

Tietokonevirusten toiminnallisuuden tutkiminen

Jonne Okkonen, TTV18S3
Joonas Niinimäki, TTV18S3

Harjoitustyö
Kyberturvallisuus, Jarmo Nevalainen
17.11.2019
Tieto – ja viestintätekniikka

Sisältö

1	Johdanto	3
2	Virusten historiaa 1960-1979	3
2.1	Vuodet 1980-1989	5
2.2	Vuodet 1990-1999	8
3	Virukset informaatioaikakautena 2000-2019	9
3.1	Korkeaprofiilisia viruksia	10
3.2	Tietokonevirusten trendit maailmalla	17
4	Tutkittavat virukset	20
5	Pohdinta	25
	Lähteet	26

Kuvat

Kuva 1	The Creeper tietokoneviruksen näyte.	4
Kuva 2	Elk-cloner tietokoneviruksen näyte.	5
Kuva 3	Cascade tietokoneviruksen näyte.	7
Kuva 4	CyberAIDS tietokoneviruksen näyte.	8
Kuva 5	Happy99 tietokoneviruksen näyte	9
Kuva 6	CryptoLocker-tietokoneviruksen näyte.	11
Kuva 7	ILOVEYOU-tietokoneviruksen viestinäyte.....	12
Kuva 8	MyDoom tietokoneviruksen näyte.	13
Kuva 9	Storm Worm tietokoneviruksen näyte.	14
Kuva 10	Sasser & Netsky tietokoneviruksen näyte.	14
Kuva 11	Anna Kournikova tietokoneviruksen näyte.	15
Kuva 12	SLammer viruksen näyte F-Securelta.....	16
Kuva 13	Stuxnet viruksen lähdekoodin osan näyte.....	17
Kuva 14	Kiristysohjelmien esiintyvyys maapallolla 2018.	18
Kuva 15	Coin-mining esiintyvyys maapallolla 2018.....	18

Kuva 16 Google Transparency Report trendit 2017.	19
Kuva 17 Esimerkki Windows 7 Virtuaalikoneen asetuksista	21
Kuva 18 WannaCry haittaohjelman ikkuna	22
Kuva 19 LoveLetterin ylikirjoittamia kuvatiedostoja	23
Kuva 20 Skynet viruksen kirjoittama viesti	24

1 Johdanto

Mitä ovat tietokonevirukset? Mistä ne tulivat? Miksi niitä on olemassa? Mitä ne tekevät? Tässä raportissa pyritään perehtymään tietokonevirusten toimintaan ja tutkia millä tavoin ne hyökkäävät turvattomiin päätelaitteisiin. Tietokonevirusten historia on lähes yhtä vanha kuin ensimmäiset elektroniset ja ohjelmoitavat tietokoneet ovat.

Comodo Antivirus sivuston artikkeli What is Computer Virus and its Types (Judge, K. 22.8.2019) määrittelee tietokonevirukset haittaa tavoitteliviksi itse-replikoituviksi ohjelmiksi, jonka tarkoituksena on saastuttaa alttiita laitteita virukselle ja varastaa käyttäjäpäänteen koneelta henkilön arkaluontoista dataa.

2 Virusten historiaa 1960-1979

Kuten aiemmassa johdantokappaleessa lyhyesti mainittiin, virusten historia on lähes yhtä pitkä kuin itse elektronisten ja ohjelmoitavien tietokoneiden historia on. Ensimmäinen elektroninen ja ohjelmoitava tietokone the Colossus keksittiin joulukuussa 1943 ja sen kehitti Tommy Flowers (Computer Hope, 8.2.2019).

Noin kaksikymmentä vuotta sen jälkeen John Von Neumann julkaisi artikkelin Theory of self-reproducing automata vuonna 1966 (Von Neumann, J. Theory of self-reproducing automata. 1966. haettu arkistosta 12.7.2010). Artikkelin käsitteli itsereplikoituvaa ohjelmaa, josta Von Neumann puhui luennoillaan.

The Creeper ja Wabbit

Ensimmäinen kokeilullinen tietokonevirus the Creeper system kirjoitti Bob Thomas vuonna 1971 työskennellessään BBN Technologies tutkimus – ja kehitysyrityksessä. Creeper saastutti (Thomas, C. Jean-Marc, R. The Evolution of Viruses and Worms. 2004) DEC PDP-10 tietokoneita, jotka käyttivät TENEX operointi järjestelmää.

Se hyödynsi AARPANET yhteyttä ja kopioi itsensä etäiselle laitteelle ja viesti saastuttamisen näytön viestillä ”I am the creeper, catch me if you can!”. Creeper ohjelma poistettiin Reaper nimisellä ohjelmalla (Deborah, R., Gangemi, G. T. Computer Security Basics. Kesäkuu 1991).



Kuva 1 The Creeper tietokoneviruksen näyte.

Vuonna 1974 Rabbit (tunnettiin myös nimellä Wabbit) virus oli enemmänkin haarukka pommi (fork bomb), eli eräänlainen palvelunestohyökkäys (virallisesti denial of service, DOS). Rabbit virus luo itsestään useita kopioita yksittäiselle tietokoneelle, kunnes se tukkii järjestelmän, näin vähentäen sen toimivuuskykyä ja lopulta saavuttaen sen kestokyvyn ja se kattaa tietokoneen (Snyder, D. The very first viruses, Creeper, Wabbit and Brain. InfoCarnivore. 30.5.2010).

ANIMAL

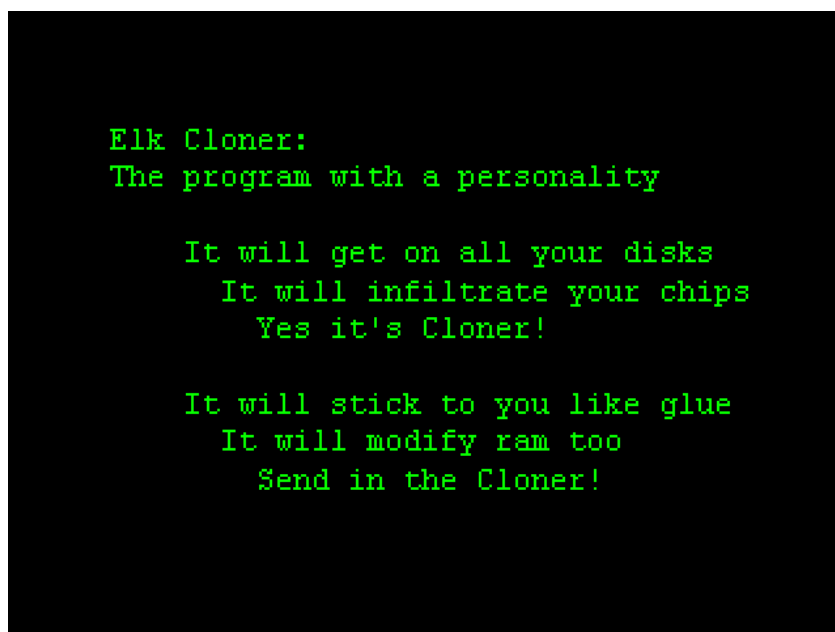
Huhtikuun 1975 John Walker kirjoitti ANIMAL ohjelman UNIVAC 1108 laitteistolle (Walker, J. ANIMAL Source Code. 1975). Ohjelmisto kyseli lukuisia kysymyksiä käyttäjältä ja yritti vastausten perusteella arvata mitä eläintä käyttäjä ajatteli.

Samalla liitännäinen ohjelma PREVADE pystyi luomaan itsestään ja ANIMAL:sta kopion kaikkiin hakemistoihin, mihin käyttäjällä oli pääsymahdollisuus. Se levisi useamman käyttäjän UNIVAC järjestelmissä, kun useampi samojen oikeuksia käyttävä käyttäjä havaitsi pelin ja kun kasettia käytettiin toisissa koneissa.

Ohjelma oli tarkoin koodattu välttämään tuhoja, ja sen leviäminen loppui, kun järjestelmäpäivitys muutti kansiotilaformaattia, jota PREVADE hyödynsi turvalliseen kopiointiin. Vaikka ohjelma oli harmiton, sitä pidetään ensimmäisenä troijalaisviruksena (Dewdeney, A. K. The Animal Episode. 21.2.1985). John Brunner keksi nimityksen ”mato (worm)” novellissaan The Shockwave Rider kuvaamaan tietokoneverkossa itsereplikoituvaa ohjelmaa (Brunner, J. The Shockwave Rider. Del Rey Books. Julkaistu 1975).

