Tallinna Ülikool
Matemaatika-loodusteaduskond
Informaatika osakond

Margit Virkoja

ARVUTIVIIRUSED

Proseminaritöö

Juhendaja:
Jaagup Kippar

Tallinn 2006

SISUKORD

SISSEJUHATUS

Vaevalt on tänapäeval enam inimest kes ei oleks kuulnud ja ka ise kasutanud sõna arvutiviirus. Kui veel aastakümme tagasi tähistas see sõna mingit mütoloogilist olendit kellesse paljud suhtusid nii nagu suhtutakse UFOdesse, siis tänapäeval on asi muutunud. Arvutiviirustest on saanud meie igapäevaelu lahutamatu osa.

Siiski on ka praegu arvamusi, mis tekitavad paanikat ilma põhjuseta. Näiteks võib tuua Trooja hobuse, mida väga suur hulk arvutikasutajaid peab kõige hullemaks viiruseks maailmas. Tegelikkus on aga see, et Trooja hobune ei ole viirus vaid on nuhktarkvara. Ta võib sisaldada arvutit ja andmeid kahjustavaid ja/või hävitavaid koode, kuid reaalsem on võimalus, et viirus sisaldab Trooja hobust.

Masin, mida peetakse tänapäeva arvutite eelkäijaks, loomist alustati 1812. aastal. Aastal 1883 alustati selle masina tootmist. Nimeks oli tal Diferentsiaal mootor ja loojaks Charles Babbage. On teada, et sellele masinale viiruseid ei leidunud.

Jälgides arvutiviiruste arengut on oluline pidada silmas ka arvuti enda arengut. Tähelepanu peaks väärima järgmised aasta arvud:

- 1896 – sellel aastal asutas Herman Hollerith firma, millest peale mitmeid ühinemisi teiste firmadega, sai 1924. aastal IBM.
- 1970 – IBM valmistas esimese „floppy” seadme.
- 1976 – ehitati esimene Apple arvuti. Valmistajateks olid Steve Jobs ja Steve Wozniak.
- 1981 – valmistati esimene personaalarvuti: arvuti sellisel kujul nagu meie seda tunneme. Valmistajaks oli IBM.
- 1992 – ülemaailmselt hakati kasutama Internetti, kuigi leiutatud oli ta aastal 1962. Kuni seni ajani kasutati enamasti sõjaväele mõeldud APARNetti.

Täpselt nii, kuidas arenes arvuti arenevad ka viirused.

Oma töös käsitlen ma arvutiviiruste tüüpe, nende arengut ehk siis ajalugu ning vaatlen ka tuntumaid arvutiviiruseid.

1 ARVUTIVIIRUSTE TÜÜBID

Viiruste toimest lähtuvalt on väljatöötatud viiruste erinevad tüübid. Järgnevalt ongi välja toodud viiruste tüübid koos kirjeldusega mida vastavad viirused teevad.

1.1 „Süütud" viirused

„Süütud" on need viirused seetõttu, et nad ei hävita ega kahjusta programme ning andmeid. Oma kohalolekust annavad nad teada animatsioonide, helide, meloodiate, ekraanile ilmuvate teadete ja muude selliste tegevustega. Seda tüüpi viirused on programmeeritud aktiveeruma mingil kindlal tingimusel. Näitena võib välja tuua aktiveerumise mingi kindla kuupäeva, kellaaja, kõvaketta vaba ruumi või klaviatuurivajutuste arvu korral, aga ka mingi kindla programmi käivitamisel.

1.2 Andmeid hävitavad viirused

Andmeid hävitavaid viiruseid liigitatakse kaheks:

- Korraga hävitavad viirused, mis kirjutavad üle terve kõvaketta või osa sellest.
- Astmeliselt hävitavad viirused, mis kustutavad või rikuvad kõvakettal paiknevaid andmeid aegamööda.

Mõlemal juhul tavaliselt hävitatakse või rikutakse operatsioonisüsteemi failid ning arvuti ei suuda kas osaliselt või siis täielikult korralikult töötada. Tulemuseks on arvuti operatsioonisüsteemi uuesti installimine.

1.3 Programmifaile nakatavad viirused

Programmifaile nakatava viirused liigitatakse kaheks:

- Kohese mõjuga viirused, mis valivad ühe või mitu programmi ja nakatavad neid igakordsel käivitamisel.
- Residentsed viirused, mis peidavad end nakatunud programmi esmakordsel käivitamisel mällu ja seejärel nakatavad teisi aktiveeritud programme.

