Hakkeririkollisuuden historia puhelinkaappauksista tietomurtoihin ja viruksiin

Nuutti Rintala

Helsinki 11.5.2004

Seminaari

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department

Tekijä — Författare — Author

Nuutti Rintala

Työn nimi — Arbetets titel — Title

Hakkeririkollisuuden historiapuhelinkaappauksista tietomurtoihin ja viruksiin

Oppiaine — Läroämne — Subject

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
	11.5.2004	11 sivua

Tiivistelmä — Referat — Abstract

Hakkereiden historiaa

Avainsanat — Nyckelord — Keywords

Hakkerit, historia, virukset

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — övriga uppgifter — Additional information

Sisältö

1 Johdanto

Internetissä liikkuu kaikenkarvaista väkeä. Kaikkien tavoitteet eivät ole lainmukaisia. Tämä seminaariesitelmä pyrkii kertomaan Internetin lainsuojattomista ja mitä he ovat saaneet aikaan vuosien varrella. Esitelmä keskittyy hakkeroinnin pimeään puoleen eli tietomurtoihin ja viruksiin. Suurin osa aiheista käsittelee Yhdysvaltain tapauksia, koska hakkeroinnin juuret ovat siellä.

Seuraavat kappaleet käsittelevät hakkereiden alkuperää, kuuluisia hakkerointitapauksia, viruksia, hakkerointia Suomessa, haktivisimia ja lopuksi pohditaan hakkeroinnin vaikutusta tietoturvan kehitykselle.

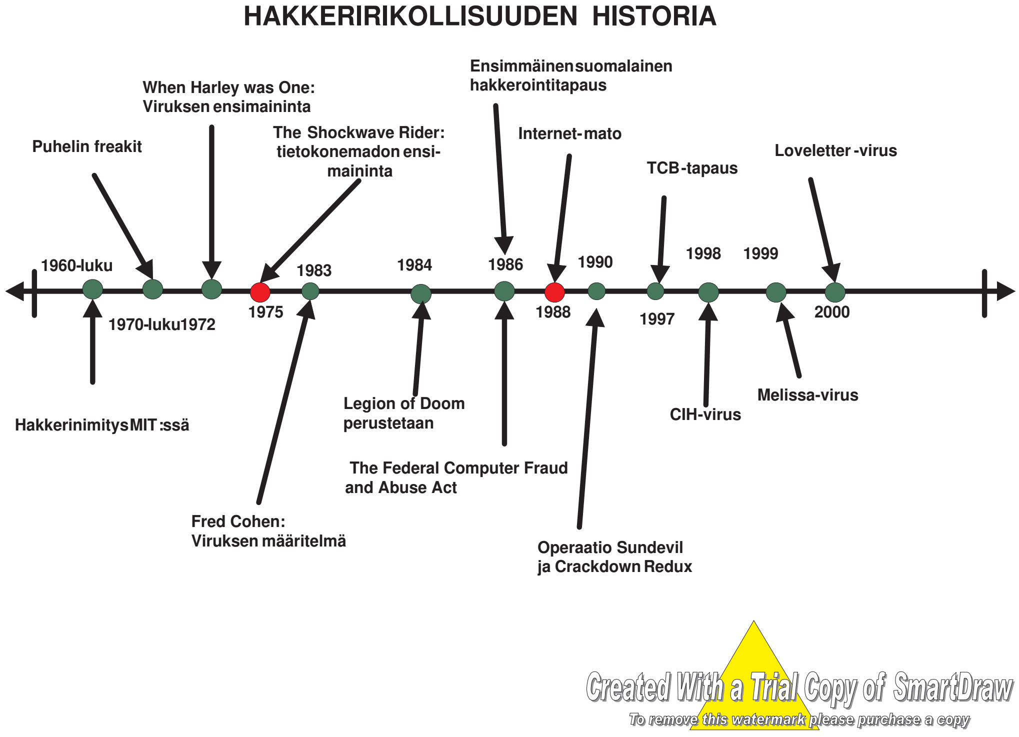
2 Hakkeri

Hakkeri-sana tulee englannin kielen sanasta hacker. Alunperin sana hacker tarkoitti henkilöä, joka valmisti huonekaluja kirveellä. Sittemin sana on saanut merkityksen, joka tarkoittaa henkilöä, joka on innostunut tietokoneharrastaja, hyvä ohjelmoimaan tai muuten vain kiinnostunut tietokonetekniikasta.