2.1 Vuodet 1980-1989

Vuonna 1981 ohjelma nimeltä Elk Cloner kirjoitettiin Apple II järjestelmille. Sen loi lu-kiolainen Richard Skrenta ja sen alkuperäisenä tarkoituksena oli olla kepponen. Ohjelma oli boot sector virus. Joka latasi koneen käynnistyessä itsensä koneen muistiin ja kun käyttäjä syötti puhtaan levyn ja ajoi catalog komennon, joka luki listan levyn tiedostoista kirjoitti ohjelma itsestään kopion tälle levyille. Tämän levyn avulla virus lähti leviämään eteenpäin. Virus oli ainoastaan ärsyttävä käyttäjälle ja aika harmiton verrattuna nykypäivän viruksiin. Julkisuuden tietämättömyys mitä haittaohjelmat olivat ja miten niitä voi turvata johtivat ensimmäiseen laajamittaiseen tietokoneviruksen leviämiseen (First virus hatched as a practical joke. Sydney Morning Herald. 3.9.2007).



Kuva 2 Elk-cloner tietokoneviruksen näyte.

Elokuu 1984 Ken Thompson julkaisee uranuurtavan paperin Reflections on Thrusting Trust missä hän kuvailee, miten hän muokkasi C-kääntäjän niin, että kun sitä käytetään rakentamaan tiettyä versiota Unix pohjaisesta käyttöjärjestelmästä, se luo takaoven kirjautumiskomentoon.

Kun sitä käytetään rakentamaan uusi kopio itsestään, se kirjoittaa sen takaoven lisäskoodiin silloinkin, kun kumpikaan takaovi tai takaoven lisäskoodi ei ole läsnä uuden kopion lähdekoodissa (Thompson, K. Communications of the ACM., Vol 27. s 761-763. Elokuu 1984.).

Vuonna 1986 Brain boot sector virus vapautetaan. Sitä pidetään ensimmäisenä IBM PC:hen käyvänä viruksena ja on vastuussa IBM PC:n virusepidemiasta. Sen loi veljekset Brasit Farooq Alvi ja Amjad Farooq Alvi Lahoren kaupungissa Pakistanissa (Leyden, J. PC virus celebrates 20th birthday. 19.1.2006).

Aktiiviset virusten vuodet 1987-1989

Vuodet 1987-1989 olivat vilkkaita vuosia viruksille. Ensimmäistä kertaa IBM alustalla Vienna niminen virus neutralisoitiin (Wentworth, R. Computer Virus! Digital Viking. Heinäkuu 1997).

Leigh virus Yalen yliopistolta US, Stoned Uudesta-Seelannista ja 1988 Ping Pong Italiasta ja ensimmäinen itsekryptaava tiedostovirus Cascade. Leigh pysäytettiin kampuksella ennen kuin se levisi pidemmälle. Cascaden leviäminen johti IBM kehittämään sen omaa antivirus tuotetta. Lokakuussa Jerusalem virus havaittiin Jerusalemissa. Se tuhosi kaikki ajotiedostot (Wentworth, R. Computer Virus! Digital Viking. Kesäkuu 1997).

```

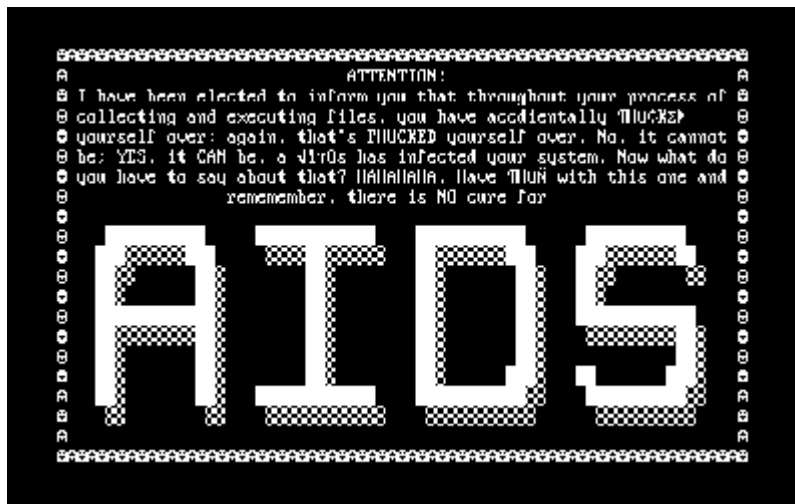
COUNTRY.S S      COUNTRY.TXT      DEBUG.EXE      EDIT.COM      EXPAND.
FDISK.EXEY      FORMAT. OM      KEYB.COM      KEYBOARD.SYS  MEM.EXEEXE
NETWORKS. X      NLSFUNCC XE     OS2.TXT      QBASIC.EXE    README.T
SCANDISK. X      SYS.COM.E       XCOPY.EXE    CHOICE.C M    DEFRAG.EXT
DEFRAG.H T      DELOLDOS.E E    DOSHELP.HLP  EGA.CPI O     EGA2.CPIXE
EGA3.CPI E T     EMM386.EXE      KEYBRD2. YS   MSCDEX.E E    SCANDISK.INI
ANSI.SYSLP E     APPEND.E E      CHKSTATESSYS DBLWIN.H      DELTREE.EXE
DISKCOMP. O      DISKCO M        DISPLAY.Y     DRUSPACE S    DRUSPACE EX
DRUSPACE.CL      DRUSPAPYX F     DRUSPACE S    MSD.EXECLP    REPL CE..XEE
STORE. H         HELP.HCE.C      DRIVER.SS S   EDIT.HLPOM    FAST ELPE X
STOPENEXE       FC.EXELP X      FIND.EXE.SYS  GRAPHICS COM  GR P I S
LP. OM.EX       HIMEM.SY.IO     INTERLNKYE E  I TER UR. XE  L . X
READF X C M      E MAKERS NE     MEMMAKER      M MMA ER N    M C M
FA OU B OM       E.COM.E         MOVE E H      OO L          P . X
HE C 3           DR UE.S S      SE E E        E              S E
LO I L 6P        R N.E E       M H           S
MON M X          O .C M      F X           S
QBASIC.          U B          O 6           A
SMARTDR. 1 ( M    X4,300 . . . . . A H C .
TREE.CO. M M      Y9 0 4 TVER . . . . . ABEL E .
COMMANDH ROR X    ARTMXEX . . . . . ODE. O E
C:\DOS>U 8 SAM I T O INTD.N. MST LS.. OWER E E
C:\DOS>M.P E UMA TMAC. M S NFIG03B L SHAR .EXDE IZER.EXEE
C:\DOS>.CEME ANFORME3,01 Ubytes.UMBLP SORT.EXEEI UBST.EXEPRO
C:\DOS>930fi e s)UTOEX30,84 , 2 Cbytes.freeP PRINT.EXEL F UNDELETE.EXE

```

Kuva 3 Cascade tietokoneviruksen näyte.

Marraskuussa 1987 SCA virus, bootti sektorin tason virus Amiga Computers ilmenee. Saastuttaessa se luo saman tien pandeemiseen viruskirjoitus kaaoksen. Pian SCA vapauttaa toisen huomattavasti tuhoisemman viruksen Byte Banditin. Joulukuussa Christmas Tree EXEC oli ensimmäinen laajalti häiritsevä ohjelma, joka halvaannutti kansainvälisellä tasolla tietoliikenneverkkoja.

Kesäkuussa 1988 CyberAIDS ja Festering Hate Apple ProDOS virukset levisivät piraatti BBS järjestelmistä saastuttaen valtavirran tietoverkkoja. Marraskuussa 1988 Morris mato saastuttaa DEC VAX ja Sun koneita, jotka käyttivät BSD UNIX ja olivat liitettyinä internettiin, ja siitä tulee ensimmäinen laajasti levinnyt mato. The Father Christmas mato iskee DEC VAX koneisiin, jotka käyttivät VAX/VMS ja olivat liitettyinä DECnet Internettiin, vaikuttaen tutkimuslaitoksiin ja Nasaan.



Kuva 4 CyberAIDS tietokoneviruksen näyte.

