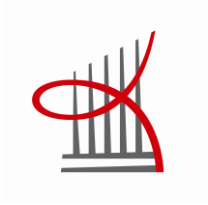


INFORMAATIOSODANKÄYNTI – TIETOVERKKOJEN VAARAT

Juhani Lillbacka

Opinnäytetyö
Huhtikuu 2012
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

JUHANI LILLBACKA:
Informaatiosodankäynti - tietoverkkojen vaarat

Opinnäytetyö 69 sivua
Huhtikuu 2012

Tietotekniikan ja Internetin kehittyessä, yhä useammilla ihmisillä on ollut mahdollisuus päästä käsiksi Internetissä jaettavaan tietoon. Samalla myös tietoturvauhat ovat kehittyneet vaarallisemmiksi ja niistä on nykyään enemmän haittaa, kuin koskaan ennen. Ainut asia mikä ei ole kehittynyt vuosien varrella, on ihmisten perustieto tietoturvasta. Yhä useammat ihmiset ovat muuttuneet huolimattomammiksi ja eivätkä seuraa mitä he tekevät Internetissä.

Tässä opinnäytetyössä käsitellään yleisimpiä hyökkäystekniikoita ja sovelluksia, joita verkkohyökkääjä voi käyttää informaation varastamiseen tai verkkoliikenteen häirintään.

Tämän opinnäytetyön tarkoituksena on antaa monipuolista tietoa lukijalle erilaisista vaaroista, joita piileksii nykypäivän tietoverkoissa, menemättä monimutkaisiin teknisiin tietoihin.

Opinnäytetyö on jaettu kahteen pääkategoria ja kahteen pienempään aiheeseen. Ensimmäinen kategoria kattaa yleiskuvauksen eri haittaohjelmatyypeistä ja niiden alaluokista, sekä miten ne leviävät ja toimivat. Toinen kategoria kattaa yleiskuvauksen useista erilaisista ja yleisistä verkkohyökkäystekniikoista. Viimeiset kaksi aihetta eivät kuulu kumpaankaan pääkategoriaan, mutta ne liittyvät kuitenkin vahvasti molempiin.

Asiasanat: haittaohjelma, verkkohyökkäys, tietoturva, tietokoneuhat, tietotekniikka

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Computer Systems Engineering
Telecommunication Engineering

JUHANI LILLBACKA:
Information warfare – dangers of computer networks

Bachelor's thesis 69 pages
April 2012

As information technology and Internet have developed, more and more people have had the chance to access the information shared on the Internet. At the same time information security threats have developed more dangerous and they are now more harmful than ever before. The only thing that has not developed over the years is the people's basic knowledge of information security. More and more people have become careless and do not follow what they are doing on the Internet.

This Bachelor’s thesis discusses the common methods and applications that a network attacker might use to steal data or to disrupt network traffic.

The purpose of this thesis is to give a comprehensive insight to the reader about the different dangers that are lurking in today’s computer networks, without delving into complex technical details

The thesis is divided into two main categories and two smaller subjects. The first category covers a general description of different malware classes and their subclasses, and how they spread and work. The second category covers a general description of a number of common network attack techniques. The remaining two subjects do not fall into either category, but they are, however, strongly related to the both of them.

Key words: malware, network attack, information security, computer threats, information technology

SISÄLLYS

LYHENTEET JA TERMIT

ACPI	(engl. Advanced Configuration and Power Interface) Määrittelee yleisen rajapinnan laitteiston tunnistusta, emolevyä, laitteiston määritystä ja virranhallintaa varten.
ARP	(engl. Address Resolution Protocol) Protokolla, jolla selvitetään Ethernet-verkossa laitteen MAC-osoite.
ARP-taulukko	Taulukko, joka sisältää ARP-tietoja.
Autentikointi	(engl. authentication) Toiminto käyttäjän tai palvelun identiteetti varmentamiseen. Voidaan tehdä esimerkiksi salasanan perusteella.
Autentikointipalvelin	(engl. authentication server). Palvelin missä autentikointi suoritetaan.
Banker	Haittaohjelma, joka erikoistuu pankkitietojen kaappaamiseen.
Backdoor-ohjelma	(suom. takaporttiohjelma) Haittaohjelma, joka mahdollistaa luvattoman pääsyn tietokoneeseen.
BIOS	(engl. Basic Input-Output System) Tietokoneohjelma, joka lataa käyttöjärjestelmän keskusmuistiin, sekä käynnistää sen tietokoneen käynnistyessä. Tarjoaa myös alkeellisen laitetuen.
Botti	Lyhenne sanasta robotti. Haittaohjelma, jota käytetään tietokoneiden saastuttamiseen ja niiden hallintaan.

DHCP	(engl. Dynamic Host Configuration Protocol) Verkkoprotokolla, jonka yleisin tehtävä on IP-osoitteiden jakaminen verkkoon kytkeytyville laitteille.
DHCP-palvelin	Jakaa verkkoon kytkeytyville laitteille IP-osoitteita. Voi tarvittaessa jakaa muitakin osoitetietoja.
DHCP-pyyntö	Verkkoon kytkeytyneen laitteen lähettämä pyyntö DHCP-palvelimelle osoitetietojen saamiseksi.
Dialer	Haittaohjelma, joka katkaisee Internet-yhteyden muodostamiseen käytetyn puhelinyhteyden ja avaa sen uudelleen muodostaakseen uuden yhteyden maksulliseen numeroon.
DNS	(engl. Domain Name System) Nimipalvelujärjestelmä tietokoneille, palveluille tai muille Internetiin tai lähiverkkoon kytketyille laitteille. Se muuntaa verkkotunnuksen IP-osoitteeksi.
DNS-kysely	Nimipalvelukysely.
Ethernet	Pakettipohjainen lähiverkkoratkaisu
FTP	TCP-protokollaa käyttävä tiedostonsiirtomenetelmä kahden tietokoneen välillä. Toimii asiakas-palvelin –periaatteella.
Haavoittuvuus	Haavoittuvuus on järjestelmässä tai ohjelmassa oleva virhe, josta aiheutuu uhka järjestelmällä. Jotta uhka toteutuisi, tarvitaan hyökkääjä, haavoittuvuus ja hyökkäysvektori.
Hajakoodausfunktio	(engl. hash function) Algoritmi, jota käytetään hajautustaulutietorakenteen muodostamisessa. Sen avulla voidaan luoda salasanatiivisteitä.

Hakukonehuijaus	Hakukonehuijauksen tarkoituksena on nostaa Internet-sivun näkyvyyttä hakukoneessa. Hakukonehuijausta voidaan kuitenkin käyttää myös haittamielisten sivustojen näkyvyyden nostamiseen.
Hook	(suom. koukku) Ohjelmointitermi, joka kattaa monta eri tekniikkaa joita käytetään muuttamaan tai laajentamaan käyttöjärjestelmän, ohjelman tai muiden ohjelmistokomponenttien toimintaa sieppaamalla funktiokutsuja.
HTTP-liikenne	
Hyökkäysvektori	Reitti, jonka kautta haavoittuvuutta käytetään hyväksi.
ICMP	(engl. Internet Control Message Protocol) TCP/IP-pinon kontrolliprotokolla. Välittää tietoa erilaisista virhetilanteista.
ICMP redirection	ICMP-viestien uudelleenohjaus.
IP-osoite	(engl. Internet Protocol) Osoite, joka yksilöi jokaisen tietoverkkoon kytketyn laitteen.
IRDP spoofing	(engl. ICMP Router Discovery Protocol) IRDP on reititysprotokolla, jonka avulla reititin voi mainostaa oletusreittiä. IRDP ei kuitenkaan käytä minkäänlaista autentikointia, jonka johdosta hyökkääjä voi väärentää oletusreittimainokset. Tämän seurauksena tietoverkosta ulosmenevä verkkoliikenne katkeaa kokonaan.
Jaettu salaisuus	(engl. shared secret). Tietokone joka lähettää viestin toiselle tietokoneelle, salaa viestin sisällön jaetulla salaisuudella. Vastaanottava tietokone taasen purkaa viestissä olevan salauksen samalla jaetulla salaisuudella. Jaettua salaisuutta ei koskaan lähetetä verkon yli.

Kazaa	Vertaisverkko-ohjelma, jota voidaan käyttää tiedostojen lataamiseen ja lähettämiseen.
Keylogger	(suom. näppäilytallennin) Ohjelma, joka tallentaa käyttäjän näppäinpainallukset.
Kernel	(suom. ydin). Tietokoneen ohjelmien toiminnot ovat riippuvaisia käyttöjärjestelmän ytimestä.
Keskeytys	(engl. interrupt) Signaali, joka saa tietokoneen suorittimen keskeyttämään meneillään olevan ohjelman suorituksen.
Keskitin	(engl. hub) Verkkolaite, joka vastaanottaa signaalin ja lähettää sen edelleen muuttumattomana.
Kopiointisuojausohjelma	Ohjelma, jonka tarkoituksena on estää luvaton kopiointi.
Kytkin	(engl. switch) Toimii samalla tavalla kuin keskitin, mutta se pystyy tunnistamaan paketeissa olevien tietojen perusteella paketin päämäärän ja täten lähettämään paketin suoraan sille tarkoitettuun osoitteeseen.
Linux	Yleisesti käytössä oleva termi, jolla viitataan UNIX-kaltaisten käyttöjärjestelmien perheeseen, jotka käyttävät Linux-ydintä.
LKM	(engl. Loadable Kernel Module) Ladattava kernel-moduuli. Laajentavat ytimen toimintaa, esim. tukemalla uutta laitteistoa.
MAC-osoite	(engl. Media Access Control) Verkkosovittimen yksilöivä osoite.
Makro	Makroja käyttämällä voidaan ohjata ohjelmien toimintaa, esim. Microsoft Wordissa.

Master Boot Record	MBR sisältää levyn osiointitiedot ja ohjeet, joiden avulla BIOS löytää käyttöjärjestelmän latauskoodin.
MediaMax CD-3	Sony BMG:n käyttämä kopiointisuojausohjelma.
Ohjelmisto	Useiden tietokoneohjelmien muodostava kokonaisuus, perhe, esim. Microsoft Office.
Oikeuksien laajentaminen	(engl. Privilege Escalation) Toiminto, jossa hyväksikäytetään käyttöjärjestelmän tai ohjelman vikaa, suunnittelu- tai konfigurointivirhettä, jolla käyttäjän oikeuksia saadaan laajettua sille kuulumattomalle tasolle.
Oletusyhdyskäytävä	(engl. default gateway) Reitti aliverkosta ulkoiseen verkkoon.
OSI-malli	(engl. Open Systems Interconnection Reference Model) Kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa. Kukin kerroksista käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs.
Paketti	Pakettikytkentäisessä verkossa (Ethernet) viestit lähetetään paketteina.
Password stealer	Troijalainen, joka on luotu kaappaamaan salasanoja.
Payload	Haittaohjelman sisältämä ns. lisäohjelmointi, joka toimii eräänlaisena lastina. Sisältää usein muita haittaohjelmia.
Ponnahdusikkuna	(engl. pop-up window) Ikkuna, joka pompahtaa esiin. Sitä käytetään yleensä Internet-mainonnassa.
Port stealing	(suom. portin varastaminen) Toiminto, jossa hyökkääjä huijaa kytkintä ohjaamaan verkkoliikenteen toiseen kytkimen porttiin.

PXE	(engl. Preboot eXecution Environment) Mahdollistaa tietokoneen käynnistyksen yhteydessä käynnistysympäristön lataamisen tietoverkon yli.
Reititin	(engl. router) Tietoverkkoja yhdistävä laite, jonka tehtävänä on välittää tietoa tietoverkkojen eri osien välillä.
Salasanatiiviste	(engl. hash) Hajakoodausfunktiolla muodostettu salasanan merkkijono.
Sosiaalinen manipulointi	(engl. Social engineering) Toiminta, joka perustuu ihmisten hyväuskoisuuteen. Sen tarkoituksena on saada käyttäjä paljastamaan tai antamaan pääsy luottamukselliseen tietoon huijaamalla tai esiintymällä luotettavana tahona.
STP	(engl. Spanning Tree Protocol) Siltojen ja kytkimien käyttämä protokolla, jonka avulla estetään mahdolliset verkkosilmukat.
STP mangling	(suom. STP-runtelu) MITM-hyökkäyksessä käytettävä tekniikka, jolla hyökkääjästä voidaan tehdä uusi juurisilta.
SQL-injektiohyökkäys	Hyökkäystekniikka, joka hyväksikäyttää tietokantapohjaisten sovelluksien tietoturva-aukkoja. Sen avulla on mahdollista tunkeutua järjestelmään.
Topologia	Verkon rakenne, eli tapa jolla verkkolaitteet ovat kytkettynä toisiinsa.
Traffic tunneling	(suom. tietoliikenteen tunnelointi) Toiminto, joka muodostaa tietoliikenteelle tunnelin kahden halutun osoitteen välille.

UNIX	Laitteistoriippumaton käyttöjärjestelmäperhe. Sen kehittivät AT&T:n Bell Labsin työntekijät Ken Thompson ja Dennis Ritchie vuonna 1969.
Usenet	Usenetin muodostavat erilaiset keskusteluryhmät, jotka ovat keskustelu-, tiedotus- ja tiedonvaihtopalstoja. Viestien lukemiseen ja lähettämiseen tarvitaan ryhmiä varten tehty ohjelma.
Vertaisverkko	Verkko, joka ei sisällä kiinteitä palvelimia tai asiakkaita. Jokainen verkkoon liitetty laite toimii samaan aikaan palvelimena että asiakkaana verkon muille laitteille.
VM	(engl. Virtual Machine) Ohjelmallisesti toteutettu tietokone, eli virtuaalikone.
VMM	(engl. Virtual Machine Monitor) Virtuaalikoneen monitori, joka käsittelee oikeat resurssit ja tarjoaa ne virtuaalikoneille.
VPN	(engl. Virtual Private Network) Virtuaalinen yksityisverkko on tapa, jolla voidaan yhdistää kaksi tai useampaa verkkoa julkisen verkon yli.
XCP	(engl. Extended Copy Protection) Sony BMG:n käyttämä kopiointisuojausohjelma.
XSS-hyökkäys	Hyökkäystekniikka, joka hyödyntää WWW-sovelluksissa esiintyviä tietoturva-aukkoja. Sen avulla on mahdollista tunkeutua verkkosivulle.
Yksityinen avain	Yksityisellä avaimella voidaan vahvistaa lähettäjän identiteetti. Tätä kutsutaan viestin allekirjoittamiseksi. Kun vastaanottaja vastaanottaa yksityisavaimella allekirjoitetun viestin, voi vastaanottaja olla varma, että viestin lähettäjä on todellakin lähettänyt kyseisen viestin.

Zombie-tietokone	Botilla saastutettu tietokone, jota hyökkääjä voi etähallita. Osa bottiverkoa.
Zone Labs	Tietoturvaratkaisuja tarjoava yritys. Tunnettu palomuureistaan ja VPN-tuotteistaan.

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on kertoa kokeneille ja kokemattomille tietokoneen käyttäjille tietoverkoissa piilevistä vaaroista. Työssä pyritään käymään kattavasti läpi yleisimpiä hyökkäystekniikoita ja sovelluksia, joita verkkohyökkääjä voi käyttää informaation varastamiseen tai verkkoliikenteen häiritsemiseen. Työ sisältää lisäksi laajan termistön ja niiden selostukset. Enemmän asiasta kiinnostuneille työ tarjoaa hyvät lähteet alkuperäisteoksiin, sekä tietoturva-aiheisiin sivustoihin.

Tämä dokumentti on jaettu kahteen pääkategoriaan ja kahteen pienempään aiheeseen. Ensimmäisessä kategoriassa kerrotaan yleisimmistä haittaohjelmatyypeistä, niiden mahdollisista alaluokista, haittavaikutuksista ja leviämistekniikoista. Toisessa kategoriassa käsitellään yleisimpiä verkkohyökkäystekniikoita ja niiden toteutustapoja. Kahdessa pienemmässä aiheessa käydään läpi tietojenkalastelu ja bottiverkot.

Työssä ei suoriteta haittaohjelmille ruumiinavausta, eikä käsitellä niiden tartuntatilastoja. Työssä ei lisäksi oteta kantaa tietoturvauhkien tulevaisuuden näkymiin.

2 HAITTAOHJELMATYYPIT

2.1 Malware-haittaohjelma

Haittaohjelma on ohjelma, jonka tarkoituksena on häiritä tietokoneen toimintaa, kerätä luottamuksellista tietoa tai mahdollistaa luvaton pääsy järjestelmään. Haittaohjelmatyyppejä ovat tietokonevirukset, tietokonemadot, troijalaiset, vakoiluohjelmat, mainosohjelmat ja muut haittamieliset ohjelmat.

2.2 Crimeware-rikollisohjelma

Crimeware ei varsinaisesti ole haittaohjelmatyyppi. Crimewareksi voidaan määritellä kaikki ohjelmat ja sosiaalinen manipulointi, joiden tavoitteena on taloudellisen hyödyn hankkiminen petollisin keinoin. Petolliset keinot voivat tarkoittaa esimerkiksi pankkitilin tyhjentämistä kaapatulla salasanalla tai myymällä luottamuksellista tietoa eteenpäin. (Panda Security: Crimeware - the silent epidemic.)

Crimewaren haittoja ovat:

- Luottamuksellisen tietojen kaappaaminen
- Identiteettivarkaudet
- Yksityisyyden suojan menettäminen
- Lailliset ongelmat, kun kolmas osapuoli käyttää saastunutta konetta haittatarkoituksiin
- Salasanakaappauksista aiheutuvat rahalliset menetykset
- Järjestelmän hidastumisen, käyttöjärjestelmävirheiden, jne. takia
- Lisääntynyt roskaposti, mainonta ponnahdusikkunoiden avulla, jne (Panda Security: Crimeware - the silent epidemic).