Hakkeri-nimikettä alettiin käyttää 1960-luvulla MIT:n (Massachusetts Institute of Technology) tekoälylaboratoriossa työskennelleistä erittäin taitavista FORTRAN- ja muiden kielten ohjelmoijista. He venyttivät etevillä ohjelmointiratkaisuilla eli hackeillä suuret ja kankeat keskustietokoneet äärirajoilleen.

1980-luvulla hakkeri-sanaa alettiin käyttää mediassa harhaanjohtavasti tietokonerikollisista, jotka murtautuivat tietoverkkoihin. Tehdäkseen eron itsestään hakkerit alkoivat kutsua näitä rikollisia krakkereiksi (eng. cracker). Krakkerit kuitenkin julistivat itsensä hakkereiksi ja siten erottelua näiden välillä on vaikeata tehdä. Petteri Järvinen menee jopa niin pitkälle, että väittää IT-tietosanakirjassaan, että hakkeri-sanalla on suomenkielessä vain negatiivinen merkitys.

Koska hakkeri on vakiintunut suomenkielen käyttöön tarkoittamaan tietokonerikollisia, tässä artikkelissa ei tehdä sanallista erottelua lainkuuliaisten ja lainsuojattomien hakkereiden välillä. Esitelmän aihepiiristä johtuen hakkerilla tarkoitetaan jatkossa tietokonerikollisia, tiedostaen kuitenkin etteivät kaikki hakkerit ole rikollisia.



Kuva 1: timeline

3 Captain Crunch ja puhelinfriikit

Hakkeroinnin voidaan katsoa saaneen alkunsa 1970-luvun puhelinfriikeistä (phone phreakers), jotka käyttivät hyödykseen teknistä tietämystään ja puhelinverkkojen puutteita soittaakseen ilmaisia puheluita. Heistä kuuluisin lienee John T Draper alias Captain Crunch, joka on saanut lempinimensä Captain Crunch -muroista. Muropaketin sisällä oli pilli, jolla sai imitoitua puhelinkeskusten soittoääniä ja näin aikaiseksi ilmaisia puheluita [Dra04]. Draperi rakensi teknisiä apuvälineitä soittojen tekoon, sinisiä laatikoita, ja hän pystyi välittämään puhelun itselleen maailman ympäri ja takaisin. Hän tutki puhelinverkon rakennetta, ilmoitti löytämistään virheistään, mutta yritti myös salakuunneellaa mm. FBI:n linjoja. [Par83].

Esquiren 1971 numerossa [Ros71] kerrotaan yksityiskohtaisesti puhelinfreakeistä ja miten ilmaisia puheluita voidaan soittaa. Muiden mukanan Kalifornian Homebrew Computer Club:n kaksi jäsentä innostuvat tästä ja alkavat rakentaa sinisiä laatikoita (blue boxes), joilla ilmaisten puheluiden soittaminen helpottuu entisestään. Nämä kaksi herraa olivat Applen perustajat Steve Jobs ja Steve Wozniak. Woz osasi rakentaa sinisen laatikon artikkelin perusteella, mutta otti yhteyttä Draperiin, saadakseen selville miten sitä käytetään. Draperin opastuksella Woz ensimmäiseksi soitti paaville.

Sininen laatikko oli laite, jolla pystyi matkimaan puhelinkeskusten välittämiä soittokomentoja. Puhelinkeskukset välittivät soittokomennota samaa linjaa pitkin kuin mitä puheääni kulki. 2600 Hz tajuuden ääni on puhelinkeskuksen antamaa linja vapaa -merkki. Kun 70-luvulla antoi tämän merkin kesken puhelun, keskus alkoi odotella sisäisiä soittokomentoja. Niitä pystyi antamaan suoraan linjalle sinisellä laatikolla. Jos soitti 800-alkuiseen ilmaisnumeroon, pystyi puhelun keskeyttämään 2600-merkillä ja välittämään ilmaiseksi minne tahansa maailman sinisen laatikon merkkiäänien ja oikeiden koodien avulla.