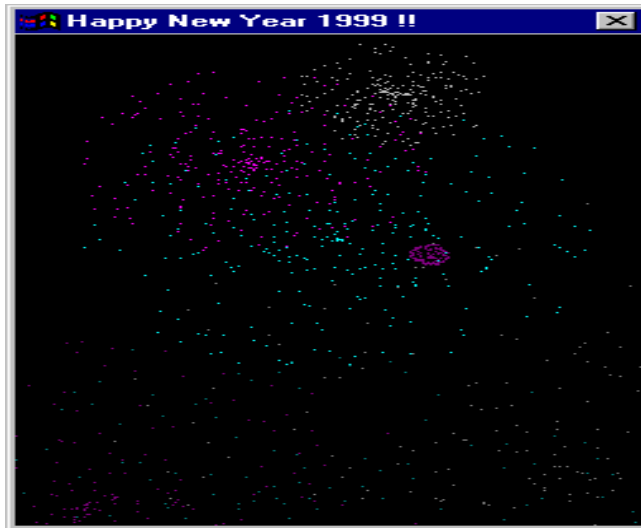
Lokakuu 1989 Ghostball, Friðruj Skúlason havaitsee ensimmäisen multi-partioidun viruksen. Se saastutti sekä ajettavat .COM tiedostot, että bootti sektorin MS.DOS järjestelmät. Joulukuussa AIDS Troijan, ensimmäinen tunnettu kiristysohjelma saastuttaa useat tuhannet levykkeet enkryptaamalla sisällön ja vaatimalla dekryptaamisohjelmasta 189 \$ maksua (Wentworth, R. Computer Virus! Digital Viking. Kesäkuu 1997).

2.2 Vuodet 1990-1999

Mark Washburn työskennellessään analyysia Vienna ja Cascade viruksista Ralf Burgerin kanssa, luo ensimmäiset polymorfisen virusten perheen The Chameoleon perhe vuonna 1990 (Washburn, M. Burger, R. Virus DOS Chameleon. 1990). Kesäkuussa Form niminen tietokonevirus eristetään Sveitsissä.

1992 Maaliskuussa Michelangelo virusta odotettiin luovan maailmanlopun maaliskuun 6. päivänä kun miljoonien koneiden tiedot katosiva valtamedian raporttien mukaan. Myöhemmissä arvioissa tuho oli pientä.

Vuonna 1995 ensimmäinen Macro virus nimeltä Concept luotiin ja se hyökkäsi Microsoft Word dokumentteihin (Glossary – Securelist. Viruslist.com. Haettu arkistosta 10.7.2010). 2.6.1998 ensimmäinen CIH virus ilmenee. Se on ensimmäinen tunnettu virus, joka pystyi poistamaan flash ROM BIOS sisällön.



Kuva 5 Happy99 tietokoneviruksen näyte.

Vuonna 1999 tammikuun 20. päivänä Happy99 mato ilmestyy. Se pystyi liittämään itsensä näkymättömästi sähköposteihin ja se muokkasi Windows 98 järjestelmän tiedostoja. 6.6.1999 ExploreZip mato paljastui, se tuhoaa Microsoft Office dokumentteja. Syyskuussa CTX virus eristetään. 30.12.1999 Kak JavaScript pohjainen mato hyödynsi Outlook Expressin bugia leviämiseen (Wscript KakWorm. Symatec. Haettu arkistosta 29.3.2012).

3 Virukset informaatioaikakautena 2000-2019

Informaatioaikakautena virusten suosio, määrä ja näkyvyys kuluttajan jokapäiväisessä elämässä on kasvanut ja korkeaprofiiliset virustartuntatapaukset ovat kasvattaneet yksityishenkilöiden ja yritysten tietoisuutta tietokoneviruksista ja kyberturvallisuudesta. Siitä huolimatta yksi keskeisimmistä kyberturvallisuuden ongelmista on se, että lähes ketään ei kiinnosta tietoturva.

Vuosituhanneen vaihteen jälkeen tietokoneviruksien muoto on laajentunut ja hyökkäykset käyttävät monia eri tapoja ja monia eri tarkoituksia. Termeihin alalla kuuluu valkohattu hakkereita, jotka ovat kyberturvallisuuteen erikoistuneita asiantuntijoita ja joiden tehtävä on ohjelmistojen, palveluiden ja yritysten tietoturvan penetraatio-testaaminen.

Harmaahattu hakkerit eivät suoranaisesti halua aiheuttaa ongelmia, mutta he saattavat rikkoa lakia ja eettisiä standardeja, ja he usein tavoittelevat jotakin itselleen, kuten työllistymistä.

Mustahattuhakkerit käyttävät viruksia kiristääkseen tai tuhotakseen haavoittuneiden koneiden omistajaa tai yritystä, jolle hän on töissä. Heidän tarkoituksensa on puhtaasti oman edun tavoittelu rahallisesti tai muuhun tarkoitukseen, ja he rikkovat tietoturvalakia päästäkseen tavoitteisiinsa.

3.1 Korkeaprofiilisia viruksia

Norton antivirus tiimin helmikuun 2016 blogipostauksen mukaan 8 vaarallisinta virusta vuosituhatosen vaihteen jälkeen ovat olleet Cryptolocker, ILOVEYOU, MyDoom, Storm Worm, Anna Kournikova, Slammer ja Stuxnet (The 8 Most Famous Computer Viruses of All time. Helmikuu 2016).

Cryptolocker

Cryptolocker on ransomware, eli kiristysohjelmisto, joka ottaa saastuneen käyttäjän tietokoneen kansiot panttivangeiksi. Vapautettu syyskuussa 2013, Cryptolocker levisi sähköpostiviesteihin liitetyn liitteen avulla ja se encryptasi tiedostot niin, että käyttäjällä ei ollut mahdollista saada pääsyä niiden sisältöön.

Hakkerit lähettivät yleensä noin muutaman sadan punnan tai jopa muutaman tuhat punnan rahavastineesta decryption avaimen uhrille. Muutamilla hakkerointiyrityksillä ja järjestelmänpalautusyrityksillä palautusohjelmisto toimi, mutta monissa tapauksissa uhri ei päässyt käsiksi tiedostoihinsa, jos hän ei maksanut lunnaita.



Kuva 6 CryptoLocker-tietokoneviruksen näyte.

Kesäkuu 2014 operaatio Torvar sai kiinni Evgenly Bogachev, Cryptolockerin viruksen luoneen hakkerijengin johtajan. FBI tarjosi 3 miljoonan dollarin palkkiota Bogachevista (Reward Announced for Cyber Fugitive. FBI National Press Office. 24.2.2015).

Käyttäjille arvioiduista kuluista on arvioitu aiheutuneen noin 30 miljoonan kulut 100 päivän aikana, kun virus oli aktiivinen (Jeffers, D. Crime pays very well: Cryptolocker grosses up to \$30 million in ransom. PC World. 20.12.2013).

ILOVEYOU

ILOVEYOU kuulostaa harmittomalta ja piristävältä viestiltä, mutta todellisuudessa kyse oli paljon salakavallammasta ongelmasta. ILOVEYOU on yksi kaikkien aikojen tunnetuimmista ja tuhoisimmista viruksista. Se lähti leviämään 5.5.2000 ja vuosituhannen alussa se oli silloin yksi vaarallisimmista viruksista. Nykyään sitä pidetään suhteellisen kesynä ja vaarattomana.

Osasyynä viruksen tehokkuudelle oli se, että vielä vuosituhannen vaihteessa haittaohjelmia pidettiin myytteinä ja erityisesti ilman käyttäjän huomaamista. Virus levisi sähköpostin kautta, minkä viestissä luki 'I love you.' Viestin konnotaatio oli tarpeeksi

herättämään uteliaiden ihmisten mielenkiinnon, vaikka he eivät tunteneet lähettäjä. Haittaohjelma oli liitteessä oleva mato 'LOVE-LETTER-FOR-YOU.TXT.vbs'.



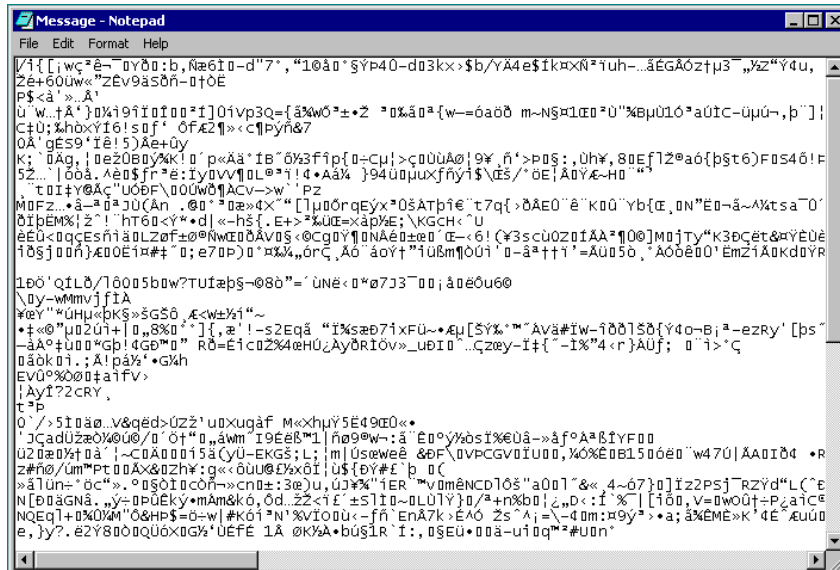
Kuva 7 ILOVEYOU-tietokoneviruksen viestinäyte.