1.4 Spawing-tüüpi viirused

Seda tüüpi viiruste eesmärk on nakatada EXE-fail. Samas jääb fail muutmata. Viirus kasutab ära DOS-i omapära lugeda kõigepealt COM-faili ja seejärel alles EXE-faili, juhul kui mõlemad failid on sama nimelised. Viirus loob samanimelise viiruse koodi sisaldava COM-faili suurusega 8,064 baiti.

1.5 Parasiitviirused

Parasiitviirusteks nimetatakse viiruseid, mis kirjutavad oma koodi peremees-faili otsa (EXE- ja COM-failid). Seetõttu muutub fail viiruse koodi võrra pikemaks. Peale veel mõnede EXE- ja COM-failide nakatamist pannakse käima õige programm. Seda tüüpi viirused enamasti hävitavat koodi ei sisalda. Viiruse olemasolust annab märku faili suurenemine viiruse koodi võrra ja viirusele iseloomulik string faili lõpus. Samas ei ole uuemate viiruste korral alati võimalik faili suurenemisest lähtuda, sest peremees-faili koodi kokkupakkimisel faili suurus ei suurene.

1.6 Süsteemiviirused ehk boot-sektori viirused

Seda tüüpi viirused kirjutavad oma koodi boot-sektorisse. Seega tehes algkäivituse nakatunud kettalt aktiviseeritakse ka viirus. Sellised viirused on tavaliselt üsna destruktiivsed, sest kirjutades viiruse koodi boot-sektorisse, kirjutatakse üle seal eelnevalt asunud info ketta kohta.

1.7 Makroviirused

Makroviirused levivad ainult makrokeele kasutamist võimaldavates süsteemides. Seda tüüpi viiruste lemmikobjektideks on MS Wordi ja MS Exceli dokumendid.

1.8 „Antiviirus" viirused

„Antiviirus" viirused ei ole disainitud mitte ainult nakatama käivitusfaile, vaid sisaldavad ka teatud antiviiruse koodi. Sellised viirused sisaldavad mootorit, mis on võimeline võimetuks tegema või isegi kõrvaldama antiviiruse programme ja ka konkureerivaid viiruseid.

2 ARVUTIVIIRUSTE AJALUGU

Esimeste arvutiviiruste ilmumise kohta on ainult niipalju teada, et 1970-ndate keskpaiku olid viirused juba olemas. Idee arvutiviirustest ilmus aga palju varem. Lähtepunktiks võiks lugeda tuntud õpetlase John von Neumanni töid end isereprodutseerivatest matemaatilistest automaatidest. 1940-ndatel aastatel. 1951. aastal pakkus ta välja selliste automaatide loomisviisi.

Samas tuleks ära märkida, et teadlaste jõupingutused ei olnud ju mitte teoreetilise põhja loomisele arvutiviiruste tulevaseks arenguks. Nende eesmärgiks oli hoopis maailma täiustamine. Tolle aegsete õpetlaste uurimused said aluseks hilisematele robotitehnika ja tehisintellekti alastele töödele ning nemad ei ole ju süüdi, et tulevased põlvkonnad tehnilise progressi vilju kuritarvitasid.

2.1 1962. aasta

Sellel aastal loodi kompanii Bell Laboratories'i inseneride V.A. Vysotsky, G.D. Macilroy ja R. Morris poolt arvutimäng Darwin, mille põhimõtteks oli omavahel rivaalitsevate vastaspoolte ruumiuurimis-, paljunemis- ja hävitamisfunktsioone omavate programmikoopiate hävitamises ja võitlusvälja vallutamises.

2.2 1970-ndate aastate algus

Interneti eelkäijas – sõjalises arvutivõrgus APRAnet – avastati viirus Creeper. Tol ajal levinud operatsioonisüsteemile kirjutatud programm võis modemi kaudu iseseisvalt siseneda võrku ja edastada kaugarvutitele oma koopiaid. Oma kohalolekust teavitas viirus teatega „I'M THE CREEPER … CATCH ME IF YOU CAN". Samas oli see viirus oma pealetükkivusest hoolimata kahjutu.

Viiruse eemaldamiseks kirjutas keegi tundmatu programmi Reaper, mis oma sisult oli samuti viirus täites üksnes mõningaid antiviiruse funktsioone. Reaper otsis ja hävitas arvutivõrgus Creeperi viiruskehasid.

Tänapäeval ei oska enam keegi öelda, kas see oli esimeste viiruseloojate kahevõitlus või olid mõlemad programmid loodud sama autori poolt, kes oma viga parandada püüdis.