Vuonna 1972 friikit perustivat Youth International Party Line-lehden, josta myöhemmin tuli radikaalimpi TAP (Technological Assistance Program). Lehti jakeli teknisiä neuvoja sinisten laatikoiden tekoon ja ilmaisten puheluiden tekemiseen, mutta myöhemmin myös kotitekoisten pommien ja aseiden rakennusohjeita.

Esquire Magazinen jutun jälkeen AT&T ja FBI alkoivat jahdata puhelinfriikkeja ja erityisesti heidän esikuvakseen kohonnutta Captain Crunchia. Captain Crunch sai 1972 viiden vuoden ehdollisen tuomion ja 1000 dollarin sakot, kun FBI oli salakuunellut hänen soittojaan. Heti tuomionsa päättyessä FBI asetti Crunchille ansan ja saivat hänet uudelleen tuomittua tällä kertaa vuodeksi vankeuteen ja viideksi vuodeksi ehdolliseen. Tämä ei vielä riittäny vaan, Crunch sai vielä kolmannen tuomion rakennettuaan automaattisen numeroskannerin, joka soitteli numeroihin ja testasi eri koodien vaikutuksia [Par83]. Nykyään hän tekee tietoturvaohjelmistoja.

1980-luvulla vanhat puhelinverkot korvattiin nykyaikaisemmilla ja sinisten laatikoiden mahti katosi. Puhelinfriikit kehittyivät mukana ja nykyisin on olemassa punaisia laatikoita, joilla saa aikaiseksi vastaavanlaisia vaikutuksia.

4 Hakkeriryhmät, hakkerisodat ja ajojahti

Puhelinfriikkien innostus laantui sitä mukaa, kun varsinaiset tietoverkot yleistyivät. 1980-luvulla hakkereita alkoi kiinnostaa Internetiä edeltävät tietoverkot (ARPAnet, yms.). Hakkereita motivoi seikkailunhalu, näyttämisenhalu ja osaa myös rikollinen toiminta. 1984 perustettiin 2600: the Hacker Quarterly -lehti, joka jakoi neuvoja puhelin- ja tietoverkkohakkeroinnista. Samoin syntyy useita hakkeriryhmiä, joista kuuluisimpia olivat The Legion of Doom, Master of Deception ja Milwaukee 414. Milwaukee 414 oli ensimmäinen hakkeriryhmä, joka pidätettiin 1983. Ryhmä koostui teini-ikäisistä nuorista, jotka olivat murtautuneet useisiin koneisiin ympäri USA:ta. Hakkerointi tapahtui varsin yksinkertaisesti käyttämällä järjestelmien oletusarvoisia salasanoja kuten "TEST"tai "SYSTEM", joita ylläpitäjät eivät koskaan olleet vaihtaneet.

Legion of Doom perustettiin 1984. Ryhmää pidettiin hakkereiden eliittinä ja se veti puoleensa alan parhaat. LoD julkaisi useita teknisiä artikkeleita, joissa yksiyiskohtaisesti kerrottiin tietokoneista, tietoverkoista ja tiedonsiirtotavoista ja näiden artikkeleiden sarja tunnetaan hakkereiden opaskirjana. Eräs ryhmän jäsenistä Phiber Optik (Mark Abene) riitaantui Erik Bloodaxen (Chris Goggins) kanssa ja sai potkut ryhmästä. Hän perusti kilpailevan ryhmän the Masters of Deception.

USA:n kongressi ei jäänyt toimettomaksi kasvavan hakkeriongelman kanssa. 1984 Comprehensice Crime Control Act antaa salaiselle palvelulle toimivallan luottokortti- ja tietokonerikoksissa. Tämän lisäksi vuonna 1986 säädetään Computer Fraud and Abuse Act , joka mahdollistaa viiden vuoden tuomion tietokonerikoksesta, ja vielä seuraavana vuonna Electronic Communications Privacy Act. Chicagon syyttäjät muodostavat Computer Fraud and Abuse Task Force 1988 auttamaan lakien toimeenpanossa.