Se ylikirjoitti järjestelmäkansioita ja henkilökohtaisia kansioita ja se levitti itseään jatkuvasti uudelleen. Vaikka viruksesta uutisoitiin otsikoissa maailmanlaajuisesti, ihmiset silti klikkailivat sitä. Virus oli niin tehokas, että se ylsi Guinness World Recordsiin kaikista tarttuvaisempana viruksena.

Tekijöiksi tunnistettiin filippiiniläiset ohjelmoijat Reonel Ramones ja Onel de Guzman, mutta heidän rikossyytteensä kaatui koska haittaohjelmien kirjoittamisesta ei ollut lakia vielä (The 8 Most Famous Computer Viruses of All time. Helmikuu 2016). Kuluarvioiksi on arvioitu 5 miljardia dollaria (The 8 Most Famous Computer Viruses of All time. Helmikuu 2016).

MyDoom

MyDoomia pidetään yhtenä tuhoisimmista viruksista. Kuten ILOVEYOU, MyDoom on yksi ennätyskirjaa nopeiden sähköpostiviestin välityksellä levinneistä matoviruksista. Se iski lähinnä isoprofiilisin teknologiayrityksiin kuten SCO, Microsoft ja Google aiheuttamalla palvelunestohyökkäys (Distributed Denial of Service, DDOS).

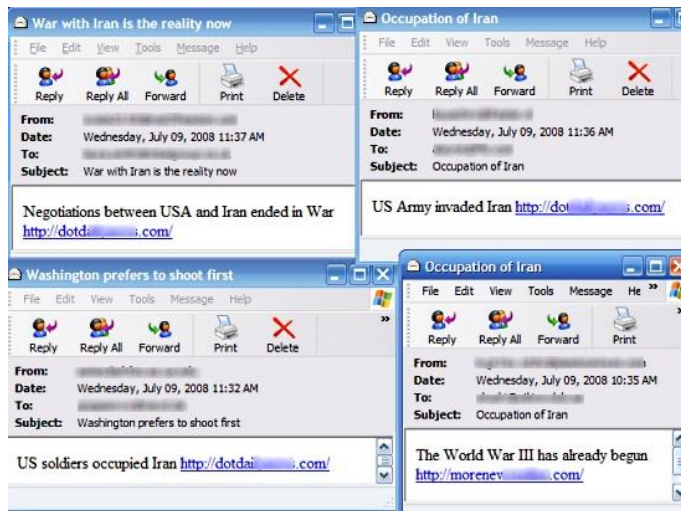


Kuva 8 MyDoom tietokoneviruksen näyte.

Sen lisäksi se lähetti roskapostia saastuneilta tietokoneilta. 2004 suurin piirtein 16-24% kaikista sähköposteista olivat saastuneita (MyDoom infects 19% of e-mails. 29.1.2004) ja kuluiksi on arvioitu noin 38 miljardia dollaria (The 8 Most Famous Computer Viruses of All time. Helmikuu 2016).

Storm Worm

Storm Worm levisi vuonna 2006 ja sitä pidetään harvinaisen rankkana hyökkäyksenä. Se levisi sähköpostin välityksellä viestinään '230 dead as storm batters Europe'. Linkkiä painamalla se avasi uutisen ja sieltä levisi Storm Worm Troijalaisvirus (virus, joka esittää laillista ohjelmaa tavoitteena saada pääsy käyttäjän koneelle).

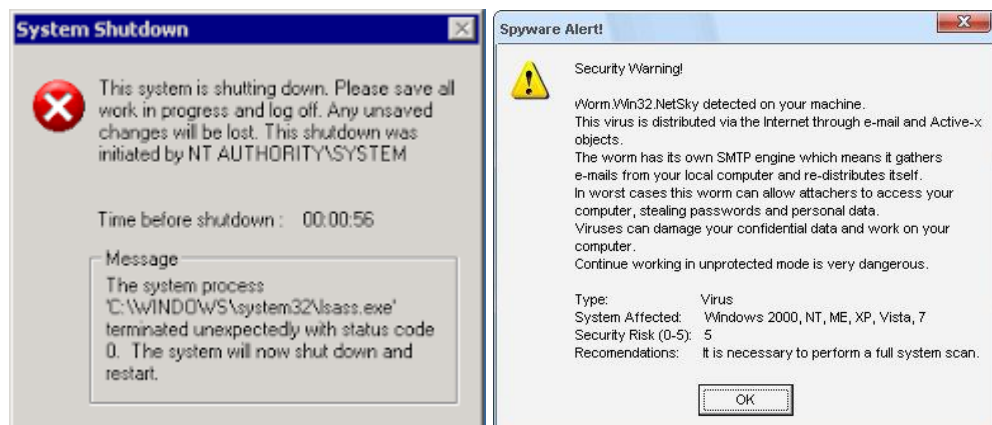


Kuva 9 Storm Worm tietokoneviruksen näyte.

Se muutti saastuttaneet koneet zombeiksi tai boteiksi, jotka jatkoivat viruksen lähettämistä roskapostina. Heinäkuun 2007 mennessä yli 200 miljoonaa sähköpostia oli saaneet kyseisien viestien.

Sasser & Netsky

17-vuotias saksalainen opiskelija Sven Jaschan loi madot Sasser & Netsky. Matojen samankaltaisuus sai asiantuntijat uskomaan, että ne on luonut yksi henkilö. Sasser levisi skannaamalla yksittäisten tietokoneiden IP osoitteita ja ohjeistamalla niitä lataamaan virus. Netsky oli sähköpostimato. Spekulaatioiden mukaan Jaschanin epäiltiin luoneen virukset ajaakseen kauppaa vanhempiensa tietokoneyritykseen. Lisäksi hän halusi myös nähdä levisikö hänen viruksensa nopeammin kuin MyDoom.

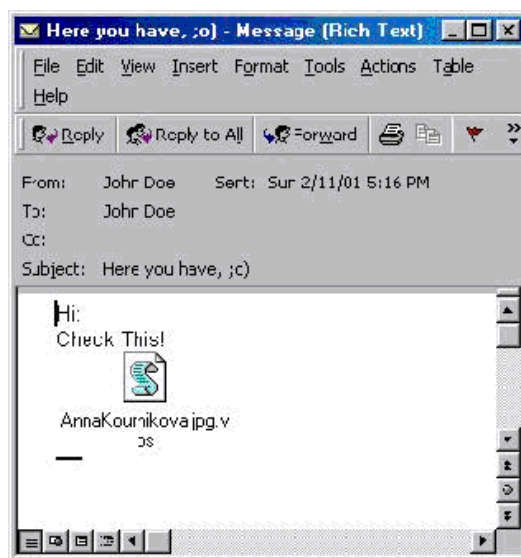


Kuva 10 Sasser & Netsky tietokoneviruksen näyte.

Se oli niin tehokas leviämään, että kolmasosa Taiwanin postitoimistoista piti pysähtyä, se lakkautti 130 suomen pankin haaraa ja pakotti reitti- ja transatlanttisten lentojen peruuttamiseen (The 8 Most Famous Computer Viruses of All time. Helmikuu 2016). Arvioutu hinnaksi noin 31 miljardia dollaria.

Anna Kournikova

Muista listan viruksista poiketen Anna Kournikova on niihin verrattuna laimea. 2000-2005 entinen tennispelaaja oli etsityimpiä termejä internetissä. Silloin hollantilainen 20-vuotias Jan De Witt loi viruksen vitsinä. Sen viestissä luki ”Here you have, ;0)” ja liitteenä oli AnnaKournikova.jpg.vbs.



Kuva 11 Anna Kournikova tietokoneviruksen näyte.

Vaikka virus ei tehnyt paljon tuhoja, De Witt antautui itse poliisille. Kaupungin pormestari sanoi, että kaupungin olisi oltava ylpeä tuottaessaan niin taitavan nuoren miehen ja tarjosi tälle töitä tekniikoiksi, kun hän oli valmistunut opinnoistaan. Hintalapuksi tuli 166 000 dollaria.

Slammer

Muista listan viruksista poiketen Slammer oli mato, joka keskittyi laajempiin kokonaisuuksiin eikä tähdännyt ainoastaan tietokoneita. Muutaman sekunnin kuluessa tartunnasta virus kopioi itsensä muutaman sekunnin välein. 15 minuutissa se oli tartuttanut lähes puolet kaikista internettiä pyörittävistä servereistä (Boutin, P. Slammed! Wired. 7.1.2003).