Crimewareksi luetaan:

- Trojanit, varsinkin keyloggerit, salasanan varastajat ja bankerit
- Automatisointia hyödyntävät sovellukset, kuten botit
- Phishing, jonka avulla käyttäjältä yritetään kalastella pankkitunnuksia jne.
- Adware
- Spyware
- Roskapostitus
- Dialerit, joiden avulla modeemiyhteydet saadaan soittamaan maksullisiin numeroihin (Panda Security: Crimeware - the silent epidemic).

Crimeware ei aiheuta ongelmia pelkästään yksityishenkilöille, vaan siitä on myös haittaa yrityksille. Esimerkiksi vuonna 2009 eräs rakennusyritys joutui crimewaren hyökkäyskohteeksi ja yrityksen pankkitililtä vietiin 447000 $ muutamien minuuttien aikana. (Lemos 2009.)

2.3 Computer Virus-tietokonevirus

Tietokonevirus on haittaohjelmatyyppi, joka leviää liittämällä itsensä osaksi ohjelmaa tai dokumenttia. Tietokonevirukset eivät leviä itsestään tietokoneesta toiseen, kuten tietokonemadot, vaan ne ovat riippuvaisia käyttäjän vuorovaikutuksesta. (Chen & Robert 2004.)

Suurin osa tietokoneviruksista on liitetty käynnistystiedostoon, jonka johdosta tietokonevirus voi oleskella järjestelmässä aktivoimattomana. Kun käyttäjä suorittaa käynnistystiedoston, siinä oleva tietokoneviruksen haittakoodi aktivoituu, jonka johdosta tietokonevirus alkaa levitä järjestelmässä. Yleensä tietokoneviruksen sisältävä ohjelma toimii normaalisti haittakoodin aktivoinnin jälkeen, mutta jotkut tietokonevirukset estävät koko ohjelman toimimisen. Tietokonevirukset leviävät tietokoneesta toiseen käyttäjän avustuksella. Käyttäjä voi esimerkiksi liittää tietokoneviruksen sisältävän ohjelman tai tiedoston sähköpostiliitteeseen. (Chen & Robert 2004, 1-2.)

2.3.1 Tietokoneviruksen historia ja evoluutio

Ensimmäinen tietokoneviruksiin liittyvä akateeminen työ julkaistiin vuonna 1949, jonka tekijänä oli John von Neumann. Neumann käsitteli työssään ”Theory of elf-reproducing automata” kuinka tietokoneohjelma voidaan suunnitella lisääntymään itsestään. (von Neumann 1966.)

Vuonna 1971 BBN Technologiesilla työskentelevä Bob Thomas ohjelmoi maailman ensimmäisen tietokoneviruksen, Creeperin. Creeper oli kokeellinen, itsestään lisääntyvä ohjelma, joka levisi Internetin esi-isässä ARPANETissä ja se saastutti TENEX-käyttöjärjestelmällä varustettuja DEC PDP-10 tietokoneita. Saastutettuaan tietokoneen Creeper-tietokonevirus näytti viestin ”I’m the creeper, catch me if you can!”. (Chen & Robert 2004, 3.)

Vuonna 1972 Veith Risak julkaisi artikkelin ”Selbstreproduzierende Automaten mit minimaler Informationsübertragung”, joka perustui John von Neumannin työhön. Risak käsitteli artikkelissaan Siemens 4004/35 tietokonejärjestelmässä toimivaa assemblerilla ohjelmoitua tietokonevirusta. (Risak 1972.)

Vuonna 1980 Jürgen Kraus kirjoitti diplomityönsä ” Selbstreproduktion bei Programmen” Dortmundin yliopistossa. Työssään Kraus oletti, että tietokoneohjelmat kykenevät toimimaan samankaltaisesti, kuin biologiset virukset. (Kraus 1980.)

Ensimmäinen vapaasti leviävä mikrotietokoneita saastuttanut tietokonevirus, oli Elk Cloner. Sen oli ohjelmoinut vitsinä 15-vuotias Richard Skrenta vuonna 1981 ja se saastutti Apple DOS 3.3 käyttöjärjestelmällä varustettuja tietokoneita. (Rouse 2005.)

Vuonna 1984 University of Southern Californian opiskelija Fred Cohen kirjoitti seminaarityön ”Computer Viruses – Theory and Experiments”. Se oli ensimmäinen työ, jossa itsestään lisääntyvää ohjelmaa nimitettiin nimenomaan tietokonevirukseksi. (Cohen 1984.) Myöhemmin vuonna 1987, Cohen todisti väitöskirjassaan, ettei ole olemassa sellaista algoritmia, joka tunnistaisi onnistuneesti kaikki erilaiset tietokonevirukset. (Chess & White 2000.)

Ensimmäinen MS-DOSissa toimiva tietokonevirus Brain havaittiin vuonna 1986. Brain korvasi saastuneen levykkeen käynnistyssektorin viruksella ja siirsi alkuperäisen käynnistyssektorin toiseen sektoriin ja merkkasi sen huonoksi. Kun saastunutta käynnistyssektoria yritettiin lukea, Brain näytti alkuperäisen käynnistyssektorin sisällön, täten onnistuen välttämään havaitsemisen. (McAfee: Rootkits, Part 1 of 3 – The Growing Threat 2006, 3.)

Vuonna 1990 Mark Washburn ja Ralf Burger kehittävät ensimmäisen polymorfisen tietokonevirusperheen, Chameleonin, analysoimalla Vienna- ja Cascade-tietokoneviruksia. (Securelist: History of malicious programs – 1990.)

Maailman ensimmäinen makrovirus, Concept, havaitaan vuonna 1995. (F-Secure: W32/Concept.)

Vuonna 1998 Taiwanissa havaitaan CIH-tietokonevirus. CIH oli yksi maailman tuhoisimmista tietokoneviruksista. Sen oli ohjelmoinut Taiwanilainen Chen Ing-hau. CIH-viruksen tuhoisa haittakuorma aktivoitu ensimmäisen kerran 26. huhtikuuta 1999, aiheuttaen yli 250 milj. dollarin vahingot. (Symantec: W95.CIH.)

2.3.2 Toimintatapa

Jotta tietokonevirus voi lisääntyä, sen pitää päästä suorittamaan koodia ja kirjoittamaan työmuistiin. Tämän takia monet tietokonevirukset ovat liitettyinä käynnistystiedostoihin, jotka voivat olla osa luotettavaa ohjelmaa. Jos käyttäjä yrittää käynnistää saastuneen ohjelman, tietokoneviruksen haittakoodi saatetaan suorittaa ensiksi. Tietokonevirukset voidaan jakaa kahteen eri ryhmään toimintatavan mukaan. (AnVir: Virus.)

Suoraan toimivat tietokonevirukset etsivät heti aktivoiduttuaan saastutettavia kohteita ja saastuttavat ne. Tämän jälkeen tietokonevirus käynnistää isäntäohjelmansa ja lopettaa toimintansa ja jää odottamaan seuraavaa aktivointikertaa. (AnVir: Virus.)

Muistinvaraiset tietokonevirukset taas eivät etsi saastutettavia kohteita, kun ne aktivoituvat. Ne sen sijaan lataavat itsensä työmuistiin aktivoinnin yhteydessä ja siirtävät hallinnan isäntäohjelmalle. Tietokonevirus pysyy kuitenkin taustalla aktiivisena ja se saas-

tuttaa uusia tiedostoja, kun käyttöjärjestelmä tai muut ohjelmat käyttävät niitä. (AnVir: Virus.)

2.3.3 Tyypit

Tietokonevirukset luokitellaan kahden tekijän perusteella, mitä ne saastuttavat ja miten ne saastuttavat. Erityyppisiä tietokoneviruksia on useita. (OmniSecu: Types of Computer Viruses.)

2.3.3.1 Käynnistyssektorivirus

Käynnistyssektorivirus saastuttaa kiintolevyn ensimmäisen sektorin, jossa Master Boot Record sijaitsee. Kun tietokone käynnistetään, käynnistyssektorivirus käynnistyy saman tien ja lataa itsensä työmuistiin. (OmniSecu: Types of Computer Viruses.)

2.3.3.2 Tiedostoja poistava tietokonevirus

Tiedostoja poistava tietokonevirus on suunniteltu poistamaan käyttöjärjestelmän kriittisiä tiedostoja. (OmniSecu: Types of Computer Viruses.)

2.3.3.3 Makrovirus

Makrovirukset ovat ohjelmoitu makroiksi. Ne saastuttavat tiedostoja, joita käsitellään makrotoimintoja sisältävillä ohjelmilla. (OmniSecu: Types of Computer Viruses.)

2.3.3.4 Retrovirus

Retrovirukset ovat tietokoneviruksia, jotka hyökkäävät käyttöjärjestelmän viruksentorjuntaohjelmaa vastaan. Jotkut retrovirukset yrittävät sammuttaa viruksentorjuntaohjelman tai tuhota virustunnisteiden tietokannan. (OmniSecu: Types of Computer Viruses.)

2.3.3.5 Suojatut tietokonevirukset

Jotkut tietokonevirukset käyttävät salakirjoitusta tunnistamisen välttämiseksi. Salakirjoitusta käyttävä tietokonevirukset sisältävät pienen salauksenpurkumoduulin ja salakirjoitetun kopion tietokoneviruksen lähdekoodista. Jos tietokonevirus salakirjoittaa itsensä joka kerta eri salausavaimella, ainut osa joka on kokoajan pysynyt samana, on salauksenpurkumoduuli. Tässä tapauksessa viruksentorjuntaohjelma ei tunnista tietokonevirusta allekirjoituksen perusteella, mutta se voi silti tunnistaa salauksenpurkumoduulin, jonka avulla tietokoneviruksen epäsuora tunnistaminen on mahdollista. (AnVir: Virus.)

2.3.3.6 Piilotietokonevirukset

Tietokonevirus voi piilottaa itsensä sieppaamalla viruksentorjuntaohjelman lähettämän tiedoston lukupyynnön. Sieppauksen jälkeen tietokonevirus vastaa lukupyyntöön lähettämällä lukupyyntöä koskettavasta tiedostosta saastumattoman version, jotta viruksentorjuntaohjelma ei tunnista tietokonevirusta. Ainut varma tapa kiertää tietokoneviruksen sieppausyritykset, on käyttää luotettavaa ulkopuolista järjestelmää tiedostojen tarkistamiseen. (AnVir: Virus.)

2.3.3.7 Polymorfinen tietokonevirus

Polymorfista koodia sisältävät tietokonevirukset käyttävät salakirjoitusta. Polymorfisen tietokoneviruksen käyttämä salakirjoitustapa poikkeaa kuitenkin suojatun tietokoneviruksen käyttämästä tavasta. Polymorfinen tietokonevirus salakirjoittaa myös salauksenpurkumoduulinsa, joten jokaisen salauskerran jälkeen tietokoneviruksen allekirjoitus on erilainen. Viruksentorjuntaohjelmat voivat kuitenkin tunnistaa polymorfisen tietokoneviruksen tilastollisella malli analyysilla tai purkamalla sen salauksen emulointiohjelmalla. (AnVir: Virus.)

2.3.3.8 Metamorfinen tietokonevirus

Jotta tietokonevirus voi välttää emulointiohjelmalla suoritetun tunnistamisen, sen pitää uudelleenkirjoittaa itsensä joka kerta, kun se saastuttaa uuden tiedoston. Tietokoneviru-kset jotka käyttävät tätä tekniikkaa, ovat metamorfisia tietokoneviruksia. Metamorfinen tietokonevirus on yleensä erittäin suuri ja monimutkainen. (AnVir: Virus.)

2.4 Computer Worm-tietokonemato

Tietokonemadot ovat ohjelmia, jotka lisääntyvät, toimivat itsenäisesti ja liikkuvat verkkoyhteyksiä pitkin. Tietokonematojen ja tietokonevirusten keskeisin ero on tapa, jolla ne lisääntyvät ja leviävät. Virukset ovat riippuvaisia tiedostoista, haittakoodin aktivoinnista ja tiedostojen siirtämisestä tietokoneiden välillä, jotta ne kykenevät leviämään. Tietokonemadot ovat taas kykeneviä toimimaan täysin itsenäisesti ja ne voivat levitä omasta aloitteestaan, verkkoyhteyksiä pitkin. (Spencer: Computer Worms.)

Tietokonemadoista aiheutuva suurin haitta on niiden kyky lisääntyä itsestään. Tietokonemadon saastuttama tietokone kykenee lähettämään eteenpäin satoja tai tuhansia kopioita itsestään. Tietokonemato voi esimerkiksi lähettää kopion itsestään jokaiseen sähköpostiosoitekirjassa olevaan osoitteeseen. Mikäli tietokonemato onnistuu saastuttamaan vastaanottajan tietokoneen, se toistaa saman toiminnon kuin lähettäjän tietokoneessa, jatkaen sitä seuraavissa kohteissa. (Beal 2011.)

Tietokonemadon lisääntyminen ja leviäminen kuormittaa saastunutta tietokonetta, joka voi aiheuttaa järjestelmän hidastumisen tai sen kaatumisen. (Beal 2011.)

2.4.1 Tietokonematojen historia

Termi tietokonemato juontaa juurensa vuonna 1975 julkaistuun John Brunnerin kirjoittamaan The Shockwave Rider romaaniin. Vuonna 1979 John Shochin ja Jon Huppin tieteelliset kokeilut liittyivät Brunnerin romaanissa kuvailtuun verkkopohjaiseen lapamatoon. (Chen 2003.)

Yksi ensimmäisistä Internetin kautta levinneistä tietokonemadoista, oli Morris-mato. Sen oli ohjelmoinut Cornell yliopiston opiskelija, Robert Tappan Morris. Lähdekoodiltaan Morris-mato oli 99 riviä pitkä ja se lähti leviämään Massachusettsin teknologian instituutista 2. marraskuuta 1988. Alun perin Morris-madon oli tarkoitus levitä salassa ja aiheuttamatta vahinkoja. Ohjelmointivirheen vuoksi kuitenkin Morris-mato hidasti saastuneita tietokoneita kopioimalla toistuvasti itseään. Alle 90 minuutissa ensimmäisestä tartunnasta, saastunutta järjestelmää oli mahdotonta käyttää suuren kuormituksen vuoksi. Kaiken kaikkiaan Morris-mato saastutti yli 6000 tietokonetta ja se aiheutti 0,1-10 milj. dollarin taloudelliset tappiot vahingoittamatta laitteistoa. (Schmidt & Darby 2001.)

Seuraavan kerran tietokonemadot aiheuttivat suurta huomiota vasta vuonna 1999, kun Melissa-mato lähti leviämään alt.sex keskusteluryhmässä Usenetissä. Melissa-madon jälkeen tietokonemadot ovat olleet vuosittain uutisotsikoissa. (Fosnock 2005, 4.)

2.4.2 Toimintapa ja haittavaikutukset

Tietokonematojen nopeasta leviämisestä aiheutuva kuormitus ei pelkästään rajoitu saastuneisiin koneisiin. Koska tietokonematojen tavoitteena on juurikin nopea leviäminen, ne myös kuormittavat tietoverkkoa, jossa ne leviävät. (Spam Laws: Computer Worm Malware – How It Works.)

Tietokonemadot voivat teoriassa myös levitä minkä tahansa tyyppisen tietoverkon kautta. Mikäli kohteiden, tietokoneiden, puhelinten tai verkkotilien välillä on reitti mitä pitkin tietokonemadot voivat levitä tietoverkosta toiseen, voi älykäs haittaohjelmien tekijä luoda tietokonemadon, joka pystyy leviämään tietoverkon tyypistä riippumatta. (F-Secure: About Worms.)

Nopean leviämisen ja siitä johtuvan kuormituksen lisäksi, tietokonemadot kykenevät myös suorittamaan muita toimintoja. Tietokonematojen kantamat haittakuormat voivat asentaa saastuneeseen tietokoneeseen backdoor-ohjelman, poistaa tai salata tiedostoja, lähettää dokumentteja sähköpostin kautta, jne. Yleisin tietokonematoihin liitetty haittakuorma on backdoor-ohjelma, jonka avulla saastunut tietokone voidaan tarvittaessa liit-

tää osaksi bottiverkkoa. (Panda Security: Worms.) Tämän vuoksi roskapostittajat ovat hyvin usein yhdistetty tietokonematojen rahoitukseen ja luontiin. (McWilliams 2003.)

2.4.3 Tyypit ja leviäminen

Jokainen tietokonemato on tyypiltään erilainen ja tyypistä riippuen, ne leviävät eri tavalla. Tavallisimmat tyypit ovat sähköposti-, verkko-, pikaviestin-, Internet-madot ja sosiaalisten verkostojen kautta leviävät tietokonemadot. Yleisin näistä tyypeistä on sähköpostimato. (F-Secure: About Worms.)

2.4.3.1 Internet-Worm-Internet-mato

Internet-madot kykenevät lähettämään itsensä etäsijainnista suoraan tietokoneeseen. Tämän tyyppiset tietokonemadot ovat luotu hyödyntämään järjestelmähaavoittuvuuksia, joiden avulla ne pääsevät sisälle järjestelmään. Internet-madot löytävät kohteensa etsimällä Internetistä haavoittuvuuksille alttiita olevia tietokoneita. Kun Internet-mato löytää sopivan tietokoneen, se lataa itsensä tietokoneeseen ja jatkaa uusien kohteiden etsintää. (F-Secure: About Worms.)

2.4.3.2 Net-Worm-verkkomato

Toisin kuin Internet-madot, verkkomadot kopioivat itsensä tietokoneisiin, jotka ovat yhteydessä toisiin tietokoneisiin paikallisverkon kautta. Yksi verkkomatojen suosima leviämistapa on verkkojakojen käyttö. Ne kopioivat itsensä verkossa jaettavaan laitteeseen tai kansioon. Koti- ja yritysverkoissa on melko usein salasanalla suojaamattomia verkkojakoja, joiden ansiosta verkkomadon on helppo levitä verkon sisällä. (F-Secure: About Worms.)