Vuodesta 1990 lähtien LoD ja MoD aloittivat lähes kaksi vuotta kestäneen sodankäynnin keskenään. He tukkivat puhelinlinjoja, tarkkailivat toisten soittoja ja tunkeutuivat toisten koneisiin. Samaan aikaan FBI, USA:n salainen palvelu ja puhelinyhtiö AT&T käynnistivät operaatio Sundevilin tarkoituksena ottaa kiinni maan hakkerit. Useita BBS:jä, (Bulletin Board System) hakkereiden elektronisia "ilmoitustauluja", suljetaan ympäri maata hatarin perustein. Pidätyksiä tehdään muilla syillä kuin tietokonerikoksiin vedoten, mutta samassa yhteydessä takavarikoidaan epäiltyjen tietokoneet.

Ajojahti saa alkunsa, kun vuonna 1989 LoD-jäsen Prophet murtautui BellSouth AIMSX tietokoneverkkoon ja lataa koneelleen E911 dokumentin, joka kertoo puhelinlaitoksen hätäpalveluverkosta. Hän luovuttaa dokumentin Knight Lightningille, joka julkaisee sen Phrack-uutiskirjeessä. Tästä seuraa valtava määrä pidätyksiä ja oikeudenkäynti, joka ei kuitenkaan johda toivottuun tulokseen. E911 dokumentti osoittautuu suhteellisen hyödyttömäksi ja jopa julkiseksi ja oikeudenkäynnissä syytetään sen varastamisesta, vaikka alkuperäinen versio jäi yhä BellSouthille.

Tammikuussa 1990 MoD-ryhmää syytetään tammikuun 15. Martin Luther King -päivän AT&T maanlaajuisesta puhelinverkon kaatamisesta. Todennäköisesti verkon kaatuminen johtui ohjelmistovirheestä, mutta sen seurauksena salainen palvelu teki ratsiat Phiber Optikin, Acid Phreakin ja Scorpionin luo New Yorkissa. Ryhmän johtaja Phiber Opktik sai vuoden tuomion.

Massiivinen operaatio kuitenkin onnistuu siivoamaan osan hakkereista pois verkosta ja hajottamaan vanhat hakkeriryhmät. Operaation tarkoitus lienee ollut antaa viesti hakkereille, että heidän toimiaan tarkkaillaan ja niistä on seurauksia. Operaatio herättää paljon kysymyksiä siitä, mikä on oikeasti kiellettyä verkossa ja mikä ei. Liittovaltion ja salaisen palvelun toimista närkästyneenä näitä kysymyksiä ajamaan perustettiin Electronic Frontier Foundation [Ste94].

5 Kevin Mitnick

Maailman tunnetuin hakkeri lienee 36 -vuotias Kevin Mitnick, joka vapautui tammikuussa vuonna 2000 viiden vuoden vankilatuomiosta ehdonalaiseen. Kiinni Mitnick joutui 2,5 vuoden jahdin jälkeen, jolloin FBI pidätti hänet japanilaissyntyisen tietokoneasiantuntijan avustuksella. Asiantuntija alkoi jäljittää Mitnickiä havaittuaan tämän varastaneen hänelle kuuluvia tiedostoja.

Ensimmäisen kerran Mitnick joutui vankilaan tietokonerikoksesta ja murrosta 17-vuotiaana. Mitnick tunkeutui tovereineen puhelinyhtiö Bellin tietokonekeskukseen valehtelemalla vartijoille olevansa yhtiön työntekijä. Nuoret pääsivät tilaan, josta he onnistuivat anastamaan listan käyttäjätunnuksia ja salasanoja. Kiinni jengi jäi, kun hylätty tyttöystävä kävi kertomassa poikien puuhista poliisille.

Vuonna 1983 Mitnick tutustui kohtalokkaasti hakkeritoveriinsa Lenny DiCiccoon. Heidät pidätettiin samana vuonna murtautumisesta ARPAnetin kautta Pentagonin tietokoneisiin. Vuonna 1984 Mitnick teki luottokorttiväärennöksiä ja seuraavana vuonna hän jäi kiinni tunkeutumisesta NSA:n (National Security Agencyn) koneisiin DiCiccon työpaikalta. Vuonna 1987 Mitnick joutui uudelleen poliisin kynsiin käytettyään tekaistuja puhelinkortteja. Kotietsinnässä selvisi, että hänellä oli hallussaan luvattomia ohjelmistoja. Tuomioksi tuli tällöin 36 kuukautta ehdonalaista.