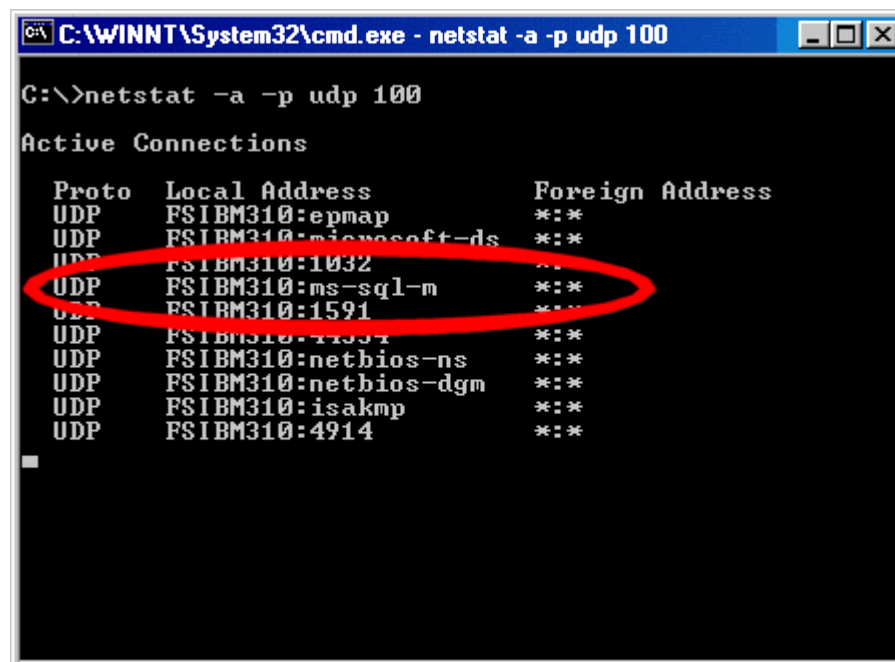


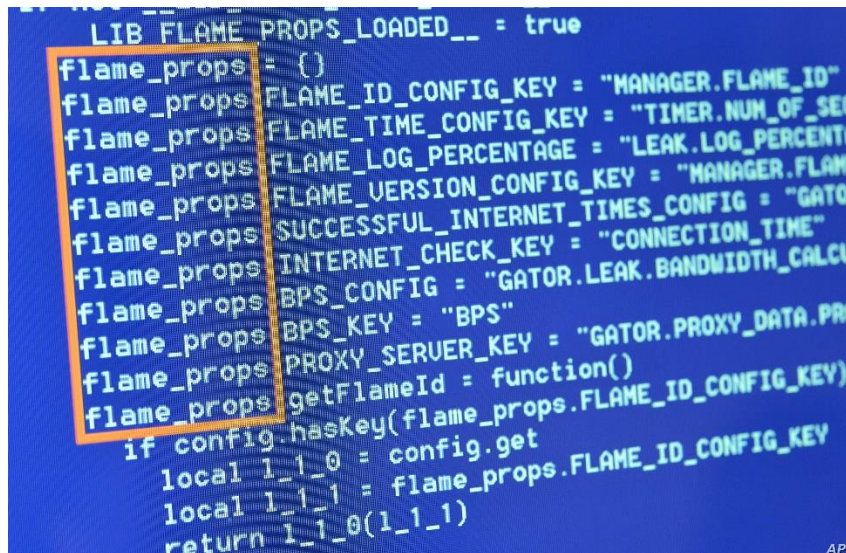
Image Copyright © F-Secure Corporation

Kuva 12 SLammer viruksen näyte F-Securelta.

Amerikan pankin automaattipalvelut kaatuivat, 911 palvelut menivät alas ja lentoja piti peruuttaa verkko-ongelmien takia. Se loi julkisuudessa paniikin, kuinka nopeasti se teki tuhoa palveluille. Arvioitujen tuhojen hinnaksi on arvioitu 1 miljardi.

Stuxnet

Stuxnet on yksi pelottavimmista ja tuhoisimmista viruksista. Sen loi Yhdysvaltojen valtion insinöörit (Zetter, K. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Wired. 11.3.2014) tavoitteena häiritä ydinohjuksien rakentamista Iranissa.



```

LIB FLAME_PROPS_LOADED__ = true
flame_props = {}
flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SEC
flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTA
flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME
flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR
flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCUL
flame_props.BPS_KEY = "BPS"
flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PRO
flame_props.getFlameId = function()
if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY)
local l_1_0 = config.get
local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
return l_1_0(l_1_1)

```

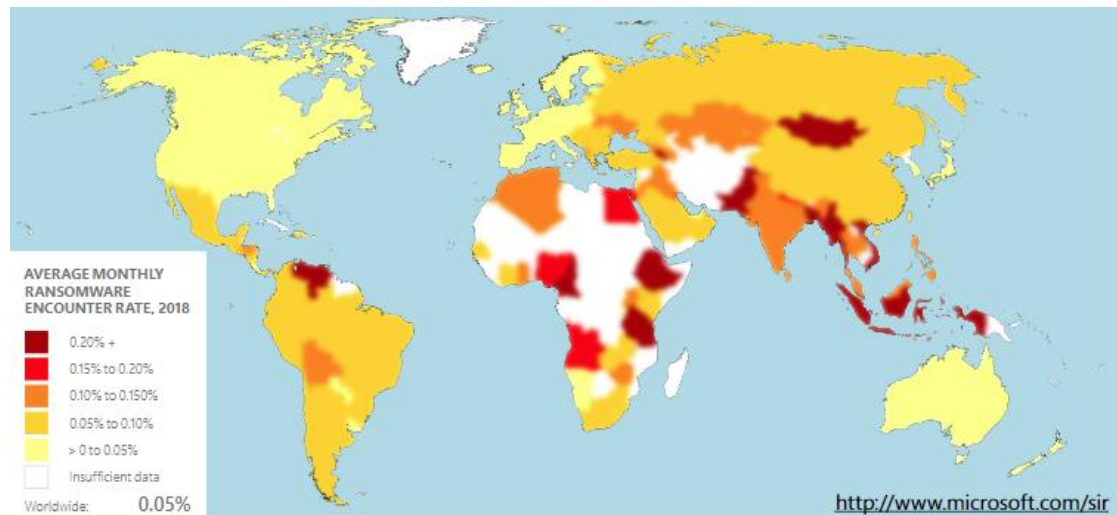
Kuva 13 Stuxnet viruksen lähdekoodin osan näyte.

Stuxnet levisi USB muistitikun välityksellä ja tavoitteli kontrolloimaan Iranin ydinvoimalaitoksen teollisuusjärjestelmien ohjelmistoa. Virus oli niin tehokas, että se aiheutti linkojen itsetuhoutumisen (Sanger, D. E. Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times. 1.6.2012).

3.2 Tietokonevirusten trendit maailmalla

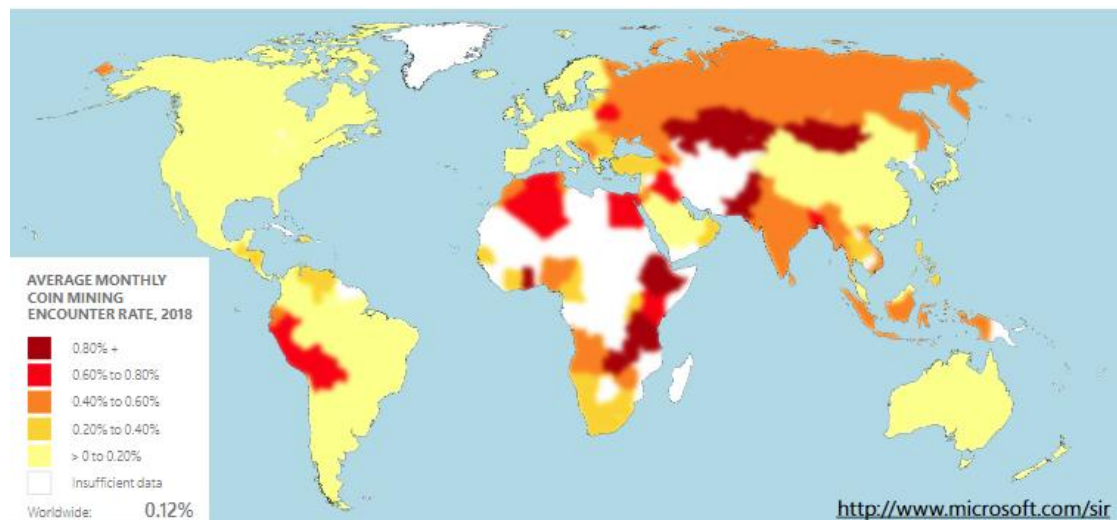
Microsoftin 24 edition 2018 julkaistun raportin mukaan vuosien 2017-2018 lopun aikana on tapahtunut asiantuntijoiden arvioinneista poikkeavia muutoksia virusten trendeihin ja yleisyyteen. Uusin hyökkäyksen muotoina on pilvipohjaiset hyökkäykset, sekä ohjelmistokehitykseen ja tuotantoon hyökkääviä haittaohjelmia.