2.4.3.3 Social Networking Worm-sosiaalisten verkostojen kautta leviävä tietokonemato

Sosiaalisten verkostojen kautta leviävät tietokonemadot ovat erikoistuneet siihen sosiaaliseen verkostoon missä ne leviävät. Esimerkiksi Facebookissa verkoston muodostavat palvelussa olevat käyttäjät. Saastunutta kohdetta taas vastaa saastunut käyttäjätili. Tämän tyyppiset tietokonemadot leviävät saastuneen käyttäjätilin julkaisemien viestien avulla ja ne ovat myös miltei aina luotu hyödyntämään kyseisessä sosiaalisessa verkostossa olevia haavoittuvuuksia. (F-Secure: About Worms.)

2.4.3.4 IM-Worm-pikaviestinmato

Pikaviestinmadot käyttävät erilaisia pikaviestinohjelmia levitäkseen. Pikaviestinmato lähettää saastuneessa koneessa olevan pikaviestinohjelman avulla viestin jokaiselle viestimen yhteystiedoissa olevalle henkilölle. Viesteissä on usein Internet-linkki haittasivustolle, joka saastuttaa jokaisen sivustolla vierailleen tietokoneen. Joissakin tapauksissa viesti saattaa sisältää haitallisen liitteen. Miltei kaikki suositut pikaviestinohjelmat ovat joutuneet pikaviestinmatojen kohteeksi. (F-Secure: About Worms.)

2.4.3.5 E-mail Worm-sähköpostimato

Sähköpostimato leviää nimensä mukaisesti sähköpostin avulla. Sähköpostimato voi esiintyä sähköpostissa haitallisena liitteenä tai se voi olla upotettuna objektina tai koodina sähköpostin viestissä. Kun sähköpostimato onnistuu saastuttamaan tietokoneen, se lähettää uusia sähköpostiviestejä saastuneen tietokoneen sähköpostikirjassa oleviin osoitteisiin. (F-Secure: About Worms.)

2.5 Trojan-troijalainen

Troijalainen on haittaohjelma, joka esittää luotettavaa ohjelmaa. Troijalainen suorittaa erilaisia toimintoja luvatta ja käyttäjän tietämättä. Troijalaiset eivät itsessään aiheuta suoranaista haittaa tietokoneelle. Niiden pääsääntöinen toiminta on asentaa saastunee-

seen tietokoneeseen muita haittaohjelmia, joiden avulla tietokonetta kyetään etähallitsemaan. (F-Secure: About Trojans.)

2.5.1 Troijalainen – susi lampaan vaatteissa

Nimensä troijalaiset saavat Kreikkalaisesta mytologiasta, Troijan puuhevosesta. Troijan puuhevosen tapaan troijalaiset sisältävät arvaamattoman haittakuorman. Haittakuormat voivat sisältää viruksilla saastutettuja tiedostoja, salasanan kaappaajia, jne. (F-Secure: About Trojans.)

Koska troijalaiset esittävät luotettavia ohjelmia, ne saastuttavat helposti hyväuskoisten käyttäjien tietokoneita. Myöskään skeptisimmät käyttäjät eivät ole turvassa, koska haittaohjelmien tekijät venyvät usein uskomattomiin suorituksiin, saadakseen troijalaisen näyttämään uskottavalta ja luotettavalta. Tämän takia troijalaiset voivat esiintyä video- ja äänitiedostoina, dokumentteina ja luotettavina ohjelmina. Yksi suosittu taktiikka on naamioida troijalainen päivitystiedostoksi. (F-Secure: About Trojans.)

2.5.2 Troijalaiset ja tietokonevirukset

Tietokonevirukset ja troijalaiset ovat teknisesti erityyppisiä haittaohjelmia. On tärkeätä erottaa ne toisistaan, vaikkakin ne voivat tuottaa saman lopputuloksen Molemmat voivat esimerkiksi poistaa tietokoneesta tiedostoja. Tietokonevirukset ja troijalaiset käyttävät kuitenkin erilaisia keinoja saman tuloksen saamiseen. Käytännössä tämä tarkoittaa sitä, että esimerkiksi tietokoneviruksen tunnistamiseksi, estämiseksi ja poistamiseksi käyttäjä joutuu käyttämään eri keinoja, kuin troijalaisen tapauksessa. (F-Secure: About Trojans.)

Tietokonevirukset ja troijalaiset eroavat toisistaan kahdella selkeällä tavalla. Tietokonevirukset kulkeutuvat tietokoneesta toiseen tiedostojen liitännäisinä, kun taas troijalaiset luottavat käyttäjän harhautukseen ja hyväuskoisuuteen, esittämällä jotain mitä ne eivät ole. Toinen eroavaisuus liittyy leviämistapaan. Troijalaiset eivät levitä kopioita itsestään, mutta tietokonevirukset levittävät. Kun troijalainen saastuttaa tietokoneen, se ei pyri etsimään uutta saastutettavaa kohdetta. Tämän takia käyttäjä pystyy keskittymään yhden ohjelman poistamiseen, eikä useamman. (F-Secure: About Trojans.)

Useat ohjelmat voidaan helposti tunnistaa troijalaiseksi tai tietokonevirukseksi. Ainoa poikkeus tästä ovat troijalais-virushybridit, joissa troijalaiseen on lisätty tietokoneviruksenkaltaista koodia virusmaisen leviämisen mahdollistamiseksi. Tämän tyyppiset haittaohjelmat ovat kuitenkin erittäin harvinaisia, koska ne ovat hyvin monimutkaisia. (F-Secure: About Trojans.)

2.5.3 Leviäminen

Vuosia sitten yleisin tapa, jolla troijalaisia ja muita haittaohjelmia levitettiin, oli niiden lähettäminen suoraan kohteeseen, yleensä sähköpostiliitteissä. Tämä levitystapa on yksi sosiaalisen manipuloinnin muodoista. Hyökkääjä joutuu tekemään sähköpostiviestistä tarpeeksi uskottavan, jotta tietokoneen käyttäjä lataa ja avaa liitetiedoston. Tämä levitystapa on kuitenkin vähitellen menettänyt suosiota laajemmissa hyökkäyksissä. (F-Secure: About Trojans.)

Nykyään troijalaiset leviävät useilla eri tavoilla. Ne voivat levitä esimerkiksi:

- Luotettavilta sivustoilta, joihin on murtauduttu
- Phishing-sivustojen kautta, jotka jakavat haittaohjelmia
- Hakukonehuijauksien avulla
- Kaapattujen sähköpostitilien tai sosiaalisten verkostojen käyttäjätilien kautta lähetettyjen haittaviestien avulla (F-Secure: About Trojans).

2.5.4 Tyypit

Troijalaisia on olemassa useita eri tyyppejä, kuten luottamuksellista tietoa kaappaavia troijalaisia, tietoturvaohjelmien toimimisen estäviä troijalaisia, etähallinnan mahdollistavia troijalaisia, jne. Troijalaisten luokittelu muuttuu alati suosion mukaan, esimerkiksi banker-troijalaiset luokitellaan kokonaan omaksi tyypiksi niiden kasvaneen suosion mukaan. (F-Secure: About Trojans.)

2.5.4.1 Trojan-Spy-vakoojatroijalainen

Vakoojatroijalainen on troijalainen, jonka avulla hyökkääjä pystyy seuraamaan käyttäjän liikkeitä saastuneessa tietokoneessa. Vakoojatroijalaisilla on laajat ominaisuudet, joihin lukeutuu keyloggerit, tietokoneen prosessien seuranta ja tiedostojen kaappaaminen. Tämän tyyppiset troijalaiset ovat hyvin suosittuja. Jotkut backdoor-ohjelmat tai tietokonemadot asentavat vakoojatroijalaisia. (F-Secure: Terminology.)

2.5.4.2 Trojan-Dropper-haittaohjelman sisältävä troijalainen

Haittaohjelman sisältävä troijalainen sisältää yhden tai useamman pakatun version toisesta haittaohjelmasta. Pakattu haittaohjelma saattaa olla tietokonemato, toinen troijalainen tai backdoor-ohjelma. Pakattu haittaohjelma puretaan kun käyttäjä suorittaa troijalaisen sisältävän käynnistystiedoston. (F-Secure: Terminology.)

2.5.4.3 Trojan-Downloader-tiedostoja lataava troijalainen

Tiedostoja lataava troijalainen lataa tiedostoja salaa Internet-sivuilta ja FTP:n kautta. Tiedostojen lataamisen jälkeen troijalainen asentaa ja suorittaa tiedostot salaa. Kun tiedostoja lataava troijalainen on suorittanut ensimmäisen ohjelmoidun prosessin, eli tiedostojen lataamisen ja suorittamisen, se voi siirtyä seuraavaan ohjelmoituun prosessiin. (F-Secure: Terminology.)

2.5.4.4 Trojan-Proxy-välityspalvelintroijalainen

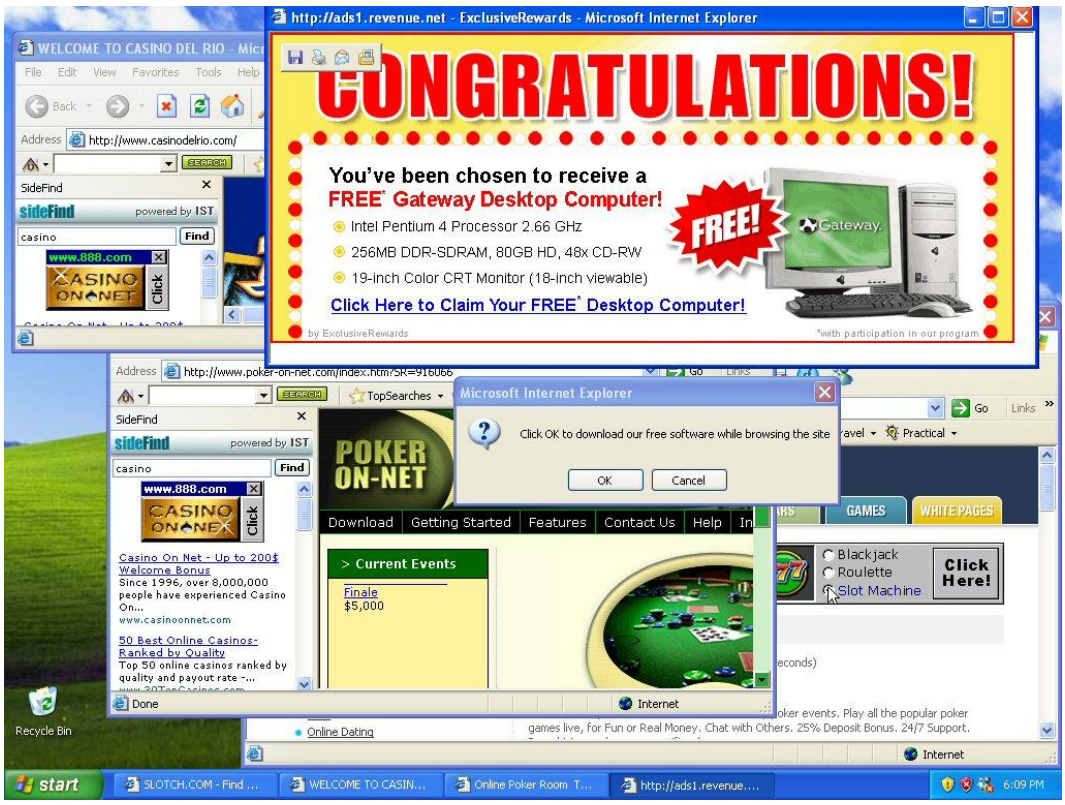
Välityspalvelintroijalainen mahdollistaa saastuneen tietokoneen käyttämisen välityspalvelimena. Hyökkääjät käyttävät usein välityspalvelimia piilottaakseen sijaintinsa Internetissä. (F-Secure: Terminology.)

2.5.4.5 Trojan-Password-salasanoja kaappaava troijalainen

Salasanoja kaappaava troijalainen on samankaltainen kuin vakoojatroijalainen. Salasanoja kaappaavan troijalaisen voidaan ajatella erikoistuvan ainoastaan käyttäjätilitietojen kaappaamiseen. Tilitietojen kaappaaminen on mahdollista troijalaisen asentaman keyloggerin ansiosta. (F-Secure: Terminology.)

2.6 Adware-mainosohjelma

Adware on eräänlainen ohjelma, joka näyttää asennettuna tietokoneen käyttäjälle mainoksia. Lisäksi jotkin adwaret voivat kerätä käyttäjästä tietoja kohdemainontaa varten. Monet ihmiset yhdistävät adwaren spywareen. Vaikka tämä onkin totta tietyin rajoin, adwaren keräämiä tietoja käytetään mainontaan, eikä rikolliseen toimintaan. Mainokset esiintyvät monissa eri muodoissa, kuten esimerkiksi mainospalkkeina selaimessa tai erittäin aggressiivisina pop-up ikkunoina (kuva 1). Adware voi myös esiintyä positiivisessa muodossa, mutta suurinta osaa adwareista pidetään haitallisina. (Spam Laws: What is Adware.)



KUVA 1. Adware ja pop-up ikkunat (Edwards 2011.)

Yleensä tietokoneen käyttäjä lataa koneellensa adwaren tietämättään. Suurin osa adwaresta on liitetty toisiin ohjelmiin, esimerkiksi ilmaisohjelmiin. Usein kuitenkin ohjelman asennusvaiheessa käyttäjää pyydetään lukemaan ohjelman käyttöoikeussopimus, jossa kerrotaan ohjelmassa olevasta mahdollisesta adwaresta. Valitettavan usein kuitenkin käyttöoikeussopimus jää lukematta, joten mahdollisesta adwaresta ei käyttäjällä ole tietoa. (Spam Laws: What is Adware.) Yksi ehkä tunnetuimmista ilmaisohjelmista, johon oli liitetty adware. oli vertaisverkko-ohjelma nimeltä Kazaa. (Wauters 2010.)

Jotkin adwaret voivat hyödyntää tietokoneessa olevia tietoturva-aukkoja. Esimerkiksi jotkut sivustot voivat asentaa tietokoneeseen adwaren tietoturva-aukon kautta. Tällaisessa tapauksessa asennusta suoritetaan ilman käyttäjän suostumusta tai tietämystä. (Spam Laws: What is Adware.)

2.7 Spyware-vakoiluohjelma

Spyware on vakoiluohjelma, joka kerää tietoja tietokoneen käyttäjästä tai yrityksestä ilman lupaa. Spyware yleensä kaappaa tietoja, joita voidaan käyttää mainontaan tai muuhun taloudellista hyötyä tavoittelevaan tarkoitukseen. (Panda Security: Spyware.)

2.7.1 Vakoiluohjelmien historia

Termiä spyware käytettiin ensimmäistä kertaa Usenetissä vuoden 1995 lopulla, jolla viitattiin humoristisesti Microsoftin liiketoimintamalliin. Termin käyttö vakiintui vuonna 1999, kun sitä käytettiin Zone Labsin lehdistötiedotteessa. Ensimmäinen spywaren poistamiseen tarkoitettu ohjelma, OptOut, julkaistiin Steve Gibsonin toimesta vuoden 2000 alkupuolella. (Wienbar 2004.)

2.7.2 Haittavaikutukset ja leviäminen

Spyware leviää pääsääntöisesti samalla tavalla kuin adware, eli haitallisten verkkosivujen kautta, ilmaisohjelmien kautta, jne. Ilmaisohjelmat voivat myös spywaren tapauk-

sessa ilmoittaa spywaren olemassa olosta käyttöoikeussopimuksessa. (Panda Security: Spyware.)

Spywareksi luokitellut ohjelmat kaappaavat:

- Salasanoja ja käyttäjätunnuksia
- IP- ja DNS-tietoja
- Tietokoneen selaushistorian
- Pankkitunnuksia
- Dokumenttien sisällön (Panda Security: Spyware).

2.8 Rootkit-murtopakki

Rootkitit eivät ole tietoturvamaailmassa kovinkaan uusi asia. Termi rootkit viittasi alun perin haitalliseksi muutettuun hallintatyökaluun tai työkaluihin, joiden avulla pystyttiin ylläpitämään hallinnollisia oikeuksia saastuneessa käyttöjärjestelmässä. Ajan myötä kuitenkin termillä ruvettiin viittaamaan haittaohjelmaan, joka piilottaa itsensä ja suorittaa toimintoja vaivihkaa. (McAfee: Rootkits, Part 1 of 3 – The Growing Threat, 1.)

2.8.1 Murtopakkien historia ja kehittyminen

Haittaohjelmien piilottaminen käyttäjiltä ja järjestelmänvalvojilta juontaa juurensa ensimmäiseen MS-DOS tietokonevirukseen. Ensimmäinen naamiointitekniikkaa hyödyntävä tietokonevirus Brain, havaittiin vuonna 1986. Brain korvasi saastuneen levykkeen käynnistyssektorin viruksella ja siirsi alkuperäisen käynnistyssektorin toiseen sektoriin ja merkkasi sen huonoksi. Kun saastunutta käynnistyssektoria yritettiin lukea, Brain näytti alkuperäisen käynnistyssektorin sisällön, täten onnistuen välttämään havaitsemisen. (McAfee: Rootkits, Part 1 of 3 – The Growing Threat, 1.)

Vähän Brainin jälkeen rootkitit levisivät myös UNIX-alustoille. Esimerkiksi SUN Microsystemsin laitteista löydettiin muokattuja järjestelmän perusylläpitotyökaluja, joiden avulla pystyttiin saamaan etäkäytössä pääkäyttäjän oikeudet, mahdollistamaan oikeuksien laajentamisen päätasolla, piilottamaan mahdolliset todisteet ja pysymään havaitsematta. (Shields 2008, 1-2.)