Seuraavan kerran Mitnick joutui oikeuteen yritettyään varastaa modeemiyhteyden kautta VMS käyttöjärjestelmän DEC:n tutkimuslaitokselta Paolo Altosta DiCiccon kanssa. Vaikka murtoyritys havaittiin miltei heti, Mitnick ei jäänyt kiinni, koska hän oli peukaloinut puhelinkeskusta eikä FBI kyennyt siksi jäljittämään puheluja. Kaiken lisäksi hän seurasi koko ajan toisella mikrolla kuinka lähellä jäljittäjät olivat ja ohjasi heidät viimein väärään osoitteeseen. Lopulta Mitnick jäi kiinni DiCiccon käryttämänä. DiCicco oli tympääntynyt rikoskumppaninsa tapaan hakkeroida hänen työpaikaltaan. Tuomioksi tuli vuosi vankeutta ja kuuden kuukauden vieroittamiskurssi tietokoneriippuvuudesta. Vuonna 1995 Mitnick tunkeutui ohjelmoijille, journalisteille, taiteilijoille, ym. tarkoitettuun WELL portaaliin. Samana vuonna japanilainen asiantuntija Tsutomu Shimomura jäljitti Netcomista luottokorttitietoja varastaneen Mittnickin, joka tällä kertaa myös onnistuttiin pidättämään [Shi04].

6 Hakkerointi Suomessa

Suomessa hakkerointi ei ole tuntematon ilmiö. Suomessa pidätettiin 1986 syksyllä ryhmä nuoria, jotka olivat tunkeutuneet mm. yliopistojen ja VTTK:n koneisiin. Tapausta uutisoitiin laajasti, suurin osa syytteistä hylättiin, koska oikeuden mukaan tunkeutuminen ei ollut toisen omaisuuden luvatonta käyttöä. Kaksi pääsyytettyä joutuivat tosin maksamaan noin 70 000 markkaa korvauksia käytetystä tietokoneajasta ja tapauksen selvittelystä. Lisäksi toinen sai 50 päiväsakkoa petoksesta ja luvattomasta tietokonepäätteen haltuunotosta (hän oli käyttänyt Jyväskylän yliopiston päätettä ilman lupaa) [Tuo87].

Tapaus herätti Suomessa pienen tietoturvabuumin. Ulkomaisia tietoturva-asiantuntijoita kiersi seminaareissa ympäri maata ja tietoturvaoppaita painettiin [Saa97]. Kymmenen vuotta myöhemmin tapahtunut hakkerointitapaus osoitti, ettei oppi ollut mennyt täysin perille.

Lähes 150 yrityksen ja yhteisön tietojärjestelmiin vuosina 1997-1998 laittomasti tunkeutunut jyväskyläläinen 25-vuotias ohjelmistosuunnittelija tuomittiin helmikuussa 2001 Jyväskylän käräjäoikeudessa viiden kuukauden ehdolliseen vankeuteen. Mies tuomittiin tietomurroista, tietojärjestelmien luvattomista käytöistä ja törkeistä viestintäsalaisuuksien loukkauksista.

TCB-hakkerina tunnettu opiskelija joutui maksamaan vahingonkorvauksia lähes 250 000 ja oikeudenkäyntikuluja noin 210 000 markkaa. Korvauksia saajina olivat muun muassa Helsingin, Kuopion, Oulun, Jyväskylän, Tampereen ja Turun yliopistot sekä Åbo Akademi, taideteollinen korkeakoulu, Helsingin kauppakorkeakoulu, valtion teknillinen tutkimuskeskus, teknillinen korkeakoulu sekä Tampereen ja Lappeenrannan teknilliset korkeakoulut. Tietomurtoja kohdistui myös muun muassa opetushallinnon palvelimiin, joiden kautta mies pääsi kuukausikaupalla lukemaan ainakin kahden ministerin henkilökohtaista sähköpostia.

TCB-hakkerin juttu osoitti sen, ettei tietoturvallisuuden taso valtion keskushallinnossa ole riittävästi hoidettu. Jos kaikkia suojauskeinoja olisi käytetty huolellisesti, ei hakkeri olisi päässyt järjestelmiin hänelle kuulumattomia käyttäjätunnuksia ja salasanoja tai erityisiä hakuohjelmia käyttämällä.