Vaikka osa vanhoista metodeista on säilyttäneet relatiivisen suosionsa kuten kalastelu (eng. phishing), uusia metodologioita ovat suosiota saavuttaneet kryptovaluutan louhinta (eng. coin-mining). Resursseihin tähtäävistä hyökkäyksistä merkittävin oli Dofail, joka levisi 6.3.2018. Dofail hyödynsi virtuaalisen kryptovaluutan louhimista. Positiivisena kehityksenä koneoppimista hyödyntävät järjestelmät kehittyvät tunnistamaan ja estämään hyökkäyksiä.



Kuva 14 Kiristysohjelmien esiintyvyys maapallolla 2018.

2016-2017 vuosien aikana tapahtui useita korkeaprofiilisia kiristysohjelmahyökkäyksiä ja niiden määrän odotettiin kasvavan vuoden 2018 aikana. Vastoin ennako-odotuksia kiristysohjelmiston suosio laski jopa 60 prosenttia (Microsoft Security Intelligence Report, Volume 24. Joulukuu 2018). Syyksi on arvioitu julkisuuden kasvattamaa tietoisuutta viruksien torjunnasta ja varmuuskopioiden tärkeydestä.

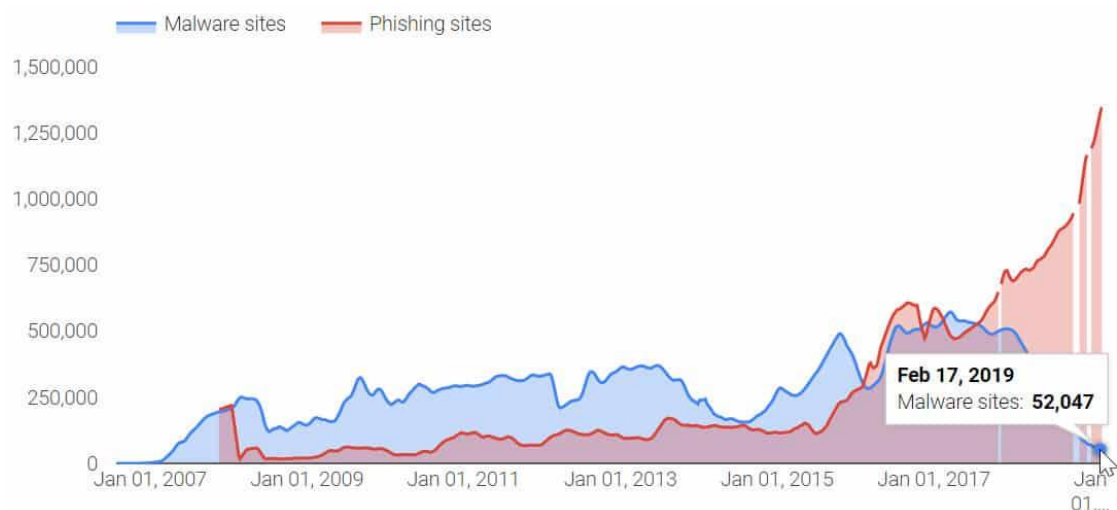


Kuva 15 Coin-mining esiintyvyys maapallolla 2018.

Kryptovaluutan louhimisen suosion kasvun on arvioitu johtuvan hyökkääjälle pienestä vaivasta, helppokäyttöisyydestä, haittaohjelmiston laajasta saatavuudesta ja pienestä näkyvyydestä uhrin tietokoneilla (Microsoft Security Intelligence Report, Volume 24. Joulukuu 2018).

Comparitech sivuston artikkelin Malware statistics and facts (Cook, S. Malware statistics and facts for 2019. Comparitech. 15.8.2019) viitatussa ISACA:n 2019 State of Cyber Security kyselyn mukaan yrittäjä asiantuntijat raportoivat 7% laskun haittaohjelmahyökkäyksissä vuonna 2018.

Googlen oman raportin mukaan haittaohjelmatartuntojen määrä on laskenut merkittävästi vuodesta 2017. Tämä näkyi varsinkin Googlen poistamien haittaohjelmasisivustojen määrässä (Safe Browsing: Malware and phishing. Google Transparency Report. 2017).



Kuva 16 Google Transparency Report trendit 2017.

SonicWallin 2019 tuottaman SonicWall Mid-Year Threat Report raportin mukaan uusien haittaohjelmien varianttien määrä on ollut 20 prosentin vuosittaisessa laskussa. Sen sijaan virustartuntojen määrä on kasvanut 4,8 miljardista 5,99 miljardiin vuoden sisällä (SonicWall Mid-Year Threat Report. Heinäkuu 2019).

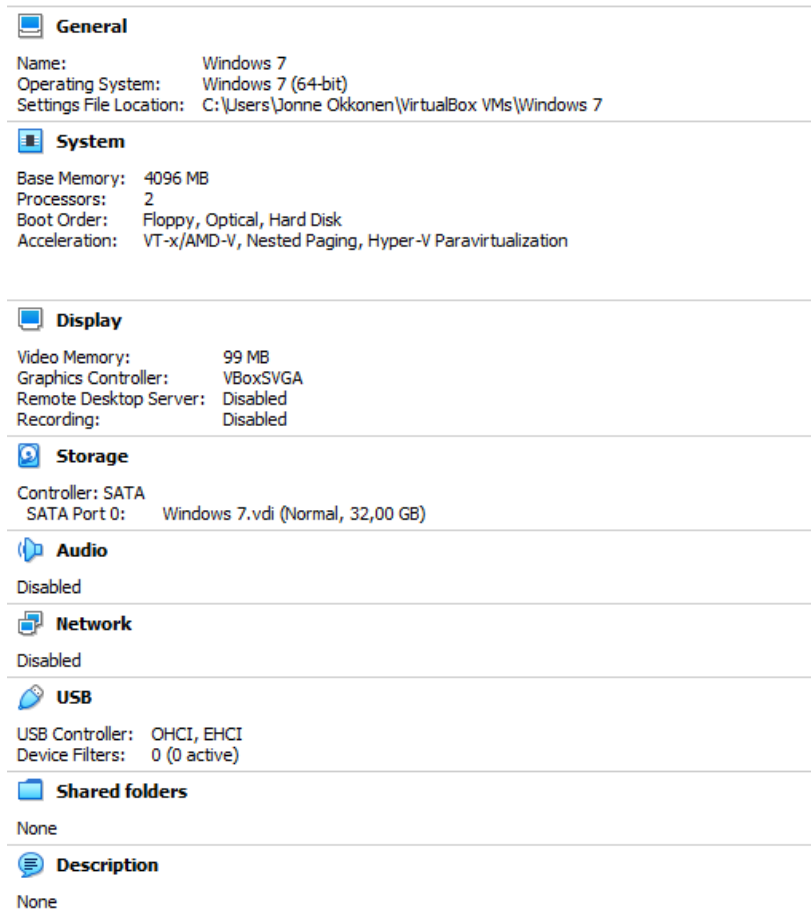
Symantec tietoturvapalveluita tarjoavan yrityksen oma raportti tukee SonicWallin löydöksiä. Symantecin raportin mukaan virusten uusien varianssien määrä laski jopa 63% jokavuotisella vauhdilla vuosien 2017-2018 välillä (Internet Security Threat Report 2019, volume 24th. Symantec. 2019).

WatchGuardin raportin mukaan zero-day haittaohjelmat olivat lähes 36% kaikista 2019 vuoden ensimmäisenneljänneksen viruksista. Muutosta vuoteen 2017 trendeihin ei zero-day virusten kohdalla tapahtunut (Infographic – Internet Security Insights Q1 2019. Watchguard. 2019).

4 Tutkittavat virukset

Harjoitustyötä varten tutkimme viruksien toimintaa tietokoneessa käytännössä. Käytimme virusnäytteitä Yuval Nativ'in GitHub repository:sta (<https://github.com/ytisf/theZoo>), johon hän oli koonnut satoja virusnäytteitä testattavaksi. Päätimme valita viruksia hieman eri kategorioista ja päädyimme valitsemaan seuraavat haittaohjelmat: WannaCry (ransomware), LoveLetter (computer worm) ja Skynet (DOS virus).