90-luvun puolivälissä tutkijat huomasivat, että rootkittien havaitseminen oli entistä helpompaa. Työasemakohtaisia tietoturvaohjelmia, kuten Tripwirea, käytettiin estämään ylläpitotyökalujen ja kirjastojen muokkaaminen. Tästä johtuen ohjelmistotason rootkitit olivat heikompia ja helpompia havaita. (Shields 2008, 2.)

Vuosina 1997–1999 tutkijat huomasivat että rootkittien toiminnot ovat mahdollista toteuttaa alemmilla tasoilla, jonka takia niiden havaitseminen olisi selvästi entistä vaikeampaa. Mikäli rootkit toimisi kernel-tasolla, se toimisi samalla tai alemmalla tasolla kuin mikään rootkittien tunnistamiseen käytetty ohjelma. Kernel-tason rootkittien takia havaitseminen muuttui kissa-hiiri-leikiksi hyökkääjien ja tutkijoiden välillä. (Shields 2008, 2.)

2000-luvun alussa rootkittien havaitseminen muuttui jälleen kerran, kun virtualisointitekniikoissa oli saatu aikaan läpimurto. Virtuaalikoneiden avulla rootkittejä pystyttiin havaitsemaan kernel-tasoa alemmalla tasolla, virtualisointitasolla. Vastaavasti myös hyökkääjät pystyivät käyttämään rootkitteja virtualisointitasolla. Nykyään tutkijat ovat huolissaan että rootkitteja on myös olemassa virtualisointitasoa alemmalla tasolla, laiteohjelmistotasolla. (Shields 2008, 2.)

2.8.2 Käyttökohteet ja tyypit

Rootkitit hyödyntävät erilaisia tekniikoita, joilla järjestelmä saadaan kaapattua. Rootkit asentuu kohdetietokoneeseen, joko automaattisesti toisen ohjelman rinnalla tai hyökkääjän toimesta, pääkäyttäjän tai järjestelmänvalvojan oikeuksilla. Oikeudet hyökkääjä saa joko sosiaalisella manipuloinnilla, hyödyntämällä tunnettuja tai tuntemattomia tietoturva-aukkoja tai eskalaatioaukoilla. Kun rootkit on asennettu kohdetietokoneeseen onnistuneesti, sillä pystytään piilottamaan tunkeutumisen jäljet ja ylläpitämään hyökkääjän ylemmän tason oikeuksia. (Shields 2008, 2-3.)

Rootkitit voivat haittakäytössä:

- Antaa hyökkääjälle pääsyn kohdetietokoneeseen takaoven kautta
- Tehdä kohdetietokoneesta zombien ja liittää sen osaksi olemassa olevaa botti-verkkoa (Wikipedia: Rootkit.)
- Piilottaa haittaohjelmia, kuten keyloggerin tai viruksen (Russinovich 2005.)
- Mahdollistaa digitaalisten oikeuksien hallinnoinnin toimeenpanemisen (Russinovich 2006).

Joissakin tapauksissa rootkitit voivat olla myös hyödyllisiä. Hyötykäytössä rootkitit voivat:

- Piilottaa huijaamisen Internet peleissä huijauksenesto ohjelmilta (Lemos 2005.)
- Havaita hyökkäyksiä, esim. honeypotissa (Rose 2003.)
- Vahvistaa emulointi- ja tietoturvaohjelmistojen toimintoja (Russinovich 2006.)
- Toimia piilotettuna varkaudenestojärjestelmänä (Ortega & Sacco 2009)
- Mahdollistaa Microsoft tuoteaktivoinnin kiertämisen (Kleissner 2009).

Rootkitteja on olemassa ainakin viittä eri tyyppiä; ohjelmistotaso, kirjastotaso, kerneltaso, virtualisointitaso ja laiteohjelmistotaso. (Shields 2008, 2.)

2.8.2.1 Ohjelmistotaso

Ohjelmistotason rootkitit korvaavat kohdetietokoneessa normaalit järjestelmäbinäärit rootkitin omilla, uudelleen käännetyillä binääreillä tai ne muuttavat olemassa olevien sovelluksien käyttäytymistä päivityksillä tai injektoimalla niihin koodia. (Shields 2008, 3.)

2.8.2.2 Kirjastotaso

Kirjastotason rootkitit päivittävät, kaappaavat tai korvaavat järjestelmän kirjastoihin tehtyjä kutsuja. Tämän tyyppistä rootkittia käyttämällä, hyökkääjä pystyy salaamaan hyökkäysprosessin olemassaolon vastaamalla muokatuilla tiedoilla kutsuihin, jotka paljastaisivat hyökkäysprosessin olemassaolon. Suurin ero kirjastotason rootkittien ja ohjelmistotason rootkittien välillä on se, että kirjastotason rootkitit vaikuttavat useaan jär-

jestelmän binääriin ainoastaan muokkaamalla muutamaa kirjastoa. Tämän takia kirjastotason rootkittien on helppo piiloutua havaitsemiselta, koska ne eivät tee järjestelmään silminnähtäviä muutoksia. (Shields 2008, 3.)

2.8.2.3 Kernel-taso

Kernel-tason rootkitit saattavat lisätä uutta tai muuttaa olemassa olevaa koodia käyttöjärjestelmän ytimessä. Tämä on mahdollista suorittaa muokattujen laiteajurien kautta Windowsissa tai ladattavien kernel-moduulien (LKM) avulla Unix järjestelmissä. On erittäin todennäköistä että tämän tyyppinen rootkit aiheuttaa järjestelmässä epävakauksia, koska se muokkaa käyttöjärjestelmän ytimen toimintaa. Kernel-tason rootkittejä on vaikea löytää koska ne toimivat samalla käyttöoikeustasolla kuin itse käyttöjärjestelmä. (Shields 2008, 3-4.)

Kernel-tason rootkitteihin lukeutuu myös bootkit rootkitit. Ne korvaavat tai muuttavat alkuperäisen bootloaderin. Tietokoneen käynnistyksen yhteydessä bootloader ajetaan ennen käyttöjärjestelmää, jonka johdosta rootkit aktivoituu ennen kuin käyttäjä on päässyt käyttöjärjestelmään. Bootkitit ovat vakava tietoturvauhka, koska niitä käytetään salausavaimien ja salasanojen kaappaamiseen. (Schneier 2009.)

2.8.2.4 Virtualisointitaso

Virtualisointitason rootkitit ovat, poislukien laiteohjelmistotason rootkitit, alimman tason rootkittejä. Ne toimivat itse varsinaista käyttöjärjestelmää alemmalla tasolla. Virtualisointitason rootkitillä saastutettu järjestelmä voi muokata alkuperäistä käynnistysjärjestystä tai siirtää koko käyttöjärjestelmän rootkitin virtualisointialustaan ilman uudelleenkäynnistystä. Kun saastutettu järjestelmä uudelleenkäynnistetään, järjestelmä lataa ensiksi virtualisointitason rootkitin, joka vuorostaan lataa käyttöjärjestelmän. Hyökkääjän käyttämän virtualisointitekniikan ansiosta saastuneen järjestelmän käyttäjät eivät ikinä tiedä käyttävänsä virtuaalikonetta (VM). Virtualisoinnin takia virtualisointitason rootkitit pystyvät kaappaamaan kaikki käyttöjärjestelmän tekemät laitteistokutsut. (Shields 2008, 4.)

Virtualisointitason rootkittejä on olemassa kahdenlaisia, ohjelmistopohjaisia ja laitteistoavusteisia virtuaalikone-rootkittejä. Ohjelmistopohjaiset virtualisointitason rootkitit käyttävät virtuaalikonevalvojaa (VMM) laitteiston resurssien hallintaan. VMM myös emuloi laitteistotason rajapinnan yhdelle tai useammalle virtuaalikoneelle. VMM toimii yhdyksenä asennetulle VM:lle ja alla olevalle laitteistotasolle. Sijoittamalla VM:n koko alkuperäisen käyttöjärjestelmän alle ja emuloimalla laitteistoa ohjelmiston kautta, on mahdollista kaapata kaikki laitteistokutsut ja välittää takaisin vääristettyä tietoa. Lopputuloksena on rootkit, joka toimii sellaisella tasolla, jota alkuperäinen käyttöjärjestelmä ei käytännössä pysty havaitsemaan. (Shields 2008, 4.)

Laitteisto avusteiset virtuaalikone -rootkitit ovat samanlaisia kuin ohjelmistopohjaiset virtualisointitason rootkitit. Ne toimivat yhtä tasoa alempana kuin itse käyttöjärjestelmä ja ovat täten lähes mahdottomia havaita ylempänä toimivan käyttöjärjestelmän osalta. Ohjelmistopohjaisista virtualisointitason rootkiteistä poiketen, ne lataavat itsensä suoraan käynnissä olevan käyttöjärjestelmän alle ja muuttavat käyttöjärjestelmän itselleen vierailija VM:ksi. Tämän mahdollistaa laitteisto, joka itse tukee virtualisointiteknologioita, kuten AMD-V tai Intel VT. (Shields 2008, 4-5.)

2.8.2.5 Laiteohjelmistotaso

Laihteohjelmistotason rootkitit toteutetaan laitteistotasolla. Laitteiston koodia muokkaamalla hyökkääjä voi suunnitella haittaohjelman haluamansa mukaan ja samalla pitää sen erittäin vaikeasti havaittavana. Laiteohjelmistotason rootkitin voi sijoittaa esimerkiksi oheislaitteisiin, levyohjaimiin, USB-muistitikkuihin, prosessoreihin jne. (Shields 2008, 4.)

Laiteohjelmistotason rootkittien ideana on, että laiteohjelmistoa voidaan muokata suoraan käyttöjärjestelmästä. Erityisesti BIOS, ACPI, ROM-moduulien ja verkkokorttien PXE-järjestelmiä voidaan muuttaa ajamalla koodia hallinnollisilla oikeuksilla. Useissa tapauksissa nämä laiteohjelmistot käynnistetään tietokoneen käynnistyksen yhteydessä, ennen varsinaista käyttöjärjestelmää. Tämän johdosta laiteohjelmistotason rootkit voi hookata keskeytyksiä, joita käyttöjärjestelmä voi kutsua myöhemmin. On esimerkiksi mahdollista hookata videokeskeytys ja muokata ohjelman suorittamista keskeytyksien suorittamisen perusteella, laiteohjelmiston avulla. (Shields 2008, 4.)

Laiteohjelmistotason rootkittien poistaminen on erittäin vaikeata. Käyttöjärjestelmän uudelleenasennus, kiintolevyn ylikirjoittaminen tai uuden tallennuslaitteen käyttöönottaminen eivät poista haitallista koodia. Laiteohjelmisto, joka sisältää itse rootkitin, pitää palauttaa alkuperäiseen tilaan, jotta rootkit saadaan poistettua. (Shields 2008, 4.)

2.8.3 Tunnistamismenetelmät

Rootkittien tunnistaminen on erityisen vaikeaa, varsinkin jos ne toimivat kernel-tasolla. Kernel-tason rootkitit kykenevät muuttamaan ohjelmien toimintoja, mukaan lukien tietoturvaohjelmien. Ei voida luottaa että saastunut käyttöjärjestelmä kykenee tunnistamaan itseensä tai sen komponentteihin tehtyjä luvattomia muutoksia. Toiminnot, kuten käynnissä olevien prosessien listaaminen tai kansiossa olevien tiedostojen listaaminen, voivat toimia normaalista poiketen. Toisin sanoen, saastuneessa koneessa käytettävät rootkittien tunnistustyökalut toimivat ainoastaan sellaisia rootkitteja vastaan, joilla on jokin heikkous naamioinnissa tai jos ne toimivat alemmalla käyttöoikeustasolla kuin itse kernel-tasolla toimiva tunnistustyökalu. (Shields 2008, 5.)

Rootkittien tunnistamiseen on monia eri tapoja, kuten allekirjoitukseen perustuva tunnistus, eheydentarkistaminen, eroavaisuuspohjainen tunnistus ja heuristinen tunnistus. (Shields 2008, 5.)

2.8.3.1 Offline-tunnistus

Tehokkain tunnistustapa käyttöjärjestelmäkerroksen rootkittien tunnistamiseen on niin sanottu offline-tunnistaminen. Siinä saastunut kone sammutetaan ja sen muisti tarkistetaan käyttämällä vaihtoehtoista, luotettavaa järjestelmää, kuten pelastuslevyä. Tällä tavoin saastuneen koneen muistissa oleva rootkit ei pysty piiloutumaan vaihtoehtoiselta järjestelmältä, koska rootkit ei ole aktiivisessa tilassa. (Shields 2008, 5.)

2.8.3.2 Heuristinen tunnistus

Järjestelmän poikkeava käyttäytyminen voi johtua rootkitistä. Esimerkiksi kiintolevyn poikkeava vapaantilan määrä voi osoittaa levyn sisältävän dataa jota järjestelmä ei raportoi käyttäjälle. Käyttäytymiseen perustuva tunnistus on mahdollista kun rootkit tekee työnsä puutteellisesti. Tietotekniikassa heuristiset menetelmät ovat välillä virhealttiita. Vaikkakin käyttäytymiseen perustuva tunnistus ja heuristinen tunnistus perustuvat rootkitin käyttäytymisen seurantaan ja analysointiin, sisältävät menetelmät silti valitettavan usein arvailua, joten ne eivät ole erehtymättömiä. (Shields 2008, 6.)

2.8.3.3 Allekirjoitukseen perustuva tunnistus

Allekirjoitukseen perustuva rootkittien tunnistus perustuu aikaisemmin tunnistetuista rootkiteistä tehtyyn allekirjoitustietokantaan. Tunnistusmenetelmässä kohdekäyttöjärjestelmä skannataan skannaustyökalulla, joka etsii järjestelmästä merkkejä ennaltatiedetyistä allekirjoituksista. Allekirjoitukseen perustuva tunnistus on rajallinen, koska se ei kykene löytämään uusia rootkit tyyppejä joista ei ole vielä tehty allekirjoitusta. Menetelmä on kuitenkin erittäin helppo toteuttaa ja käyttää, verrattuna muihin menetelmiin. (Davis, Bodmer & LeMasters 2009, 285-286.)

2.8.3.4 Eroavaisuuspohjainen tunnistus

Eroavaisuuspohjaisessa tunnistuksessa yksinkertaisesti vertaillaan haluttuja kohteita keskenään. Esimerkiksi levyllä olevaa järjestelmän käyttämää binääriä voidaan verrata käyttömuistissa olevaan kopioon, jonka pitäisi olla identtinen, jos se ei ole saastunut. (Davis, Bodmer & LeMasters 2009, 286-288.)

2.8.3.5 Eheydentarkistaminen

Luomalla kopion koko tiedostojärjestelmästä tai osasta siitä, tai luomalla salaustiivisteen osasta tiedostojärjestelmän sisällöstä, voidaan niitä myöhemmin verrata sen hetkisen tiedostojärjestelmän tilaan ja selvittää onko järjestelmään tehty luvattomia muutok-

sia. Tämä tapa on yksi tehokkaimmista tavoista havaita rootkit, mutta se on kaikkein vaikein luoda ja käyttää, koska se sisältää erittäin suuren määrän muuttuvia tekijöitä. Toisaalta tämä tapa on vähiten virhealtis. (Perrin 2007.)

2.8.4 Ennakkotapaukset

Vaikka rootkitit ovatkin olleet olemassa yli toistakymmentä vuotta, nousivat ne normaalien tietokonekäyttäjien tietoisuuteen vasta 2000-luvulla.

2.8.4.1 Kreikan salakuunteluskandaali

Vuosina 2004 ja 2005 useiden parlamentin jäsenten, puolustusvoimien työntekijöiden, yhden Amerikan suurlähetystön työntekijän ja muutaman liikemiesten puhelimia salakuunneltiin. Kreikkalaiset ovat syyttäneet tapauksesta amerikkalaisia, koska he uskovat salakuuntelun liittyneen vuoden 2004 olympialaisten turvallisuuteen. Salakuuntelu oli toteutettu asentamalla Ericssonin valmistamiin puhelinkeskuksiin rootkit, jonka avulla salakuunteluohjelman olemassaolo pystyttiin salaamaan. Rootkitin olemassaolo huomattiin vasta vuonna 2005 erään päivityksen yhteydessä. Päivityksen johdosta asiakkaat eivät pystyneet lähettämään tekstiviestejä, jonka takia Vodafone Greece otti yhteyttä Ericssoniin ja lähetti heille puhelinkeskuksissa käytetyt laiteohjelmistot. (Academic: Greek telephone tapping case 2004-2005.)

2.8.4.2 Sony BMG kopiointisuojaus

Vuonna 2005 rootkitit saivat erittäin laajaa huomiota, kun Sony BMG oli käyttänyt kahta uutta kopiointisuojausohjelmaa, XCP ja MediaMax CD-3, eri artistien albumeissa. Kopiointisuojausohjelma asentui käyttäjän tietämättä hänen koneeseensa kun hän kuunteli levyä ensimmäistä kertaa. (Gibbs 2005.)

Sony BMG rootkit huomattiin 2005 lokakuussa Mark Russinovichin toimesta. Valitettavasti Sony BMG reagoi rootkitin aiheuttamaan mediamyrskyyn vasta, kun haittaohjelmien tekijät olivat ruvenneet hyödyntämään Sony BMG rootkittiä. Myöhemmin Sony

BMG julkaisi työkalun, jolla rootkitin naamiointitekniikka saatiin poistettua käytöstä, mutta itse rootkittiä työkalu ei poistanut. Lisäksi työkalu avasi käyttäjän koneeseen erittäin suuren tietoturva-aukon. Sony BMG globaalin liiketoiminnan puheenjohtaja kommentoi rootkitistä aiheutunutta kohua sanomalla, ”Useimmat ihmiset eivät edes tiedä mikä rootkit on, joten miksi heidän pitäisi välittää siitä”. (Schneier 2005.)