Vahingonkorvaukset arvioitiin ensialkuun miljooniksi, mutta tutkinnassa varmistui, ettei opiskelija hyötynyt murroista taloudellisesti tai tietoja myymällä. Syytteisiin yhtyi 25 yhteisöä ja yrityksiä, jotka vaativat noin 740 000 markan korvauksia ja asianomistajia oli kaikkiaan 139. Yliopistoille tästä aiheutui isoja harmeja siitä, että koko tietojärjestelmä oli tutkimuksia varten kaksi kolme päivää irti kytkettynä. Tapaus osoitti karusti sen, miten suuria vaurioita hakkerit voivat aiheuttaa järjestelmille. Kihlakunnansyyttäjän mukaan tapaus nosti tietoturvallisuuden tasoa yliopistoissa ja toivottavasti myös yrityksissä ja yhteisöissä.

7 Virusten historiaa

Virukset ovat nykypäivän hakkereiden normaaleja työkaluja, mutta 80-luvun alussa ne olivat lähinnä tutkijoiden tekemiä.

Viruksista tietokoneissa puhutaan ensimmäistä kertaa 1972 David Gerroldin kirjassa When Harley was One. Määritelmä ei vastaa kuitenkaan viruksen nykymääritelmää ohjelmasta, joka muokkaa muita ohjelmia lisätäkseen itsensä niihin. Tietokonematoista puhutaan ensimmäistä kertaa 1975 ilmestyneessa scifi-kirjassa The Shockwave Riderissa. John Brunnerin kirjassa "sähkömato elää ja lisääntyy jatkuvasti niin pitkään kuin tietokoneverkko on olemassa."1980 Xeroxin Palo Alton tutkimuskeskuksessa työskennellyt John Shoch rakensi ensimmäisen tietokonemadon. Se toimi samaan tapaan kuin Brunnerin mato.

Fred Cohen määritteli viruksen nykymääritelmän vuonna 1983. Etelä-Kaliforinian yliopistossa opiskellut Fred Cohen osallistui tietoturvaseminaariin ja sai idean tehdä tietokoneviruksen. Hän teki viikossa yksinkertaisen viruksen, jonka hän esitteli luokalleen. Hänen opettajansa professori Len Adelman, ehdotti luomuksen nimeksi tietokonevirusta. Tohtori Cohenin gradu ja myöhäisempi tutkimus keskittyi pääasiassa viruksiin [Spa92].

Myöhemmin sai luvan kokeilla virustaan yliopistonsa VAX-tietokoneessa. Järjestelmä menehtyi virusinfektioon keskimäärin puolessa tunnissa tartunnan saamisesta. Tulos oli niin hätkähdyttävä, että yliopisto kielsi kokeiden jatkamisen [Bis92].

Viruksia oli ollut olemassa kuitenkin jo niinkin varhain kuin 1982 Apple II tietokoneessa. Elk Cloner -virusta pidetään ensimmäisenä varsinaisena viruksena, joka oli tehty laboration ulkopuolella. Virus sijaitsi levykkeillä ja levyn joka 50. käyttökerralla kirjoitti näytölle varsín harmittoman runon: "Elk Cloner: The program with a personality

It will get on all your disks It will infiltrate your chips Yes it's Cloner!

It will stick to you like glue It will modify ram too Send in the Cloner!"

Ensimmäinen PC-virus ilmestyi 1987 (c)Brain-nimellä. Virus kopioi itsensä levykkeiden buuttisektorille.

Marraskuun 2. 1988 Robert Morris päästi valloilleen madon, joka kaatoi kymmenesosan koko Internetistä, mikä tarkoitti siihen aikaan 6000 tietokonetta. Tämä Morris-mato synnytti USA:ssa CERT:n (Computer Emergency Response Team) vastaamaan tulevaisuudeen uhkiin. Morris oli ensimmäisiä, jotka tuomittiin Computer Fraud and Abuse Act perusteella. Hän sai 10000 dollarin sakot ja 3 vuoden ehdollisen tuomion ja 400 tuntia yhteiskuntapalvelua. Hän säästyi kovemmalta tuomiolta, sillä mato ei tuhonnut tietokoneiden tiedostoja. Vahingot olivat kuitenkin 15 miljoonan dollarin arvoiset.