Ajoimme virukset Oraclen VirtualBox ohjelmaa hyödyntäen Windows 98 ja Windows 7 virtuaalikoneissa. Ennen virusten ajamista, valmistelimme virtuaalikoneet hyvin, asentamalla virustorjunta ohjelmiston, jolla pystyisimme testaamaan virustunnistusta viruksen ajamisen jälkeen, sekä loimme erilaisia tiedostoja WannaCry:lle ja LoveLetterille tuhottavaksi. Kun virtuaalikone oli valmisteltu, teimme siitä kopion, jottei valmistelua tarvitsisi toistaa joka kerta uudestaan ja tämän lisäksi suljimme kaikki mahdolliset yhteydet host-koneelle, kuten verkkokortti, jaetut kansiot ja leikkauspöytä.



Kuva 17 Esimerkki Windows 7 Virtuaalikoneen asetuksista

WannaCry

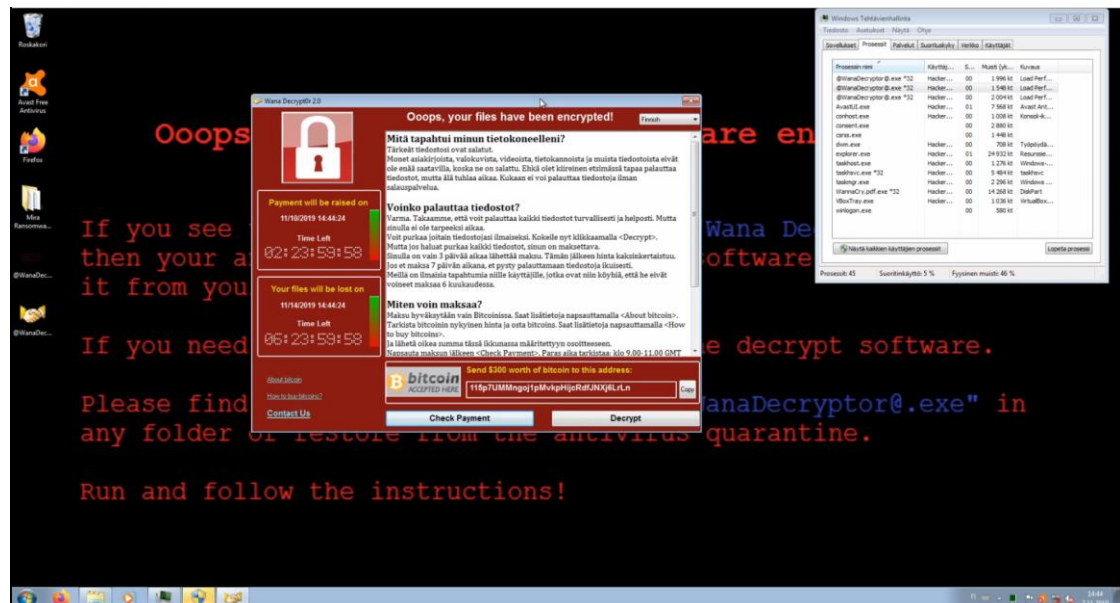
WannaCry Demo(<https://www.youtube.com/watch?v=Pu8Pu91o-zE>)

Kiristyshaittaohjelma (eng. ransomware) kategoriassa aioimme aluksi testata Mira nimistä haittaohjelmaa, koska F-Securella olisi ollut työkalu, jolla Miran salaamat tiedostot voitaisiin avata ja olisimme sitä voineet testata, mutta emme löytäneet helpposti näytettä tästä viruksesta, joten päädyimme valitsemaan WannaCry:n, joka oli julkisuudessa paljon vuonna 2017.

Aloitimme testauksen poistamalla virustorjunnan pois käytöstä ja purkamalla annetut virusnäytteet, jotka olivat pakattuna salasanalla suojatussa zip-kansiossa, jottei haittaohjelmia ajettaisi vahingossa. Purkamisen jälkeen ”naamioimme” haittaohjelman PDF-tiedostoksi tiedostopäätteellä, jonka avulla ohjelmaa esimerkiksi voitaisiin

levittää. Tiedoston avaamisen jälkeen ohjelma alkaa nopeasti toimia, salaamalla tiedostoja ja vaihtamalla taustakuvan, jossa kerrotaan, että tiedostosi ovat salattuja ja kuinka sinun tulisi toimia, jotta saat ne takaisin.

Seuraavaksi avautuu WanaDecryptor ikkuna, jossa kerrotaan useilla eri kielillä mitä on tapahtunut ja sinua pyydetään maksamaan lunnaita 300 dollarin edestä, jotta voit sit saada tiedostosi takaisin.



Kuva 18 WannaCry haittaohjelman ikkuna

Maksuaikaa on annettu 3 päivää ja mikäli et tänä aikana ehdi maksamaan hinta tuplaantuu ja jos et vieläkaan maksa lunnaita 7 päivän aikana. Tuhotaan palvelimelta salausavain, jonka avulla tiedostojen salaus purettaisiin ja tämän seurauksena tiedostoja ei enää saada palautettua.

Ohjelmassa on myös mahdollisuus purkaa salaus yhdestä satunnaisesta tiedostosta malliksi, joka antaa käyttäjälle uskoa, että maksamalla on tosiaan mahdollisuus saada tiedostot takaisin.

Toiminnan testauksen jälkeen kytkimme virustorjunnan takaisin päälle ja järjestelmän skannauksen jälkeen ohjelma tunnisti haittaohjelman WannaCry:ksi välittömästi. Tunnistuksen jälkeen ohjelma asetettiin karanteeniin ja poistettiin järjestelmästä, mutta tiedostot jäivät edelleen salatuiksi.

LoveLetter

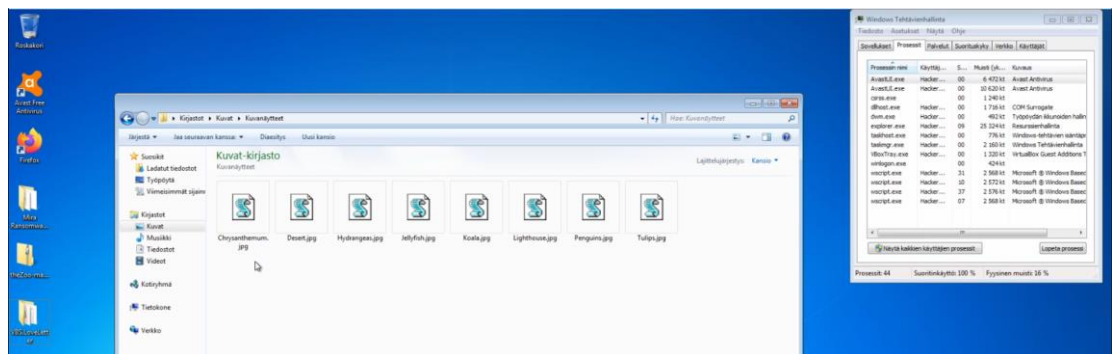
LoveLetter (<https://www.youtube.com/watch?v=5fcn2be6nSM>)

Seuraavaksi siirryimme LoveLetter tietokone matoon ja testin aluksi lataimme virtuaalikoneen kopion, joka oli jo valmiiksi valmisteltu, sekä poistimme virustorjunnan taas pois käytöstä. LoveLetter haittaohjelma saatiin samasta lähteestä kuin WannaCry ja testin aluksi purimme ohjelman salatusta zip-tiedostosta.

Scriptin ajamisen jälkeen ei tapahtunut visuaalisesti mitään, joten avasimme Windowsin Task Managerin, josta heti huomasi, että jokin käytti 100% suorittimen tehoista.

Prosessit ikkunasta näki tehoja käyttävän wscript.exe eli Microsoft Windows Based Script Host eli Microsoftin palvelu, joka ajaa Visual Basic Scriptit. Ohjelman päätarkoituksina on jakaa haittaohjelmaa eteenpäin sähköpostin avulla, jos käyttäjä on ottanut käyttöön Outlookin, sekä ladata koneelle troijalainen, joka vie koneelta tietoja, kuten salasanoja ja erilaisia tietoja koneesta. Tätä emme kuitenkaan voineet demonstroida, koska emme halunneet kytkeä konetta verkkoon.

Seuraavaksi menimme tarkastelemaan tiedostojamme, scripti oli ylikirjoittanut kaikki teksti- ja kuvatiedostot itsensä kopiolla, mutta video- ja äänitiedostoihin se ei ollut koskenut ollenkaan. Tämän jälkeen kytkimme virustorjunnan takaisin päälle ja heti ensimmäisellä skannauksella scripti löytyi ja se siirrettiin karanteeniin ja poistettiin koneelta.