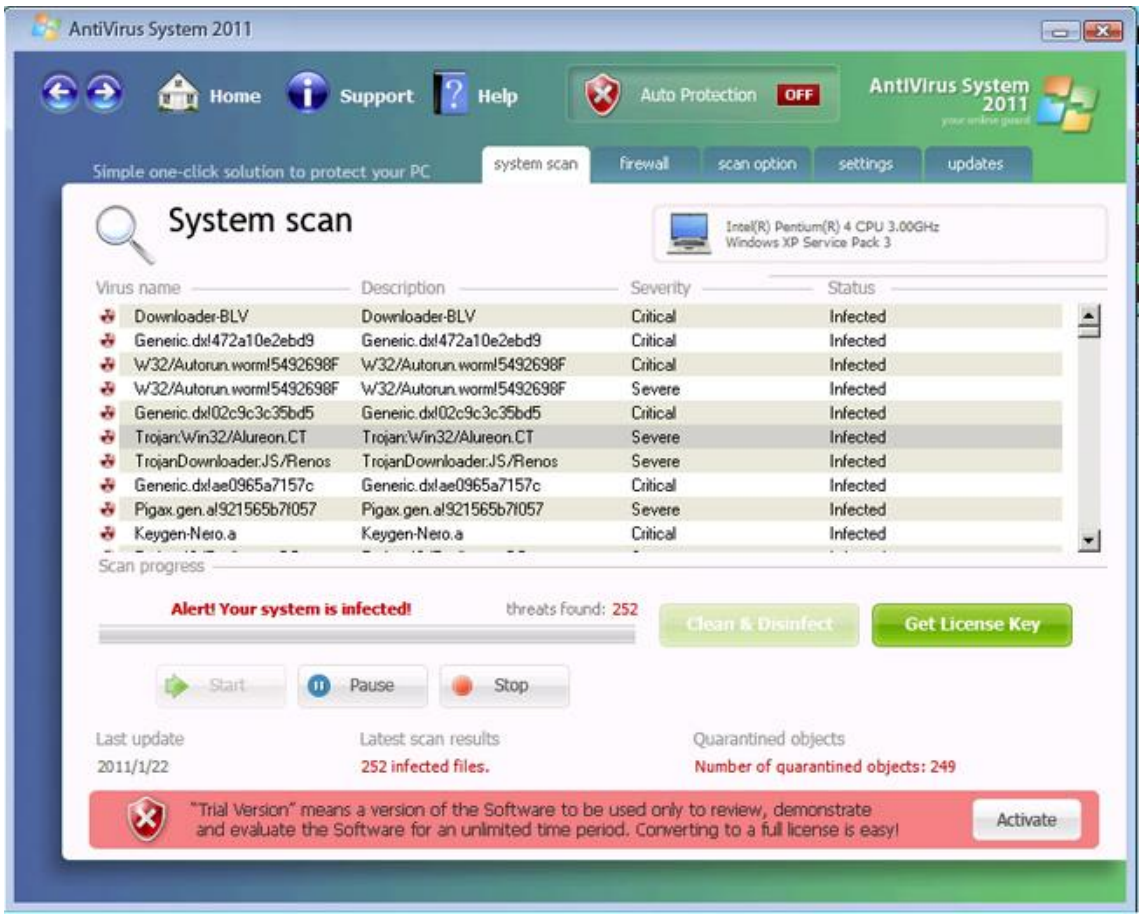
2.8.4.3 Stuxnet-mato

Stuxnet oli maailman ensimmäinen rootkitillä varustettu mato, jonka kohteena olivat tuotantojärjestelmät. Stuxnet saastutti Windows koneiden lisäksi, Siemensin ohjausjärjestelmiä. Se havaittiin ensimmäistä kertaa Iranissa vuonna 2010. Stuxnetin on epäilty olevan ohjelmoitu Iranilaisten ydinohjelman vakoilemista ja sabotointia varten. (McMillan 2010.)

2.9 Scareware-peloteohjelma

Scareware, eli niin sanottu peloteohjelmisto, on uudehko ja huomattavasti viime vuosina huomiota herättänyt haittaohjelmatyyppi. Peloteohjelmien toiminta perustuu uhrin sosiaaliseen manipulointiin pelottelun ja uhkailun avulla. Scarewarea kutsutaan myös nimellä rogueware, arvaamaton ohjelmisto.

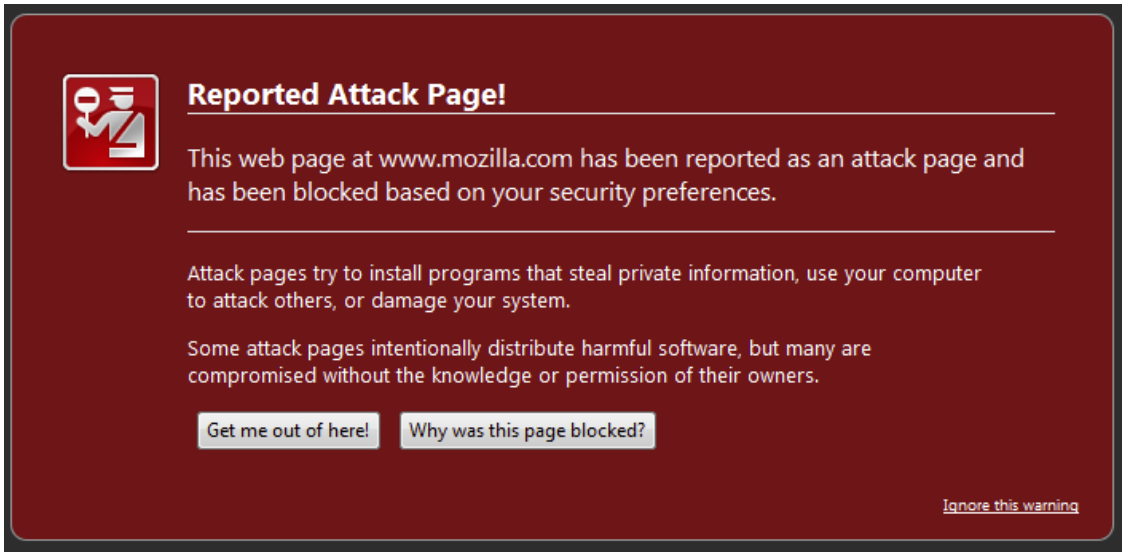
Haittaohjelmien tekijät pyrkivät yleensä naamioimaan peloteohjelman ammattimaisen virustorjuntaohjelman näköiseksi (kuva 2), jotta käyttäjä ei kykenisi huomaamaan että hän on asentanut ja on käyttämässä haittaohjelmaa. (Microsoft: Watch out for fake virus alerts.)



KUVA 2. Antivirus System 2011 rogueware (Information Security Office: Examples of Rogue Security Software.)

Peloteohjelman lataamista ja asennusta voivat ehdottaa esimerkiksi satunnaisella sivustolla ilmestyvät aggressiiviset ilmoitukset, joissa kerrotaan käyttäjän koneen olevan alttiina tietoturvauhille ja häntä suositellaan asentamaan ilmoituksessa oleva ohjelma, jolla tietoturvauhat saadaan poistettua tai estettyä (kuva 3 ja kuva 4). Peloteohjelma voi esimerkiksi asennuksen jälkeen suorittaa valeviruksentarkastuksen, joka ilmoittaa käyttäjälle valheellisesti koneessa olevista viruksista. Tällaisen pelotteen jälkeen peloteohjelma yrittää saada käyttäjää päivittämään ohjelman maksulliseen versioon, jotta virukset saataisiin poistettua. Käyttäjä voi pahimmassa tapauksessa menettää myös rahallisen summan lisäksi luottokorttitietonsa, jos hän erehtyy maksamaan ohjelman päivityksestä. (Microsoft: Watch out for fake virus alerts.)

KUVA 3. Väärennetty Firefoxin tietoturvaviesti (Correll 2010.)



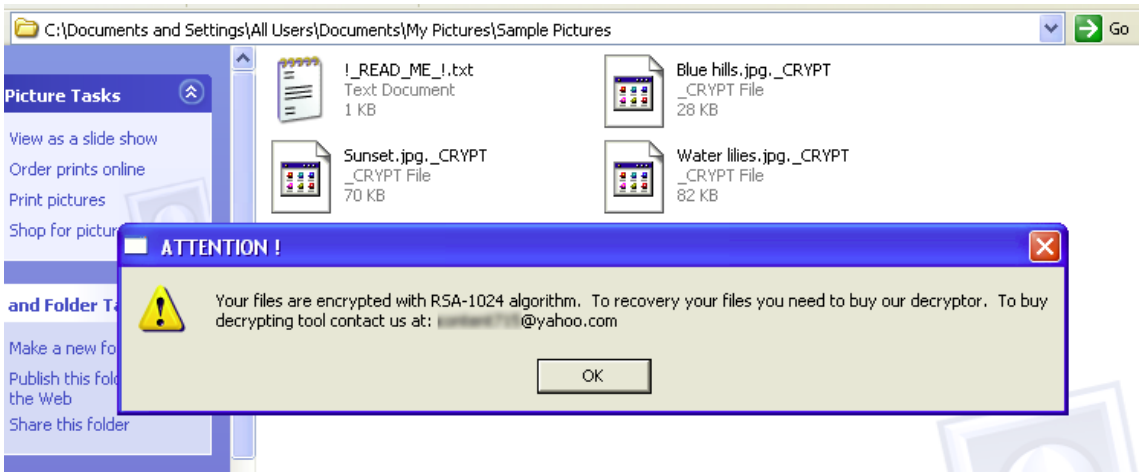
KUVA 4. Aito Firefoxin tietoturvaviesti (Information Security Office: Examples of Fradulent Security Warnings.)

Taloudellisen huijauksen lisäksi peloteohjelmat voivat:

- Estää joidenkin käyttöjärjestelmätoimintojen toimimisen
- Poistaa toimivan viruksentorjuntaohjelmiston
- Kaappaa henkilökohtaisia tietoja
- Hidastaa tietokoneen toimintaa tai korruptoida tiedostoja
- Estää käyttöjärjestelmän ja virustorjuntaohjelmiston päivitystiedostojen lataamisen (Microsoft: Watch out for fake virus alerts).

2.10 Ransomware-lunnasohjelma

Ransomware, jota joissakin tapauksissa kutsutaan salausvirukseksi, -madoksi tai -trojaniksi, on haittaohjelmatyyppi, joka rajoittaa käyttäjän tietokoneen käyttöä. Rajoitukset käyttäjä saa poistettua, kun hän maksaa haittaohjelman vaatimat lunnaat. Ransomware haittaohjelmat voivat esimerkiksi salata tietyn päätteisiä tiedostoja tehokkaalla salauksella (kuva 5), tai esittää käyttäjälle perättömiä uhkauksia tai vaateita (kuva 6). Ransomwaren toiminta perustuu pitkälti samoihin menetelmiin, kuin scarewaren toiminta. (Kassner 2010.)



KUVA 5. Salausta käyttävä ransomware (Tromer: Gpcode.ak Crypthographic Challenge.)

KUVA 5. Uhkausta käyttävä ransomware (Danchev 2010.)

3 VERKKOHYÖKKÄYSTEKNIIKAT

3.1 Network attack-verkkohyökkäys

Verkkohyökkäys on toiminta, jossa tietoverkon ja siihen kytkettyjen laitteiden välistä verkkoliikennettä heikennetään, häiritään, estetään, kaapataan, tuhotaan tai muutetaan. Verkkohyökkäys kohdistuu myös tietoverkkoon kytkettyjen laitteiden sisältämään tietoon.

3.2 Sniffer attack-verkkoanalysaattorihyökkäys

Snifferit, toiselta nimeltä verkkoanalysaattorit, ovat laitteita tai ohjelmia, joiden avulla pystytään nuuskimaan ja analysoimaan verkon liikennettä. Ne ovat tietoturvan kannalta kaksiteräinen miekka, niitä voidaan käyttää sekä hyvään että huonoon tarkoitukseen. (Valente 1996.)

Snifferit ovat verkon ylläpitäjille ja valvojille erittäin käytännöllisiä työkaluja, varsinkin suurissa verkoissa, koska niitä käyttämällä saadaan yksityiskohtaista tietoa kohdeverkosta ja sen käyttäjistä. (Colasoft: Network Sniffer Introduction.)

Niiden avulla pystytään esimerkiksi:

- Analysoimaan verkko-ongelmia
- Havaitsemaan tunkeutumisyrityksiä ja verkon väärinkäyttöä
- Eristämään saastuneita laitteita
- Seuraamaan kaistan käyttöä
- Seuraamaan liikkeellä olevaa dataa
- Seuraamaan verkon käyttöä
- Keräämään ja raportoimaan verkon statistiikasta
- Suodattamaan epäilyttävää sisältöä verkosta (Colasoft: Network Sniffer Introduction).

Valitettavasti sniffereitä voidaan käyttää haittatarkoituksessa samaan tarkoitukseen, kuin verkon ylläpidossa. Erona on kuitenkin se, että haittatarkoituksessa hyökkääjällä ei

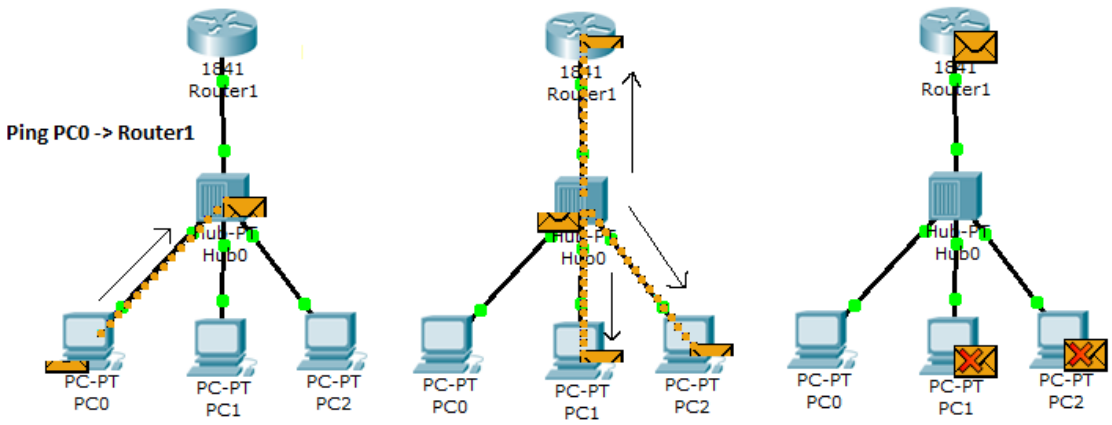
ole käsitystä kohdeverkon topologiasta ja laitteistosta, fyysistä pääsyä kohteeseen ja hänen tulee pyrkiä salaamaan snifferin olemassa olo. Lisäksi, jotta hyökkääjä voi asentaa snifferin altistettuun koneeseen, täytyy hyökkääjällä olla pääsy laitteeseen Internetin kautta tai fyysisesti. Snifferin avulla hyökkääjä voi helposti selvittää salaamattomia käyttäjätunnuksia ja salasanoja ja etsiä kohdeverkosta mahdollisia tietoturva-aukkoja, joiden avulla pystytään etenemään verkossa. (Valente 1996.)

Verkon ylläpitäjien ongelmana altistetussa verkossa on hyökkääjän käyttämän snifferi havaitseminen. Hyökkääjä voi esimerkiksi alustavasti tunkeutuessaan verkkoon asettaa snifferin kuuntelutilaan, jolloin se kerää verkossa olevien laitteiden IP-tietoja, MAC-osoitteita, käyttäjätunnuksia ja salasanoja. Tällä tavoin snifferin ei käytä merkittävästi altistetun koneen resursseja tai aiheuta merkittävää viivettä verkkoliikenteeseen. (Valente 1996.)

3.3 Eavesdropping-salakuuntelu

Salakuuntelu on yksinkertaisin verkkohyökkäysmuoto. Hyökkäys tapahtuu OSI-mallin verkkokerroksella, jossa verkossa olevien tietokoneiden lähettämiä paketteja siepataan ja niiden sisältöä luetaan. Salakuuntelu perustuu vahvasti verkkoanalysaattorien käyttöön. (SHALB 2008.)

Salakuuntelu on helpointa Ethernet-verkossa, jossa käytetään ainoastaan keskittimiä. Keskitin lähettää jokaisen vastaanotetun paketin ulos kaikista, paitsi vastaanottaneesta portista (kuva 6). (SHALB 2008.)



KUVA 6. Keskittimen toiminta

3.4 Data modification-tiedon muuttaminen

Tiedon muuttamisella tarkoitetaan verkon sisällä liikkuvan tiedon muuttamista. Jos hyökkääjä on onnistunut lukemaan verkkoliikennettä, niin hänen mahdollinen seuraava askel on liikkuvan tiedon muuttaminen. Hyökkääjä voi esimerkiksi muuttaa oston yhteydessä ostostietoja, jos liikennettä ei ole salattu. (Microsoft: Common Types of Network Attacks.)

3.5 Spoofing attack-väärennöshyökkäys

Väärennöshyökkäyksessä hyökkääjä kuuntelee ja analysoi lähettäjän ja vastaanottajan välistä verkkoliikennettä. Tämän jälkeen hyökkääjä käyttää saamiaan tietojaan tietoverkon huijaamiseksi, naamioidakseen itsensä lailliseksi osaksi tietoverkkoa. (Graves 2010, 183.)