Seuraavat merkittävät virukset olivat 1998 ilmestynyt CIH-virus, Melissa 1999 ja 2000 VBS/Loveletter virus olivat ensimmäisiä viruksia, jotka iskivät Internet-ajan kotikäyttäjien sähköposteihin massoittain ja toivat virusongelman koko kansan tietoisuuteen. Suuri osa viruksista on kohdistettu nimenomaan Microsoftin käyttöjärjestelmiä ja ohjelmistoja kohtaan.

Tänä vuonna iskenyt MyDoom-mato pitää hallussaan nopeimmin leviävän Internetmadon ennätystä [Wik04].

8 Haktivismin aika

1990-luvun lopulla hakkerointi sai uusia piirteitä. 1980-perustetuttujen ryhmien jäsenet olivat kasvaneet aikuisiksi ja osa heistä halusi käyttää taitojaan aatteiden tai poliittisten viestien välittämiseen. Ensimmäinen haktivismi tapaus oli 1999 Kosovon kriisi. Serbialaiset hakkerit kaatoivat NATOn palvelimen pari päivää sodan alettua. Kalifornialainen hakkeri puolestaan teki vastaiskun Jugoslavian hallituksen web-sivuille. Hakkerit ryhmittyivät sotaa koskevan kantansa mukaan: venäläiset ja kiinalaiset hyökkäsivät yhdysvaltalaisia vastaan, kun taas albanialaiset ja länsimaalaiset hyökkäsisvät serbialiaisille sivuille. Jotkut itäeurooppalaiset levittivät lisäksi viruksia, joissa oli NATOn vastainen poliittinen viesti [Him00].

Yhdysvaltain parhaimmin suojatut Valkoisen talon whitehouse.gov isäntänimen alla olevat internet-palvelimet joutuivat toukokuun 4. päivänä vuonna 2001 niin kutsutun. dos-hyökkäyksen (denial of service) kohteeksi. Pahantekijät onnistuivat tempussaan niin hyvin, että palvelimet menivät lopulta tukkoon ja koko palvelu halvaantui kolmeksi tunniksi. Dos-hyökkäyksen periaate on hyvin yksinkertainen: hakkerit tukahduttavat kohdepalvelimen lähettämällä sille niin paljon kyselyjä, että se ylikuormittuu eikä enää kykene vastaamaan oikealla asialla oleville työasemillekaan.

Dos-isku voidaan laukaista ohjelmallisesti samaan aikaan useilta kymmeniltä, jopa sadoilta palvelimilta. Tällaista jaettua ddos (distrubted dos) hyökkäystä vastaan on vaikea suojautua edes palomuurilla, koska ne perustavat hyökkäyksen tunnistuksen lähettävän laitteen ip-osoitteeseen. Ddosilla tukittiin Yahoon ja CNN:n nettipalvelut viime vuonna, Microsoft koki saman kohtalon kuluvan vuoden tammikuussa . Yhdysvaltalainen tietoturvayritys iDefense väittää, että tempun takana olisivat olleet kiinalaiset hakkerit. Internetin keskustelualueilla hyökkäyksen arvellaan olevan kostotoimi sen vuoksi, että amerikkalaiset "kyberpatriootit"ovat iskeneet vakoilukonevälikohtauksen takia kiinalaisiin nettipalvelimiin ja muunneelleet niiden sivustoja.

Kiinan ja Yhdysvaltain välillä näyttäisi olevan tieto noin 460:stä web-palvelusta, joiden kotisivuja on sotkettu omilla muunnoksilla. Yksi tämän "kybersodan"sankareista on "pr0phet"aliasta käyttävä hakkeri, joka on todennäköisimmin useamman eri henkilön itselleen omima nimi. Pr0phet on saanut Yhdysvalloissa laajaa julkisuutta, mikä lienee ollut koko operaation tarkoituskin [Mar01].

Internetistä on tullut maailmanlaajuinen graffitiseinä. Jatkossa voi olla varma, että tulevien kriisien yhteydessä hakkerit tuovat mielenilmauksensa näkyville haluamassaan muodossa kaataen palvelimia tai julistaen viestiään haluamillaan saiteilla.