Kuva 19 LoveLetterin ylikirjoittamia kuvatiedostoja

Skynet

Skynet (<https://www.youtube.com/watch?v=yM7nXW8oOrk>)

Viimeiseksi testattavaksi virukseksi päätimme valita jotain vanhempaa, jossa näkyisi minkä tyyppisiä ensimmäiset tietokonevirukset olisivat. Nopeiden googlailujen perusteella päädyimme Skynet nimiseen DOS-virukseen, joka on nimetty Terminator elokuva sarjan perusteella. Kun ohjelma ajettiin, se latasi itsensä muistiin ja tämän jälkeen se saastutti suoritettut exe-tiedostot kirjoittamalla itsensä tiedoston loppuun. Tämä ohjelma myös hidasti järjestelmän toimintaa ja aina kun saastutettuja ohjelmia suoritettiin virus näyttää näytöllä kuvassa 18 näytetyn viestin ja kun näppäintä painaa, muuttuisi näyttö mustaksi ja kone olisi jumissa niin pitkään kunnes se uudelleen käynnistettäisiin.



Kuva 20 Skynet viruksen kirjoittama viesti

Emme saaneet toistettu kaikkea ohjelman toimintaa, koska ohjelma olisi pitänyt ajaa pelkässä DOS-ympäristössä ja käyttämämme versio näytti vain Windows 98 ympäristössä viruksen näyttämän viestin eikä vaikuttanut koneen toimintaan juuri mitenkään.

5 Pohdinta

Raportin materiaalin perusteella voidaan havaita, että vaikka virusten monimuotoisuus on vähentynyt, niiden numeerinen määrä, näkyvyys ja tuhoisuus on kasvanut merkittävästi vuosikymmenien mittaan.

Ensimmäiset virukset ovat olleet enemmän leikkisiä käytännön pilaa tai vain hetimitäistä pientä haittaa aiheuttavia tietokoneviruksia, verrannollisesti 2000-luvun tietokonevirukset ovat rajuja ja aggressiivisia, ja niillä pyritään aiheuttamaan tuhoa ja haittaa saastuneille laitepääteille.

Myös eräät vanhat menetelmät ovat säilyttäneet suosiotaan pitkään ja erityisesti sähköpostin välityksellä lähetetyt virukset saavat edelleen suosiota haittaohjelmien levittäjien keskuudessa.

Tekoäly ja IoT tietoturva-aukot ovat yksi suurta huolta aiheuttava uusi teknologian alue. Toisaalta tekoälyä hyödynnetään myös tietoturvan parantamisessa ja sitä on jo tehty onnistuneesti. Kilpailu tulevaisuudessa haittaohjelmien tekijöiden ja tietoturvaasiantuntijoiden kanssa on kasvamassa tekoälyn myötä.

Raportissa myös saimme hyvin toteutettua haittaohjelmien testauksen suljetussa ympäristössä. Saimme todennettua viruksen toiminnan ja testattua antivirus ohjelmiston haittaohjelman tunnistusta ja poistoa.

Testausta olisi voinut parantaa luomalla paremman viimeistellymmän testiympäristön ja lisäämällä eristetyn yhteyden internettiin, jonka avulla olisi voitu paremmin todentaa esim. LoveLetter haittaohjelman toimintaa.

Lisäksi olisimme voineet testata useampia tai monimutkaisempia viruksia, joista olisi saanut hieman enemmän raportoitavaa, mutta saimme kuitenkin toteutettua hyvin harjoitustyön vaatiman tehtävän ja nyt tiedämme kuinka voisimme parantaa toimintaamme tulevaisuudessa.

Lähteet

(Infographic – Internet Security Insights Q1 2019. Watchguard. 2019. Lähde: <https://www.watchguard.com/wgrd-resource-center/infographic/internet-security-insights-q1-2019>.

Boutin, P. Slammed! Wired. 7.1.2003. Lähde: <https://www.wired.com/2003/07/slammer/>.

Brunner, J. The Shockwave Rider. Del Rey Books. Julkaistu 1975. Lähde: <https://web.archive.org/web/20080703121956/http://www.scifi.com/sfw/issue48/classic.html>.

Computer Hope, 8.2.2019. Lähde: <https://www.computerhope.com/issues/ch000984.htm>.

Cook, S. Malware statistics and facts for 2019. Comparitech. 15.8.2019. Lähde: <https://www.comparitech.com/antivirus/malware-statistics-facts/>.

Deborah, R., Gangemi, G. T. Computer Security Basics. Keskäkuu 1991. Lähde: https://books.google.fi/books?id=BtB1aBmLuLEC&printsec=frontcover&redir_esc=y#v=onepage&q&f=false.

Dewdeney, A. K. The Animal Episode. 21.2.1985. Lähde: <http://www.fourmilab.ch/documents/univac/animal.html>.

First virust hatched as a practical joke. Sydney Morning Herald. 3.9.2007. Lähde: <https://www.smh.com.au/technology/first-virus-hatched-as-a-practical-joke-20070903-gdr0fn.html?page=fullpage#contentSwap2>.

Glossary – Securelist. Viruslist.com. Haettu arkistosta 10.7.2010. Lähde: <https://www.symantec.com/security-center/writeup/2000-121908-3951-99>.

Internet Security Threat Report 2019, volume 24th. Symantec. 2019. Lähde: https://resource.elq.symantec.com/LP=6819?inid=symc_threat-report_istr_to_leadgen_form_LP-6819_ISTR-2019-report-main&cid=70138000001Qv0PAAS.

Jeffers, D. Crime pays very well: Cryptolocker grosses up to \$30 million in ransom. PC World. 20.12.2013. Lähde: <https://www.pcworld.com/article/2082204/crime-pays-very-well-cryptolocker-grosses-up-to-30-million-in-ransom.html>.

Judge, K. 22.8.2019. What is a Computer Virus and its Types. Lähde: <https://antivirus.comodo.com/blog/computer-safety/what-is-virus-and-its-definition/>.

Leyden, J. PC virus celebrates 20th birthday. 19.1.2006. Lähde: https://www.theregister.co.uk/2006/01/19/pc_virus_at_20/.

Microsoft Security Intelligence Report, Volume 24. Joulukuu 2018. Lähde:
<https://info.microsoft.com/SIRv24Report.html>.

Mydoom infects 19% of e-mails. 29.1.2004. Lähde:
<http://www.taipeitimes.com/News/worldbiz/archives/2004/01/29/2003096671>.

Reward Announced for Cyber Fugitive. FBI National Press Office. 24.2.2015. Lähde:
<https://www.fbi.gov/news/pressrel/press-releases/reward-announced-for-cyber-fugitive>.

Safe Browsing: Malware and phishing. Google Transparency Report. 2017. Lähde:
<https://transparencyreport.google.com/safe-browsing/overview?hl=en&unsafe=dataset:1;series:malware,phishing;start:-820540800000;end:1563087600000&lu=unsafe>.

Sanger, D. E. Obama Order Sped Up Wave of Cyberattacks Againsts Iran. The New York Times. 1.6.2012. Lähde:
https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=3&seid=auto&smid=tw-nytimespolitics&pagewanted=all&.

Snyder, D. The very first viruses, Creeper, Wabbit and Brain. InfoCarnivore. 30.5.2010. Lähde: <http://infocarnivore.com/the-very-first-viruses-creeper-wabbit-and-brain/>.

SonicWall Mid-Year Threat Report. Heinäkuu 2019. Lähde:
<https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/2019/SonicWall%20Cyber%20Threat%20Report-Mid-Year%20Update%20-%202019.pdf>.

The 8 Most Famous Computer Viruses of All time. Helmikuu 2016. Lähde:
https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html.

Thomas, C. Jean-Marc, R. The Evolution of Viruses and Worms. 2004. Lähde arkistoon:
<https://web.archive.org/web/20090517083356/http://vx.netlux.org/lib/atc01.html>.

Thompson, K. Communications of the ACM., Vol 27. s 761-763. Elokuu 1984.). Lähde:
<https://dl.acm.org/citation.cfm?id=358210>.

Von Neumann, J. Theory of self-reproducing automata. 1966. haettu arkistosta 12.7.2010. Lähde: <http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf>.

Walker, J. ANIMAL Source Code. 1975. Lähde:
<http://www.fourmilab.ch/documents/univac/animalsrc.html>.

Washburn, M. Burger, R. Virus DOS Chameleon. 1990. Haettu arkistosta 10.7.2010. Lähde:
<https://archive.ph/20120919103524/http://www.viruslist.com/en/viruses/encyclopedia?virusid=2008>.

Wentworth, R. Computer Virus! Digital Viking. Kesäkuu 1997.

Wscript KakWorm. Symantec. Haettu arkistosta 29.3.2012. Lähde:
<https://www.symantec.com/security-center/writeup/2000-121908-3951-99>.

Zetter, K. An Unprecedented Look at Stuxnet, the World's First Digital Weapon.
Wired. 11.3.2014. Lähde: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.