2.3 1974. aasta

Ilmus programm, mis sai nimeks Rabbit (Küülik). Mõeldud oli ta klassi CM 3 ja CM 4 arvutitele. Ainus mida see programm tegi oli paljunemine infokandjatel levimine, kusjuures oma paljunemiskiirusega õigustas ta igati oma nimetust. Rabbit kopeeris end nii kiiresti, et hõivas peagi kõik süsteemsed ressursid, vähendades samaaegselt süsteemi tootlikkust ja viies selle lõpuks hoopis rivist välja.

2.4 1975. aasta

Intsident toimus süsteemis Univac 1108 ja mõnes mõttes võib teda lugeda viiruslikuks. Tegemist oli mänguga „Pervading Animal". Mängu põhimõtteks oli arvuti püüd arvata ära mängija poolt mõeldud looma nimi. Selleks esitas ta mängijale küsimusi. Programm kätkes endas iseõppimisvõimet ning kui arvuti ei suutnud looma ära arvata tegi ta ettepaneku enda täiendamiseks ja suunavate küsimuste lisamiseks. Täiendatud mäng kirjutas üle vana versiooni ning kopeeris end lisaks sellele veel teistessegi kaustadesse, mistõttu peagi kogu ketas mängu koopiatega täitus.

Probleemi püüti lahendada varem tuntud Creeper-Reaper meetodiga. Loodi programmi uus versioon, mis otsis ja hävitas kõik oma eelkäija koopiad. Lihtsamaks lahenduseks osutus aga operatsioonisüsteemi Exec 8 uus muudetud failisüsteemiga versioon, kus mäng kaotas oma paljunemis võime.

2.5 1981. aasta

Sellel aastal hakkasid laialdaselt levima arvutid Apple II, mis äratasid ka viirusekirjutajates huvi. Nii juhtuski, et ajaloo esimene tõeliselt massiline arvutiviiruste epideemia toimus just Apple II arvutitel.

Diskettide alglaadimissektoritesse kirjutav buudiviirus Elk Cloner oli üsna mitmekülgne: pööras ümber ekraanipilti, pani vilkuma teksti ja väljastas mitmesuguseid teateid.

2.6 1983. aasta

Len Adelman kasutas seoses isepaljunevate arvutiprogrammidega esmakordselt terminit viirus. 10. novembril 1983. aastal demonstreeris arvutiviroloogia rajaja Fred Cohen USA-s Lehighi ülikoolis toimunud arvutiturvalisuse seminaril süsteemil

VAX 11/750 viirusesarnast programmi. Infoturvalisuse 7. konverentsil, mis toimus järgmisel aastal, andis ta teadusliku määratluse terminile arvutiviirus, defineerides seda, kui programmi, mis on võimeline „nakatama" teisi programme nende modifitseerimise teel, eesmärgiga juurutada neisse oma koopiad.

2.7 1986. aasta

Toimus esimene globaalne viirusepideemia IBM – ühilduvatel arvutitel. Peaaegu hetkeliselt levis üle kogu maailma 360-kilobaidiste diskettide alglaadimissektoreid nakatav viirus Brain. Viirus nakatas buutsektoreid ja muutis kettasildi fraasiks „(c) Brain". Samas ei rikkunud viirus ketastel olevat informatsiooni.

Braini eduka levimise tagas ennekõike arvutikasutajate ettevalmistamatus kohtumiseks arvutiviirustega. Sellel ajal ei olnud antiviirusprogrammid veel levinud ning kuna arvutiviiruseid oli väga vähe, siis ei järginud kasutajad ka turvalisuse põhireegleid. Efekti võimendatus oligi põhjustatud arvutiviiruste üldisest vähesest tuntusest ja uuritusest.

Braini loojateks olid vennad Basit ja Amjad Farooq Alvi Pakistanist, kes jätsid viirusesse oma nimesid, aadressi ja telefoninumbrit sisaldava tekstisõnumi. Vennad töötasid tarkvara tooteid müüvas firmas ja väitsid, et tahtsid viiruse abil välja selgitada tarkvarapiraatluse ulatust oma riigis. Kahjuks väljus eksperiment kontrolli alt ja levis üle maailma.

Huvitav on ka fakt, et Brain oli esimeseks nähtamatuks viiruseks – nakatanud kettasektori poole pöördumisel taastas ta märkamatult selle esialgse sisu.

Samasse aastasse jääb veel üks avastus. Nimelt avastas sakslane Ralf Burger programmide isepaljunemisvõimaluse lisades oma COM-formaadis koodi DOS-i täitmisfailidele. Esimene seda võimalust demonstreeriv viirus sai nimeks Virdem ja Ralf Burger tutvustas teda 1986. aasta detsembris arvuti „allilma" foorumil Chaos Computer Club, mis toimus Hamburgis. See foorum koondas VAX/VMS süsteemidesse sissemurdmisele spetsialiseerunud häkkereid.