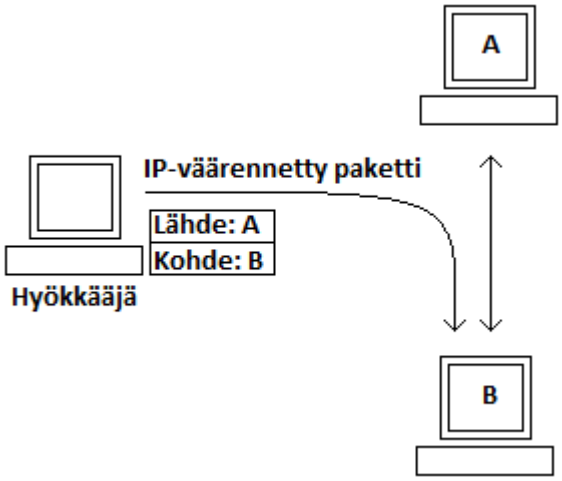
3.5.1 ARP spoofing-ARP-väärennös

Osoitteen selvitys protokollaa käyttämällä tietoverkko kykenee kääntämään IP-osoitteen MAC-osoitteeksi. Kun yksi Ethernet-verkossa oleva laite haluaa muodostaa yhteyden toiseen verkon laitteeseen, tarvitsee yhteyttävä muodostava laite kohdelaitteen MAC-osoitteen. Ensimmäiseksi yhteyttä yrittävä laite tarkistaa omasta ARP-taulukostaan kohdelaitteen MAC-osoitteen. Jos kohdelaitteen MAC-osoitetta ei ole ARP-taulukossa, yhteyttä yrittävä laite lähettää ARP-kyselyn, jossa kysytään onko jollakin IP-osoitetta jota etsitään. Jos jokin Ethernet-verkon laitteista tietää kyseisen IP-osoitteen, niin se lähettää ARP-vastausviestissä oman MAC-osoitteensa. (Graves 2010, 159.)

ARP-väärennöksessä lähetetään väärennettyjä ARP-viestejä Ethernet-verkkoon. Nämä viestit sisältävät väärennettyjä MAC-osoitteita, jotka sekoittavat verkkolaitteita, kuten kytkimiä. Tämän seurauksena viestit, joiden pitäisi päätyä laitteelle A, päätyvätkin esim. laitteelle B tai saavuttamattomaan osoitteeseen. ARP-väärennöstä voidaan myös käyttää mies välissä -hyökkäyksissä, jossa kaikki verkkoliikenne ohjataan kulkemaan hyökkääjän kautta ARP-väärennöksillä. Tätä kutsutaan yhdyskäytävän väärentämiseksi. (Graves 2010, 159.)

3.5.2 IP addresss spoofing-IP-osoitteen väärentäminen

IP-osoitteen väärennöksessä korvataan IP-pakettien lähdeosoite väärennetyllä IP-osoitteella. Lähdeosoite on sen laitteen osoite, mistä IP-paketti alun perin lähetettiin. Lähdeosoitetta muuttamalla hyökkääjä voi esittää että paketin lähetti toinen laite. Tämän avulla hyökkääjä pystyy piilottamaan identiteettinsä. (Verma 2012.)



KUVA 7. IP-väärennöksen toiminta

Kuvassa 7 on kaksi tietokonetta, A ja B, jotka kommunikoivat keskenään. Samaan aikaan hyökkääjä yrittää myös kommunikoida tietokoneen B kanssa, väärentämällä lähetettävän IP-paketin lähdeosoitteen. Kun tietokone B vastaanottaa IP-paketin, se luulee sen tulleen tietokoneelta A. (Verma 2012.)

IP-osoitteen väärentämistä käytetään esimerkiksi väärennettyjen sähköpostien, pyyntöjen ja muiden tietojen lähettämiseen. Hyökkääjät käyttävät usein IP-osoitteen väärentämistä roskapostituksessa ja palvelunestohyökkäyksissä. (Verma 2012.)

3.5.3 DNS spoofing-DNS-väärennös

DNS-väärennöksellä pystytään huijaamaan DNS-palvelinta luulemaan, että se on vastaanottanut luotettavaa tietoa, vaikka todellisuudessa se ei ole. Kun tietokoneen käyttäjä yrittää käydä Internet-sivustolla, sivuston verkkotunnuksesta lähetetään DNS-kysely DNS-palvelimelle, jotta sen IP-osoite saadaan selvitettyä. Jos DNS-palvelin on vaaran-

tunut, käyttäjä ohjataan Internet-sivustolle, jolla hän ei ole halunnut vierailla. (Graves 2010, 164.)

DNS-väärennöshyökkäyksen suorittamiseksi hyökkääjä hyväksikäyttää DNS-palvelimen ohjelmiston heikkouksia. Mikäli DNS-palvelin ei varmista DNS-päivityksien aitoutta, se tulee vastaamaan verkon käyttäjien kyselyihin väärennetyillä tiedoilla. (Graves 2010, 165.)

3.5.4 DHCP spoofing-DHCP-väärennös

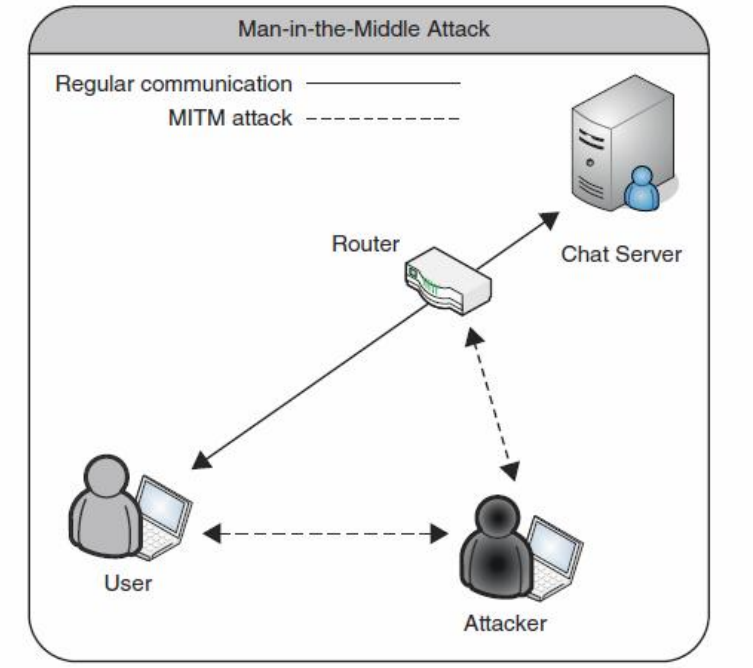
Yksi hyökkäystapa, jolla hyökkääjä voi päästä käsiksi verkkoliikenteeseen, on aidon DHCP-palvelimen lähettämien DHCP-vastausviestien väärentäminen. Laite, jota hyökkääjä käyttää DHCP-väärennöksiin, vastaa käyttäjien lähettämiin DHCP-pyyntöihin. Myös aito DHCP-palvelin voi vastata kyselyihin, mutta jos DHCP-väärennöksiin käytettävä laite on samalla verkkosegmentillä kuin itse aito DHCP-palvelin, voivat väärennetyt DHCP-vastausviestit saapua käyttäjille ensiksi. Väärennetyt DHCP-vastausviestit sisältävät IP-osoitteen ja muuta välttämätöntä tietoa, jotka osoittavat hyökkääjän käyttämän DHCP-väärennöslaitteen tietoverkossa oletusyhdyskäytäväksi tai DNS-palvelimeksi. Jos hyökkääjän käyttämä laite toimii oletusyhdyskäyvänä, käyttäjien lähettämät paketit kulkeutuvat hyökkääjän käyttämän laitteen kautta pakettien osoittamaan päämäärään. Tällaista tilannetta kutsutaan mies välissä -hyökkäykseksi. (Levis 2008, Chapter 2 - Spoofing Attacks.)

3.6 Man-in-the-Middle attack-mies välissä -hyökkäys

Mies välissä (MITM) -hyökkäys, on ollut pitkään yksi tehokkaimmista hyökkäysvektoreista. Käsitteenä mies välissä -hyökkäys on vanha, mutta uusien teknologioiden ansiosta keksitään jatkuvasti uusia tapoja ja tekniikoita sen suorittamiseen. Mies välissä -hyökkäyksessä kolmas osapuoli asettaa itsensä viestiyhteyden väliin. Tämän johdosta salakuuntelu, viestien sieppaaminen ja muokkaaminen on mahdollista. Klassisin ja yksinkertaisin esimerkki mies välissä -hyökkäyksestä, on puhelinsalakuuntelu. (Borkin, Kraus & Prowell 2010, 101.)

3.6.1 Toimintaperiaate

Kuvassa 8:n on kuvaus hyvin yksinkertaisesta MITM-hyökkäyksestä. Kuvassa yhtenäiset viivat kuvaavat normaalia verkkoliikenteen kulkua käyttäjän ja chat-palvelimen välillä. Normaalisti käyttäjältä lähtevät viestit kulkevat käyttäjän tietokoneelta reitittimelle ja siitä chat-palvelimelle. Kun tarvittavat protokollat ovat alustaneet keskusteluun vaadittavat tarpeet, käyttäjä, eli Chat-asiakas ja Chat-palvelin voivat aloittaa tietojen siirtämisen keskustelun mahdollistamiseksi. (Borkin, Kraus & Prowell 2010, 103.)



KUVA 8. Yksinkertainen mies välissä -hyökkäys (Borkin, Kraus & Prowell 2010, 103.)

Kuvassa 8:n olevat katkoviivat esittävät MITM-hyökkäystä. Hyökkääjä käyttää eri tekniikoita verkkoliikenteen uudelleenreitittämistä varten. Viime kädessä, hyökkääjä haluaa reitittää kaiken tietoliikenteen oman tietokoneensa kautta, jotta tietojen analysointi ja muuttaminen on mahdollista. Ensimmäiseksi hyökkääjä suorittaa hyökkäyksen, jolla huijataan käyttäjän tietokonetta luulemaan hyökkääjän konetta reitittimeksi. Sen jälkeen hyökkääjä suorittaa uuden hyökkäyksen, jolla huijataan reititintä luulemaan hyökkääjän tietokonetta käyttäjän tietokoneeksi. Kun hyökkääjä on suorittanut molemmat hyökkäykset onnistuneesti, verkkoliikenne reitittyy kulkemaan hyökkääjän tietokoneen kautta. Tämän jälkeen hyökkääjä voi analysoida ja muokata tietoja, joita ainoastaan käyttäjän tietokoneen, reitittimen ja chat-palvelimen pitäisi nähdä. (Borkin, Kraus & Prowell 2010, 103-104.)

3.6.2 Hyökkäystavat

MITM-hyökkäys voidaan suorittaa useilla eri tekniikoilla, riippuen hyökkääjän pääsystä kohdeverkkoon ja hyökkäyksessä käytettävistä protokollista. Hyökkääjän käyttämiä tekniikoita ovat esimerkiksi:

- Paikallisverkossa
    - ~ ARP spoofing
    - ~ DNS spoofing
    - ~ IP spoofing
    - ~ Port stealing
    - ~ STP mangling (Yang & Bhatia 2008).

- Paikallisisännästä etäisäntään (oletusyhdyskäytävän kautta)
    - ~ ARP spoofing
    - ~ DNS spoofing
    - ~ DHCP spoofing
    - ~ Gateway spoofing
    - ~ ICMP redirection
    - ~ IRDP spoofing (Yang & Bhatia 2008).

- Etäisäntänä
    - ~ DNS spoofing
    - ~ IRDP spoofing
    - ~ Traffic tunneling (Yang & Bhatia 2008).

3.7 Compromised-Key attack-vaarantunut avain -hyökkäys

Salakirjoitusavaimella voidaan varmistaa viestin eheys tai salata viestin sisältö. Salakirjoitusavaimia on olemassa useita erilaisia. Yksi salakirjoitusavaimien tyyppi on jaettu salaisuus. Tietokone joka lähettää viestin toiselle tietokoneelle, salaa viestin sisällön jaetulla salaisuudella. Vastaanottava tietokone taasen purkaa viestissä olevan salauksen samalla jaetulla salaisuudella. Jaettua salaisuutta ei koskaan lähetetä verkon yli. (Shinder 2011.)

Toinen salausavaimien tyyppi on yksityinen avain. Yksityisellä avaimella voidaan vahvistaa lähettäjän identiteetti. Tätä kutsutaan viestin allekirjoittamiseksi. Kun vastaanottaja vastaanottaa yksityisavaimella allekirjoitetun viestin, voi vastaanottaja olla varma, että viestin lähettäjä on todellakin lähettänyt kyseisen viestin. (Shinder 2011.)

Jos hyökkääjä pääsee jotenkin käsiksi salakirjoitusavaimiin, voi hyökkääjä kommunikoida oletetulla identiteetillä, käyttämällä jonkun toisen yksityisavainta. Jos hyökkääjä pääsee käsiksi jaettuun salaisuuteen, hyökkääjä voi purkaa jaetulla salaisuudella salattuja viestejä. (Shinder 2011.)

Salakirjoitusavaimia, jotka eivät ole enää salaisia kutsutaan vaarantuneiksi. Vaarantumisen jälkeen salakirjoitusavaimia ei voida enää käyttää viestien ja identiteettien salaamiseen. Salakirjoitusavaimien vaarantumisen havaitseminen on usein erittäin vaikeata. (Shinder 2011.)

3.8 Application-Layer attack-sovellustason hyökkäys

Sovellustason hyökkäys voidaan määritellä yritykseksi heikentää ohjelmaa, ohjelman käyttäjää tai ohjelman käsittelemiä tietoja haittatarkoitusta varten. Sovellustason hyökkäyksen mahdollistaa yleensä ohjelmassa oleva ohjelmointivirhe, ohjelman luomiseen käytetyn ohjelmointikielen rakenteen aiheuttama haavoittuvuus tai ohjelman monimutkaiset asetukset. (Rash 2007, 72.)

Sovellustason hyökkäykset voidaan jakaa kolmeen eri kategoriaan: Ohjelmointivirheitä tai luottamusta hyväksikäyttäviin ja resursseja näännyttäviin. (Rash 2007, 73.)

3.8.1 Ohjelmointivirheitä hyväksikäyttävä sovellustason hyökkäys

Sovelluksien kehittäminen on monimutkainen prosessi, jossa ohjelmointivirheitä tulee pakostakin tehtyä. Joissakin tapauksissa ohjelmointivirheet aiheuttavat vakavia haavoittuvuuksia, joita hyökkääjä voi hyväksikäyttää. Osa ohjelmointivirheistä aiheutuvista haavoittuvuuksista mahdollistaa esimerkiksi SQL-injektiohyökkäykset tai XSS-hyökkäykset. (Rash 2007, 73.)

3.8.2 Luottamusta hyväksikäyttävä sovellustason hyökkäys

Jotkut hyökkäykset hyväksikäyttävät luottamusta ohjelmointivirheiden sijaan. Tällaiset hyökkäykset näyttävät täysin luotettavilta ohjelmankäytön kannalta, mutta tosiasiassa hyökkäykset kohdistuvatkin ohjelmaa käyttävän henkilön luottamukseen. Tietojen kalastelu- eli phishing-hyökkäykset ovat yksi hyvä esimerkki hyökkäyksestä, jossa hyväksikäytetään käyttäjän luottamusta. (Rash 2007, 73.)

3.8.3 Resursseja näännyttävä sovellustason hyökkäys

Resursseja näännyttämällä hyökkääjä voi kaataa tai estää palvelun käyttämisen. Yleisin resursseja näännyttävä sovellustason hyökkäys on hajautettu palvelunestohyökkäys. Suorittamalla palvelunestohyökkäyksen sovellustasolla, hyökkääjä voi kohdistaa hyökkäyksen suoraan sellaiseen porttiin, jota yrityksen tai käyttäjän palomuuri ei ole suojannut, esimerkiksi HTTP-liikenteen portti 80. Hyökkääjä voi täten tukkia palvelunestohyökkäyksestä aiheutuvalla liikenteellä yrityksen web-palvelimen. (Rash 2007, 73.)

3.9 Password-Based attack-salasanapohjainen hyökkäys

Salasanapohjaisen hyökkäyksen tarkoituksena on arvata järjestelmässä käytettävä salasana. Yksi suurimmista salasanojen tietoturvaheikkouksista on salasanan ja käyttäjätunnuksen yhdistäminen alkuperäiseen käyttäjään autentikointivaiheessa. Useimmiten salasanan ja käyttäjätunnuksen sen hetkistä käyttäjää ei varmenneta käyttäjätilin alkuperäiseksi omistajaksi. Toinen ongelma salasanojen käytössä on, miten salasana ja käyttäjätunnus lähetetään. Monet vanhat palvelut lähettävät käyttäjätiedot selkokielisenä, eli niitä ei ole mitenkään salattu. (Spencer: Network Attacks.)

Salasanapohjaisia hyökkäyksiä on olemassa neljää eri tyyppiä: passiivisia, aktiivisia, yhteydettömiä ja ei-elektronisia (kuva 9).

KUVA 9. Salasanapohjaiset hyökkäykset (Rumy 2012.)

3.9.1 Passive Online attacks-passiiviset verkkohyökkäykset

Passiivinen verkkohyökkäys voidaan suorittaa langallisen tai langattoman verkon salakuuntelulla, jossa hyödynnetään esimerkiksi verkkoanalysaattoria. Passiivinen verkkohyökkäys ei näy loppukäyttäjälle. Salasanan kaappaus tapahtuu autentikointivaiheessa. Jos lähetetty käyttäjätilin salasana muodostuu salasanatiivisteestä tai se on salattu, voi hyökkääjä käyttää sen murtamiseen esimerkiksi sanakirjahyökkäystä. (Graves 2010, 97.)

Toinen passiivisen verkkohyökkäyksen muoto on mies välissä -hyökkäys. Mies välissä -hyökkäyksessä, hyökkääjä sieppaa autentikointipyynnön ja välittää sen palvelimelle. Käyttämällä verkkoanalysaattoria asiakkaan ja palvelimen välissä, hyökkääjä pystyy tutkimaan molemminsuuntaista liikennettä ja samalla kaappaan salasanoja. (Graves 2010, 98.)

