suomalaistileilta-katosi-satojatuhansia-euroja-verkkohyokkayksissa/2418148>. Luettu 10.12.2013.

2 Mónica Diogo, Ribeiro Carlos. 2013. Leveraging Honest Users: Stealth Command-and-Control of Botnets, s.11. Verkkodokumentti. INESC-ID/IST. <https://www.usenix.org/leveraging-honest-users-stealth-command-and-control-botnets>. Luettu 9.9.2013.

3 Ollmann Gunter. 2009. Botnet Communication Topologies. Verkkodokumentti. Damballa Inc. <https://www.damballa.com/downloads/r_pubs/WP_Botnet_Communications_Primer.pdf>. Luettu 27.10.2013.

4 Kamluk Vitaly. 2008. The botnet business. Verkkodokumentti. Kaspersky Lab ZAO. <http://www.securelist.com/en/analysis/204792003/The_botnet_business>. Luettu 27.10.2013.

5 Aslam Baber, Wang Ping, Wu Lei, Zou Cliff C. A Systematic Study on Peer-to-Peer Botnets. Verkkodokumentti. University of Central Florida. <http://www.eecs.ucf.edu/~czou/research/P2P-Botnet-ICCCN09.pdf>. Luettu 11.12.2013.

6 Schiller Craig, Binkley Jim, Harley David, Evron Gadi, Bradley Tony, Willems Carsten, Cross Michael. 2007. Botnets: The Killer Web App. Syngress Publishing.

7 Microsoft Security Intelligence Report : What is a Botnet?. Verkkodokumentti. Microsoft. <http://www.microsoft.com/security/sir/story/default.aspx#!botnetsection>. Luettu 13.9.2013.

8 Hallam-Baker Phillip. 2008. The dotCrime manifesto: How to stop internet crime. Boston : Pearson Education, Inc.

9 Flegel Ulrich, Bruschi Danilo. 2009. Detection of Intrusions and Malware, and Vulnerability Assesment. Berlin: Springer.

10 John John P, Moshchuk Alexander, Gribble Steven D, Krishnamurthy Arvind. 2009. Studying Spamming Botnets Using Botlab. Verkkodokumentti. University of Washington. <https://www.usenix.org/legacy/event/nsdi09/tech/full_papers/john/john_html/>. Luettu 20.9.2013.

11 Di Pietro Roberto, Riccardi Marco. Taming Zeus by leveraging its own crypto internals. Verkkodokumentti. Barcelona Digital Technology Centre. <http://ricerca.mat.uniroma3.it/users/dipietro/eCrime11.pdf>. Luettu 21.10.2013.

12 Ollman Gunter. 2009. Top-10 botnet outbreaks in 2009. Verkkodokumentti. Damballa Inc. <https://blog.damballa.com/archives/569>. Luettu 10.11.2013.

13 Manky Derek, Macdonald Doug. Zeus: God of DIY Botnets. Verkkodokumentti. Fortinet Inc. <http://www.fortiguard.com/legacy/analysis/zeusanalysis.html>. Luettu 10.11.2013.

14 Binsalleeh H, Boukhtouta A, Debbabi M, Ormerod T, Youssef A, Sinha P, Wang L. On the Analysis of the Zeus Botnet Crimeware Toolkit. Verkkodokumentti. Concordia University Montreal, Quebec, Canada. <http://www.ncfta.ca/papers/On_the_Analysis_of_the_Zeus_Botnet_Crimeware.pdf>. Luettu 15.10.2013.

15 Chien Eric, Falliere Nicolas. 2009. Zeus: King of the Bots. Verkkodokumentti. Symantec Corporation. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf>. Luettu 15.10.2013.

16 Atea, Marketvision. 2013. Windows XP yhä laajasti käytössä. Verkkodokumentti. Atea. <http://www.atea.com/main-menu/Press-Center/Press-Release-Archive-/press-releases-2013/finnish-atean-ja-marketvision-markkinakatsaus-windows-xp-yha-laajasti-kaytossa-suomessa/>. Luettu 4.11.2013.

17 Netmarketshare. 2013. Desktop Top Operating System Share Trend. Verkkodokumentti. Netmarketshare. <http://www.netmarketshare.com/>. Luettu 4.11.2013.