9 Hakkeroinnin vaikutus tietoturvan kehitykselle

Hakkeroinnilla on ollut positiivisia ja negatiivisia vaikutuksia. Hakkerit ovat paljastaneet tietoturva-aukkoja ohjelmistoissa ja yrityksissä, joita paikkaamalla yleinen tietoturvallisuus on parantunut. Myöskin yleinen suhtautuminen tietoturvaan on levinnyt laajemmalle. Enää salasanat eivät jää oletusanoiksi eikä myöskään suositella salasanaksi käytettävän omaa nimeään saatikkaa mitään sanakirjasta löytyvää sanaa. Tämä olisi varmaan 1980-luvulla ollut täysin ennen kuulumatonta.

Hakkeriuutisoinnin myötä maailma tuntuu kuitenkin turvattomammalta. Ajatus, että jossain verkossa vaanii hakkeri juuri sinun konettasi, sinun sähköpostiasi tai sinun luottokorttitietojasi, saa olon tuntumaan turvattomalta, vaikkei siihen ehkä syytä olekaan. Jatkuvan uhan kotikäyttäjille muodostavat alati uusiutuvat tietokonevirukset.

10 Yhteenveto

Hakkereiden historia alkaa puhelinfriikeistä, jotka käyttivät hyväkseen puhelinverkon keikkouksia soittaakseen ilmaisia puheluita USA:ssa 1970-luvulla. 1980-luvulle tultaessa hakkerointi (tietomurto) sai varsinaisen merkityksensä friikkien siirtyessä puhelinverkoista tietoverkkoihin. Syntyi useita hakkeriryhmiä, joiden tarkoituksena oli vaeltaa vapaana tietoverkoissa. Myöhemmin lait ja virkavalta alkoivat jahdata näitä ryhmiä. 1990-luvulla hakkerointi sai enemmän rikollisia piirteitä ja siitä jaettiin ensimmäisiä kovia tuomioita. Internetin leviämisen myötä 1990-luvun puolivälin jälkeen kotikäyttäjillekin tulivat hakkereiden virukset varsin tutuiksi.

Hakkeroinnin historia henkilöityy muutamien ihmisten ja ryhmien ympärille (Captain Crunch, Kevin Mitnick, Legion of Doom), joita voi olla mainitsematta hakkeroinnista puhuttaessa.

Lähteet

Bis92 Bishop, M., An overview of computer viruses in a research environment. Tekninen raportti, 1992. URL `citeseer.nj.nec.com/bishop92overview.html`.

Dra04 Draper, J., cap'n crunch in cyberspace. `http://www.webcrunchers.com/crunch/`. [25.02.2004]

Him00 Himanen, P. *Hakkerietiikka ja informaatioajan henki*, sivu 91. WSOY, 2000.

Mar01 Martin, B., Defaced commentary - cyberwar with china: Self-fulfilling prophecy. `http://www.attrition.org/security/commentary/cn-us-war.html`. [25.02.2004]

Par83 Parker, D. *Fighting Computer Crime*, sivut 170–192. Charles ScribnerŽs Sons, 1983.

Ros71 Rosenbaum, R., Secrets of the little blue box. *Esquire Magazine*, sivu 116.

Saa97 Saarinen, J., Tietokonepelko teknologisen katselutavan ilmentymänä. `http://www.tuug.utu.fi/~jaakko/tutkimus/gradu/`. [25.02.2004]

Shi04 Shimomura, T., Takedown biography[b. `http://www.takedown.com/bio/mitnick.html`. [25.02.2004]

Spa92 Spafford, E. H., Computer viruses—A form of artificial life? Teoksessa *Artificial Life II*, Langton, C. G., Taylor, C., Farmer, J. D. ja Rasmussen, S., toimittajat, Addison-Wesley, Redwood City, CA, 1992, sivut 727–745.

Ste94 Sterling, B., The hacker takedown, 1994. `http://www.mit.edu/hacker/hacker.html`. [25.02.2004]

Tuo87 Tuomi, I. *Ei ainoastaan hakkerin käsikirja*, sivut 13–16, 143–146. WSOY, 1987.

Wik04 Notable computer viruses and worms. `http://en.wikipedia.org/wiki/Notable_computer_viruses_and_worms`. [25.02.2004]