Kolmas passiivisen verkkohyökkäyksen muoto on toistohyökkäys. Siinä hyökkääjä kaappaa autentikointipaketit ja uudelleenlähettää ne myöhempää autentikointia varten. Tällä tavoin hyökkääjän ei tarvitse murtaa tai oppia salasanaa. (Graves 2010, 98.)

3.9.2 Active Online attacks-aktiiviset verkkohyökkäykset

Helpoin tapa saada järjestelmänvalvojan oikeudet, on arvata järjestelmänvalvojan käyttämä salasana. Salasanan arvaaminen on aktiivinen verkkohyökkäys. Se perustuu inhimillisten tekijöiden osallisuuteen salasanan luonnissa ja se toimii ainoastaan heikkoja salasanoja vastaan. Hyökkääjä voi käyttää salasanan arvaamiseen sanakirjahyökkäystä, sanalistoja, erilaisia kirjain-, numero- ja erikoismerkkiyhdistelmiä. Hyökkääjä voi myös automatisoida salasanan arvaamisen. Yksinkertaisin tapa estää salasanan arvaaminen, on ottaa käyttöön kirjautumisyrityksien rajattu määrä. (Graves 2010, 98.)

3.9.3 Offline attacks-yhteydettömät hyökkäykset

Yhteydetön hyökkäys tapahtuu muussa sijainnissa, kuin missä salasana sijaitsee tai missä salasanaa käytettiin. Yhteydettömät hyökkäykset vaativat yleensä fyysisen pääsyn kohdetietokoneeseen ja salasanatiedostoon. Hyökkääjä voi kuitenkin kopioida salasanatiedoston tai käyttäjätietokannan omalle koneellensa. Tämän jälkeen hyökkääjä voi murtaa salasanan sanakirjahyökkäyksen, hybridihyökkäyksen tai väsytysmenetelmän avulla. (Graves 2010, 99.)

3.9.3.1 Dictionary attack-sanakirjahyökkäys

Sanakirjahyökkäys on kaikkein yksinkertaisin ja nopein tapa salasanan murtamiseen. Sitä käytetään sellaisia salasanoja vastaan, jotka ovat itsessään sanoja. Sanakirjahyökkäys ei toimi salasanoja vastaan, jotka sisältävät merkkejä tai numeroita. Sanakirjahyökkäyksessä käytetään listaa sanoista, joista jokaisesta muodostetaan hajakoodausfunktiolla salasanatiiviste, käyttämällä samaa algoritmia kuin autentikointiprosessissakin. Tämän jälkeen salasanatiivisteiksi muutettuja merkkijonoja verrataan kaapattujen salasanojen tiivisteiden kanssa. (Graves 2010, 100.)

3.9.3.2 Hybrid attack-hybridihyökkäys

Hybridihyökkäys on sanakirjahyökkäyksen seuraava taso. Siinä hyökkääjä soveltaa numeroiden ja erikoismerkkien käyttöä kokeiltavissa sanoissa. Esimerkiksi monet käyttäjät lisäävät salasanansa perään numeron yksi. Hybridihyökkäyksellä pyritään etsimään kyseiset poikkeavuudet salasanoista. (Graves 2010, 100.)

3.9.3.3 Brute-force attack-väsytysmenetelmä

Kaikkein aikaa kuluttavin menetelmä on väsytysmenetelmä. Siinä hyökkääjä käyttää tietokoneen raakaa laskentavoimaa salasanan murtamiseksi. Väsytysmenetelmä käy läpi kaikki mahdolliset kirjain-, numero- ja erikoismerkkiyhdistelmät. (Graves 2010, 100.)

3.9.3.4 Nonelectronic attacks-ei-elektroniset hyökkäykset

Ei-elektroniset hyökkäykset ovat hyökkäyksiä, jotka eivät vaadi teknistä tietämystä. Olan yli kurkkiminen, sosiaalinen manipulointi ja ”roskiksen kaivelu” ovat ei-elektronisia hyökkäyksiä. (Graves 2010, 101.)

3.10 Denial-of-Service attack-palvelunestohyökkäys

Palvelunestohyökkäys on verkkohyökkäys, jolla hyökätään verkkopalvelua, tietoverkkoa tai järjestelmää vastaan. Palvelunestohyökkäyksen tavoitteena on kohteen tarjoaman palvelun häirintä tai sen estäminen. Onnistunut palvelunestohyökkäys estää muita palvelun käyttäjiä käyttämästä palvelua, kunnes hyökkäys on estetty tai lopetettu. (F-Secure: About Denial of Service.)

Yleisimpiä palvelunestohyökkäyksen kohteita ovat Internet-sivustot, etenkin isojen kaupallisten tahojen. Palvelunestohyökkäyksillä voidaan myös hyökätä sähköpostitilejä, Internet-tietokantoja ja DNS-palvelimia vastaan, mutta niin käy harvemmin. (F-Secure: About Denial of Service.)

Palvelunestohyökkäyksillä myös tavoitellaan joskus taloudellista hyötyä. Jotkut tahot vuokraavat rikollisilta bottiverkkoja palvelunestohyökkäyksiin, joita he käyttävät kilpailevien yrityksien palveluita vastaan. Toinen keino millä taloudellista hyötyä tavoitellaan, on ottamalla panttivangiksi palvelunestohyökkäyksen kohteita. Panttivangiksi joutuneelta palvelujen ylläpitämältä taholta kiristetään rahaa hyökkäyksen lopettamiseksi. (F-Secure: About Denial of Service.)

3.10.1 Hyökkäystavat

Palvelunestohyökkäykset voidaan jakaa kahteen pääkategoriaan, yhdellä järjestelmällä suoritettaviin palvelunestohyökkäyksiin (DOS) ja hajautettuihin palvelunestohyökkäyksiin (DDOS). Hajautetussa palvelunestohyökkäyksessä hyökätään useilla järjestelmillä yhtä kohdetta vastaan. (Graves 2010, 174.)

Palvelunestohyökkäys voidaan suorittaa:

- Kuluttamalla rajallisia resursseja, kuten kaistanleveyttä, levytilaa, prosessorin laskentatehoa
- Häiritsemällä tai muuttamalla ohjaustietoja, kuten reititystietoja
- Häiritsemällä tilatietoja, esim. TCP-istunnon resetoinnilla
- Häiritsemällä tietoverkon fyysisiä komponentteja (Wikipedia: Denial-of-service attack).

Palvelunestohyökkäyksissä voidaan myös käyttää haittaohjelmia, joiden tarkoituksena on:

- Prosessorin käytön maksimointi
- Käyttöjärjestelmän kaataminen
- Virhetilojen aiheuttaminen (Wikipedia: Denial-of-service attack).

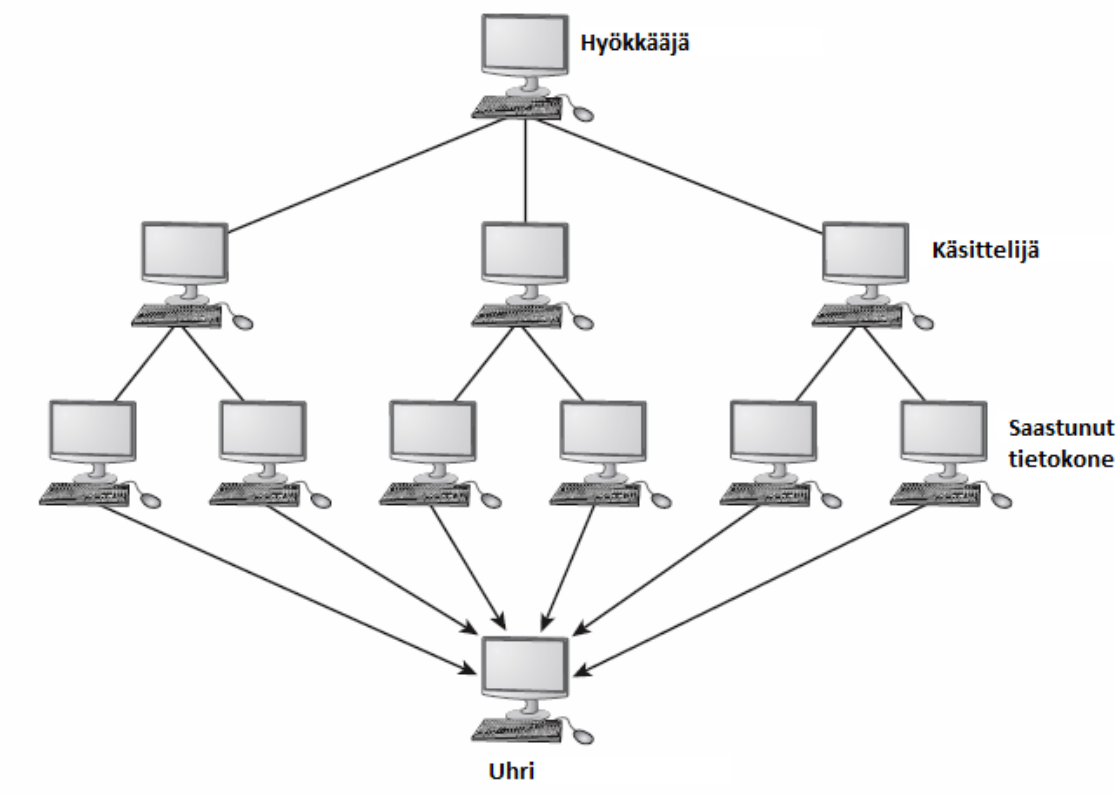
3.10.2 Hajautettu palvelunestohyökkäys

DDOS-hyökkäys on kehittyneempi versio DOS-hyökkäyksestä. DDOS-hyökkäyksen tavoitteet ovat samat kuin DOS-hyökkäyksenkin. Siinä useat järjestelmät pyrkivät estämään verkossa olevan resurssin toimimisen ja käytön, lähettämällä hyökättävään koh-

teeseen niin paljon paketteja, että se ei pysty käsittelemään niitä. Valtaosa DDOS-hyökkäyksistä suoritetaan bottiverkkojen avulla, koska niissä on tuhansia tai kymmeniä-tuhansia saastuneita tietokoneita. (Graves 2010, 177-178.)

Bottiverkon avulla suoritettu DDOS-hyökkäys koostuu (kuva 19):

- Käsittelijästä, joka käsittelee hyökkääjältä tulleen hyökkäyskäskyn ja välittää sen eteenpäin saastuneille tietokoneille.
- Saastuneista tietokoneista, jotka toimivat käsittelijän käskyjen perusteella.
- Uhrista (Graves 2010, 178).



KUVA 10. DDOS-hyökkäyksen rakenne (Graves 2010, 178.)

4 BOTNET-BOTTIVERKKO

4.1 Bottiohjelma

Botit ovat ohjelmia, jotka tekevät toimintoja toistuvasti tai toimivat käyttöliittymänä toisten ohjelmien hallitaan. Botit ovat hyödyllisiä ohjelmia yksinkertaisten toimintojen automatisoinnissa tai useiden järjestelmien hallinnan yksinkertaistamisessa. Bottiverkoissa botteja käytetään haittatarkoitukseen, koska niiden avulla hyökkääjä kaappaa ja hallitsee tietokonejärjestelmiä. (F-Secure: About Botnets.)

Hyökkääjät käyttävät erilaisia haittaohjelmia, joiden avulla he saavat botin asennettua saastutettuun järjestelmään. Yleisin tapa on saastuttaa tietokone troijalaisella, jonka kantaa haittakuormassaan bottia. (F-Secure: About Botnets.)

Kun botti on asennettu onnistuneesti saastuneeseen koneeseen, se kykenee ottamaan järjestelmän haltuunsa. Tämän jälkeen hyökkääjä voi lähettää botille erilaisia käskyjä ja käyttää sitä haittatarkoituksiin. Tältä osin botit ovat erittäin samanlaisia backdoor-ohjelmien kanssa. (F-Secure: About Botnets.)

Tietokoneet joihin on asennettu sama botti muodostavat verkon, jota hyökkääjä voi hallita. Näitä verkkoja kutsutaan bottiverkoiksi. Bottiverkot koostuvat yleensä tuhansista tai sadoista tuhansista botteilla saastutetuista tietokoneista. Yhtä saastunutta bottiverkon jäsentä kutsutaan botiksi tai zombie-tietokoneeksi. (F-Secure: About Botnets.)

4.1.1 Bottiverkon hallinta

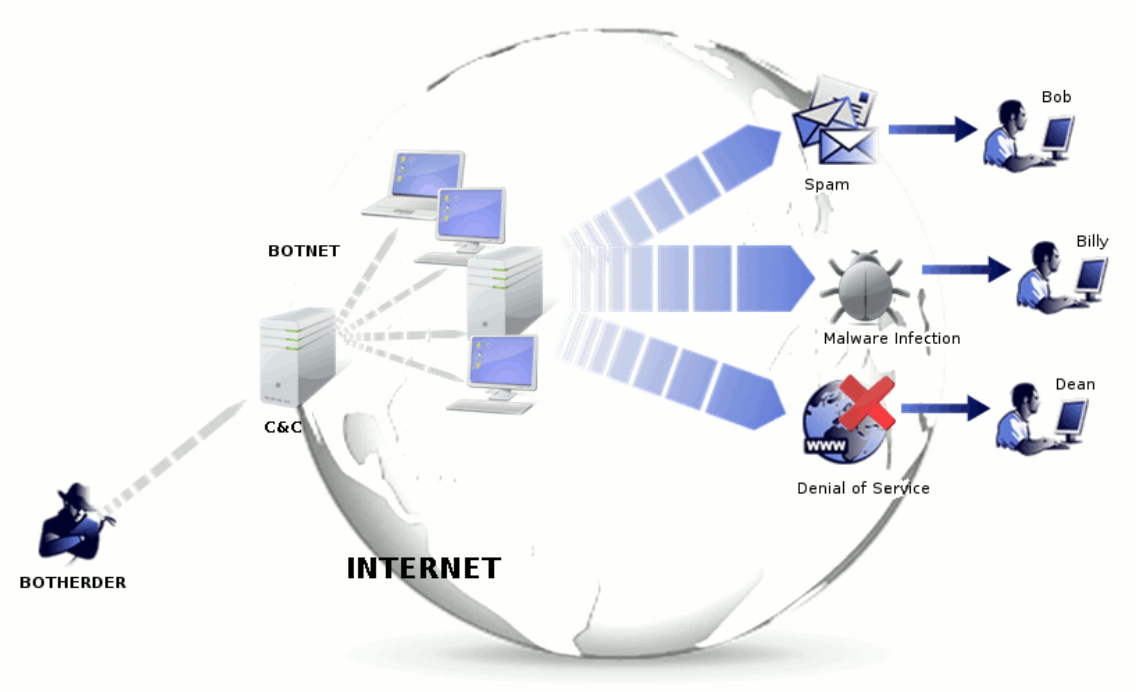
Hyökkääjää, joka antaa bottiverkolle komentoja, kutsutaan bottipaimeneksi tai ohjaajaksi. Ennen vanhaa bottiverkkoja ohjasivat yksittäiset hyökkääjät, mutta viime vuosien saatossa bottiverkot ovat suuntautuneet kaupallisiksi. Joidenkin nykyisten bottiverkkojen uskotaan kuuluvan rikollissyndikaateille. (F-Secure: About Botnets.)

Hallitakseen bottiverkoa, ohjaaja käyttää asiakas-ohjelmaa, jonka avulla hän voi lähettää boteille erilaisia komentoja. Ohjelman avulla bottiverkon käyttäminen on erittäin

tehokasta, koska komentoja pystytään lähettämään yhdelle botille, useille boteille tai koko bottiverkolle. (F-Secure: About Botnets.)

Asiakas-ohjelmaa käyttämällä, ohjaaja voi ohjata yhden botin suorittamaan jonkin tietyn toiminnon. Toiminto voi olla esimerkiksi kaikkien koneeseen tallennettujen sähköpostiosoitteiden lähettäminen tietylle Internet-sivustolle. Vaihtoehtoisesti kaikkia botteja voidaan käskeä tekemään samaa toimintoa, esim. pyynnön lähettämistä tietty Internet-sivustoon. (F-Secure: About Botnets.)

Bottit ja niitä hallitseva asiakas-ohjelma muodostavat komenna ja hallitse -infrastruktuurin (kuva 11). Zombie-tietokonetta, Internet-sivustoa tai palvelinta, jolla asiakas-ohjelma sijaitsee, kutsutaan hallintapalvelimeksi (C&C). (F-Secure: About Botnets.)



KUVA 11. Bottiverkon infrastruktuuri (F-Secure: About Botnets.)

Jotkut bottiverkot ovat kuvaa 11:kin monimutkaisempia. Niissä voi olla esimerkiksi useita hallintapalvelimia tai ne voivat käyttää redundanssia suojautumismuotona. Joissakin bottiverkoissa voi olla vain yksi hallintapalvelin, mutta se vaihtuu jatkuvasti koneesta toiseen. (F-Secure: About Botnets.)

4.1.2 Bottiverkon tuhoaminen

Bottiverkon tuhoamiseksi yleensä paras tapa on hallintapalvelimien sulkeminen. Näitä hallintapalvelimia sulkevat oikeusviranomaiset, kuten kansainväliset tietoturvaviranomaiset, CERTit (Computer Emergency Response Team). Hallintapalvelimien sulkeminen estää bottiverkon ohjaajaa käskyttämästä botteja. (F-Secure: About Botnets.)

Eräässä bottiverkkojen alasajossa epäiltiin amerikkalaista McColo Internet-palvelujentarjoajaa useiden bottiverkkojen hallintapalvelimien ylläpitäjäksi, ynnä muiden haittaperäisten palvelujen ylläpitäjäksi. Alasajon jälkeen maailmanlaajuinen roskapostitus laski 60-75 %. (F-Secure: About Botnets.)

4.1.3 Bottiverkon käyttökohteet

Bottiverkkoa ohjaava hyökkääjä voi tehdä useita eri toimenpiteitä, niin yksittäisille bottiverkon koneille ja koko bottiverkon voiman kanssa.

4.1.3.1 Tiedonkeruu

Useat ihmiset tallentavat tietokoneille luottamuksellista tietoa, kuten henkilöllisyystodistuksia, työhön liittyvää aineistoa, sähköpostiosoitteita jne. Jos tiedot ovat tallennettu osana bottiverkkoa olevaan tietokoneeseen, niin bottiverkon ohjaajalle on niihin miltei taattu pääsy. Kerättyjä luottamuksellisia tietoja voidaan myydä eteenpäin rikollisille, petoksien helpottamiseksi. (F-Secure: About Botnets.)

4.1.3.2 Varastetut resurssit

Bottiverkon ohjaajat voivat käyttää bottiverkon fyysisiä resursseja, kuten laskentatehoa tai vapaata tilaa, eri tarkoituksiin. Niitä voidaan käyttää esimerkiksi:

- Verkkohyökkäyksiin, joissa bottiverkon osia voidaan käyttää palvelunestohyökkäyksiin tai hajautettuihin palvelunestohyökkäyksiin
- Roskapostitukseen, joka on yleisin bottiverkon käyttökohde. Suurin osa maailman roskapostista on peräisin bottiverkoista
- Haittaohjelmien jakamiseen eri tavoilla, kuten sähköposti liitteiden kautta jne.
- Tietojen varastointiin (F-Secure: About Botnets).

5 PHISHING-TIETOJEN KALASTELU

5.1 Tietojen kalastelu

Tietojen kalastelu, eli phishing, on rikollistoimintaa, jolla pyritään keräämään luottamuksellisia tietoja, kuten henkilö- tai tilitietoja. Tietojen kalastelu on yksi sosiaalisen manipuloinnin muoto, jossa ulkopuolinen taho esiintyy valheellisesti tiedon saantiin oikeutettuna tahona, kuten pankkina. (Panda Security: Phishing - personal data theft.) Suomessa tietojen kalastelu on verrattain vähäistä suomenkielen takia, mutta joitakin tapauksia on Suomessa nähty.

5.2 Tietojen kalastelun ominaispiirteet

Tietojen kalastelu liittyy läheisesti sähköpostiviesteihin, jotka näyttävät tulevan luotettavista lähteistä, kuten pankeilta. Sähköpostit viestit sisältävät yleensä Internet-linkin, joka vie käyttäjän huijaussivustolle, jossa kysellään luottamuksellisia tietoja. Tällä tavoin käyttäjät saadaan uskomaan, että he asioivat luotettavan tahon kanssa. (Panda Security: Phishing - personal data theft.)

Huijausviesteille ominaisimmat piirteet ovat:

- Tunnettujen yrityksien nimien käyttö. Käyttämällä tunnetun yrityksen nimeä, rikolliset voivat suunnitella huijaussivuston ja -viestin yrityksen käyttämien sivustojen ja sähköpostiviestin mukaan. Tällä pyritään harhauttamaan käyttäjiä luulemaan viestiä aidoksi

- Aidon yrityksen työntekijöiden nimien käyttö. Rikolliset pyrkivät käyttämään työntekijöiden nimiä huijausviestin lähetyksessä. Tällä tavoin he voivat esittää viestinlähettäjän olevan töissä yrityksessä

- Harhauttavien Internet-sivustojen osoitteiden käyttö. Esimerkiksi www.goole.com (www.google.com) tai www.sampo-pankki.fi (www.sampopankki.fi)

- Uhkailu ja pelottelu. Rikolliset käyttävät usein uhkailua ja pelottelua käyttäjän harhauttamiseksi. Huijausviestissä voidaan kertoa esimerkiksi sähköpostitilin joutuneen murron kohteeksi ja käyttäjää pyydetään vahvistamaan sähköpostitiliin liittyvät tiedot tai sähköpostitili suljetaan pysyvästi (Panda Security: Phishing - personal data theft).

6 POHDINTA

Opinnäytetyön suunnitellun sisällön kanssa onnistuttiin hyvin, vaikkakin muutamia aiheita jouduttiin karsimaan pois, jo ihan opinnäytetyön laajuuden vuoksi. Nykyisistä aiheistakin olisi saanut monta kymmentä sivua lisää tekstiä, ennakkotapausten ja statistiikan muodossa. Lisäksi siinä, että aiheissa käsitellyt asiat ovat helppo ymmärtää kokemattoman käyttäjän näkökulmasta, onnistuttiin hyvin.

Opinnäytetyössä nojautuu alkuperäisteoksiin ja muihin lähteisiin erittäin raskaasti. Lähteiden paikkansapitävyyttä on pyritty seuraamaan, ettei työssä käytetä huonoa lähdetietoa. Valtaosa työssä käytetyistä lähteistä on kirjoitettu englanniksi ja niiden käännöstyössä on onnistuttu hyvin. Lauseiden sisältö ei ole menettänyt tarkoitusta käännösvaiheessa.

Vaikeinta opinnäytetyön tekemissä oli aiheiden sisällön rajaaminen niin, että aiheet käsitellään tarpeeksi perusteellisesti, kuitenkin menemättä liikaa teknisiin yksityiskohtiin. Vaikeutena oli myös kirjoittaa entuudestaan tutuista aiheista, koska se tuntui vanhan uudelleen kertaamiselta.

Työtä olisi mahdollista jatkaa tulevaisuudessa vaikka kuinka pitkälle. Tietoturvauhkien jatkuva kehittyminen ja uusista teknologioista aiheutuvat uudet tietoturvauhat tarjoaisivat varmasti paljon kirjoitettavaa. Lisäksi, kuten aikaisemmin mainittiin, statistiikan ja ennakkotapausten lisääminen jo kirjoitettuihin aiheisiin, antaisi työlle myös laajemman perspektiivin.

LÄHTEET

Davis, M., Bodmer, S. & LeMasters, A. 2009. Hacking Exposed Malware and Rootkits. New York: McGraw-Hill.

Graves, K. 2010. CEH Certified Ethical Hacker Study Guide. New York: Wiley Publishing, Inc.

Levis W. 2008. LAN Switching and Wireless: Ccna Exploration Companion Guide. Indianapolis: Cisco Press.

Rash, M. 2007. Linux Firewalls: Attack Detection and Response with Iptables, Psad, and Fwsnort. San Francisco: William Pollock.

Panda Security. Crimeware: the silent epidemic. Luettu 20.4.2012. http://www.pandasecurity.com/homeusers/security-info/types-malware/crimeware/

Lemos, R. 2009. Real-Time Hackers Foil Two-Factor Security. Technology Review. Luettu 20.4.2012. http://www.technologyreview.com/computing/23488/

Chen, T. & Robert, J-M. 2004. The Evolution of Viruses and Worms. Southern Methodist University. Luettu 1.5.2012. http://lyle.smu.edu/~tchen/papers/statmethods2004.pdf

von Neumann, J. 1966. Theory of Self-Reproducing Automata. University of Illinois Press. Luettu 1.5.2012. http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf

Risak, V. 1972. Selbstreproduzierende Automaten mit minimaler Informationsübertragung. Elektrotechnik und Maschinenbau. Luettu 1.5.2012. http://www.cosy.sbg.ac.at/~risak/bilder/selbstrep.html

Kraus, J. 1980. Selbstreproduktion bei Programmen. Technische Universität Dortmund. Luettu 1.5.2012.
http://alumni-informatik-dortmund.de/sites/default/files/Reproduktion10.pdf

Rouse, M. 2005. Elk Cloner. SearchSecurity. Luettu 1.5.2012. http://searchsecurity.techtarget.com/definition/Elk-Cloner

Cohen, F. 1984. Computer Viruses – Theory and Experiments. University of Southern California. Luettu 1.5.2012. http://all.net/books/virus/index.html

Chess, D. & White, S. 2000. An Undetectable Computer Virus. IBM Thomas J. Watson Research Center. Luettu 1.5.2012.
http://www.research.ibm.com/antivirus/SciPapers/VB2000DC.htm

McAfee. 2006. Rootkits, Part 1 of 3: The Growing Threat. Luettu 10.4.2012. http://download.nai.com/Products/mcafee-avert/whitepapers/akapoor_rootkits1.pdf

Securelist. History of malicious programs – 1990. Luettu 1.5.2012. http://www.securelist.com/en/threats/detect?chapter=111

F-Secure. W32/Concept. Luettu 1.5.2012. http://www.f-secure.com/v-descs/concept.shtml

Symantec. W95.CIH. 2002. Luettu 1.5.2012. http://www.symantec.com/security_response/writeup.jsp?docid=2000-122010-2655-99

AnVir. Virus. Luettu 1.5.2012. http://www.anvir.com/virus.htm

OmniSecu. Types of Computer Viruses. Luettu 1.5.2012. http://www.omnisecu.com/security/types-of-computer-viruses.htm

Spencer, W. Computer Worms. Tech-FAQ. Luettu 26.4.2012. http://www.tech-faq.com/computer-worm.html

Beal, V. 2011. The Difference Between a Computer Virus, Worm and Trojan Horse. Webopedia. Luettu 26.4.2012. http://www.webopedia.com/DidYouKnow/internet/2004/virus.asp

Chen, T. 2003. Trends in Viruses and Worms. Southern Methodist University. Luettu 26.4.2012. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/virus_trends.html

Schmidt, C. & Darby, T. 2001. The What, Why, and How of the 1988 Internet Worm. Luettu 26.4.2012. http://snowplow.org/tom/worm/worm.html

Fosnock, C. 2005. Computer Worms: Past, Present, and Future. East Carolina University. Luettu 26.4.2012. http://www.infosecwriters.com/text_resources/pdf/Computer_Worms_Past_Present_and_Future.pdf

Spam Laws. Computer Worm Malware: How It Works. Luettu 26.4.2012. http://www.spamlaws.com/how-worm-malware-works.html

F-Secure. About Worms. Luettu 26.4.2012. http://www.f-secure.com/en/web/labs_global/articles/about_worms

Panda Security. Worms. Luettu 26.4.2012. http://www.pandasecurity.com/homeusers/security-info/classic-malware/worm/

McWilliams, B. 2003. Cloaking Device Made for Spammers. Wired. Luettu 26.4.2012. http://www.wired.com/techbiz/media/news/2003/10/60747

F-Secure. About Trojans. Luettu 28.4.2012. http://www.f-secure.com/en/web/labs_global/articles/about_trojans

F-Secure. Terminology. Luettu 28.4.2012. http://www.f-secure.com/en/web/labs_global/terminology-t

Spam Laws. What is Adware? Luettu 22.4.2012. http://www.spamlaws.com/what-is-adware.html

Wauters, R. 2010. Kazaa Takes A Swing At Symantec After Adware Accusations. TechCrunch. Luettu 22.4.2012. http://techcrunch.com/2010/02/06/kazaa-symantec-adware/

Panda Security. Spyware. Luettu 24.4.2012. http://www.pandasecurity.com/homeusers/security-info/cybercrime/spyware/

Wienbar, S. 2004. Perspective: The spyware inferno. CNET. Luettu 24.4.2012. http://news.cnet.com/2010-1032-5307831.html

Shields, T. 2008. Survey of Rootkit Technologies and Their Impact on Digital Forensics. Donkey On A Waffle. Luettu 10.4.2012. http://www.donkeyonawaffle.org/misc/txs-rootkits_and_digital_forensics.pdf

Wikipedia. 2012. Rootkit. Luettu 11.4.2012. http://en.wikipedia.org/wiki/Rootkit

Russinovich, M. 2005. Unearthing Root Kits. Windows IT Pro. Luettu 11.4.2012. http://www.windowsitpro.com/article/intermediate/unearthing-root-kits

Russinovich, M. 2006. Using Rootkits to Defeat Digital Rights Management. Technet. Luettu 11.4.2012. http://blogs.technet.com/b/markrussinovich/archive/2006/02/06/using-rootkits-to-defeat-digital-rights-management.aspx

Lemos, R. 2005. World of Warcraft hackers using SONY BMG rootkit. The Register. Luettu 11.4.2012. http://www.theregister.co.uk/2005/11/04/secfocus_wow_bot/

Rose, J. 2003. Turning the tables: Loadable Kernel Module Rootkits deployed in a honeypot environment. SANS Institute. Luettu 11.4.2012. http://www.sans.org/reading_room/whitepapers/detection/turning-tables-loadable-kernel-module-rootkits-deployed-honeypot-environment_996

Ortega, A. & Sacco, A. Deactivate the Rootkit: Attacks on BIOS anti-theft technologies. Core Security Technologies. 2009. Luettu 11.4.2012. https://www.blackhat.com/presentations/bh-usa-09/ORTEGA/BHUSA09-Ortega-DeactivateRootkit-PAPER.pdf

Kleissner, P. 2009. The Rise of MBR Rootkits & Bootkits in the Wild. Stoned Vienna. Luettu 11.4.2012. http://www.stoned-vienna.com/downloads/The Rise of MBR Rootkits & Bootkits in the Wild.pdf

Schneier, B. 2009. “Evil Maid” Attacks on Encrypted Hard Drives. Schneier on Security. Luettu 11.4.2012. http://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html

Perrin, C. 2007. UNIX/Linux rootkits 101. TechRepublic. Luettu 11.4.2012. http://www.techrepublic.com/blog/security/unixlinux-rootkits-101/264

Academic. Greek telephone tapping case 2004-2005. Luettu 11.4.2012. http://en.academic.ru/dic.nsf/enwiki/1894956

Gibbs, M. 2005. Is Sony's CD DRM malware? Network World. Luettu 11.4.2012. http://www.networkworld.com/columnists/2005/110705backspin.html

Schneier, B. 2005. Real story of the rogue rootkit. Wired. Luettu 11.4.2012. http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69601?currentPage=all

McMillan, R. 2010. Siemens: Stuxnet hit industrial systems. Computerworld. Luettu 11.4.2012. http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

Microsoft. Watch out for fake virus alerts. Luettu 18.4.2012. http://www.microsoft.com/security/pc-security/antivirus-rogue.aspx

Kassner, M. 2010. Ransomware: Extortion via the Internet. TechRepublic. Luettu 18.4.2012. http://www.techrepublic.com/blog/security/ransomware-extortion-via-the-internet/2976

Valente, G. 1996. Hackers, crackers, and sniffers. Institute of Internal Auditors. Luettu 10.4.2012. http://findarticles.com/p/articles/mi_m4153/is_n5_v53/ai_18901643/

Colasoft. Network Sniffer Introduction. Luettu 10.4.2012. http://www.colasoft.com/resources/network-sniffer.php

SHALB. 2008. Network Eavesdropping. Luettu 1.5.2012. http://shalb.com/kb/entry/53/

Microsoft. Common Types of Network Attacks. Luettu 30.4.2012. http://technet.microsoft.com/en-us/library/cc959354.aspx

Verma, D. 2012. IP Spoofing Attack and Defenses. InfoSec Institute. Luettu 1.5.2012. http://resources.infosecinstitute.com/ip-spoofing-attack/

Borkin, M., Kraus, R. & Prowell, S. 2010. Seven Deadliest Attacks Waltham: Syngress.

Yang, Y. & Bhatia, A. 2008. Man-in-the-Middle Attack. Toolbox. Luettu 1.5.2012. http://it.toolbox.com/wiki/index.php/Man-in-the-Middle_Attack

Shinder, D. 2011. Network Encroachment Methodologies. WindowSecurity. Luettu 1.5.2012. http://www.windowsecurity.com/articles/Network-Encroachment-Methodologies.html

Spencer, W. Network Attacks. Tech-FAQ. Luettu 1.5.2012. http://www.tech-faq.com/network-attacks.html

Rumy, S. 2012. Types of Password Attack. CCNP Security. Luettu 1.5.2012. http://ccnpsecurity.blogspot.com/2012/01/types-of-password-attack.ht l

F-Secure. About Denial of Service (DOS). Luettu 3.5.2012. http://www.f-secure.com/en/web/labs_global/articles/about_denialofservice

Wikipedia. 2012. Denial-of-service attack. Luettu 3.5.2012. http://en.wikipedia.org/wiki/Denial-of-service_attack

F-Secure. About Botnets. Luettu 3.5.2012. http://www.f-secure.com/en/web/labs_global/articles/about_botnets

Panda Security. Phishing: personal data theft. Luettu 3.5.2012. http://www.pandasecurity.com/homeusers/security-info/types-malware/phishing/

Edwards, J. 2011. How To Remove Adware: Simple and Proven Tips. TekType. [kuva]. Luettu 22.4.2012. http://tektype.wordpress.com/2011/08/26/how-to-remove-adware-simple-and-proven-tips/

Information Security Office. Examples of Rogue Security Software. Carnegie Mellon University. [kuva]. Luettu 18.4.2012. http://www.cmu.edu/iso/threats/rogue-software/rogue-software.html

Correll, S-P. 2010. Twitter used for Rogueware Distribution. PandaLabs. [kuva]. Luettu 18.4.2012. http://pandalabs.pandasecurity.com/twitter-used-for-rogueware-distribution/

Information Security Office. Examples of Fradulent Security Warnings. Carnegie Mellon University. [kuva]. Luettu 18.4.2012. http://www.cmu.edu/iso/threats/rogue-software/rogue-warnings.html

Tromer, E. Gpcode.ak Crypthographic Challenge. [kuva]. Luettu 18.4.2012. http://tau.ac.il/~tromer/gpcode/

Danchev, D. 2010. Copyright violation alert ransomware in the wild. ZDNet. [kuva]. Luettu 18.4.2012. http://www.zdnet.com/blog/security/copyright-violation-alert-ransomware-in-the-wild/6095?tag=nl.e550