2.8 1987. aasta

Ilmus viirus Vienna, mis oma päritolu ja peaaegu ülemaailmse levikuga tekitas suurt vastukaja ja tuliseid vaidlusi selle autorluse üle. Nime sai see viirus Franz Swoboda

käest. Swoboda oli ka see kes esimesena tõstis kära ja hoiatas uue isepaljuneva programmi eest. Kuna tema sõnum edastati paljude maailma juhtivate infoagentuuride poolt, siis sai sellele osaks ühiskonna valvas tähelepanu. Loomulikult üritati välja selgitada epideemia alguspunkti. Suudeti tuvastada, et Swoboda sai viiruse tuntud Ralf Burgerilt, kes aga seda eitas ja vastupidist väitis. Tulemuseks oli, et Vienna loojat ei õnnestunudki välja selgitada.

Samal aastal ilmusid veel mitmed IBM PC-dele kirjutatud viirust. Nendeks olid USA Bethlehemi linnas asuva ülikooli auks nimetatud kuulus Lehighi viirus, viirusteperekond Suriv, rida buudiviiruseid (Yale, Stoned, Ping-pong) ja arvutite ajaloo esimene isešifreeruv failiviirus Cascade.

Lehighi viirusega kaasneb tänapäeval aga iroonia kuna Lehighi ülikooli loetakse arvutiviroloogia hälliks. Samuti on tähelepanuväärne see, et see viirus oli esimene olulist kahju tekitav viirus. Kuna ülikoolis leidus piisavalt kõrgeltkvalifitseeritud virolooge, siis suudeti viirusepuhang kiiresti lokaliseerida. Teisalt soodustas epideemia likvideerimist ka viiruse enda toimemehhanism, mis nakatas üksnes süsteemseid faile COMMAND.COM, jätte kõik ülejäänud täitmisfailid puutumata. See vähendas viiruse levimis kiirust. Veel oli viirusele programmeeritud käsk peale neljanda faili nakatamist hävitada aktiivsel kettal olevad failid. Selle hävitustöö käigust hävitas viirus ka iseenda.

1980. aastate lõpus hakkasid kasutajad juba ka turvalisusele tähelepanu pöörama. Omandati ka tol ajal aktuaalne reegel, et arvuti nakatumise esimene tunnus on faili COMMAND.COM suurenemine. Tol ajal piisaski viiruse avastamiseks vaid selle faili suuruse jälgimisest.

Ära märkimist väärib veel tundmatu Iisraeli programmeerija poolt loodud residentsete failiviiruste perekond Suriv. Ka selle viiruse puhul on raske öelda, kas see oli nüüd kontrolli alt väljunud eksperiment või tahtlik kahjurlus. Kaldutakse arvama, et see oli siiski nurjunud eksperiment.

Suriv-1 nakatas COM-faile. Suriv-2 oli esimene viirus, mis suutis EXE-failidesse juurduda. Suriv-3 koondas endasse kahe esimese saavutused ning suutis nakatada võrdse eduga nii COM, kui ka EXE-faile

Šifreeritud viirus Cascade tekitas peale aktiveerimist „tähesaju" ja kõik ekraanil olevad sümbolid poetati alumisele reale. See viirus koosnes kahest osast – šifreerijast, mis muutis viiruse keha nii, et see nägi igas failis erinev välja, ja viiruskehast.

Cascade'i võib lugeda alalist programmikoodi mitteomavate, kuid oma funktsionaalsust säilitavate polümorfsete viiruste eelkäijaks.

Sama aasta detsembris leidis aste esimene massiline võrguviiruste epideemia. Põhjustajaks oli operatsioonisüsteemis VM/CMS levinud REXX keeles kirjutatud Christmas Tree. Viirus lasti võrku 9. detsembril ühes Lääne-Saksa ülikoolis. 13. detsembril halvas viirus võrgu, olles selle oma koopiatega ummistanud. Käivitamisel väljastas Christmas Tree ekraanile jõulukuuse kujutise ning saatis oma koopiad kõigile süsteemsetest failidest NAMES ja NETLOG leitud võrgukasutajate aadressidele.

2.9 1988. aasta

Ka sellel aastal jätkas Cascade põhjustades tõsise juhtumi IBM Belgia filiaalis. See seik andis IBM-ile tõuke oma antiviirusprogrammi loomiseks. Samas kasutati seda programmi kuni 1989. aasta septembrini ainult firma siseselt.

Olulisemaiks juhtumiks viiruste vallas sellel aastal oli siiski hoopis Suriv-4, mida rohkem tuntakse kui Jerusalem, poolt tekitatud globaalne epideemia. Viirus avastati samaaegselt paljudes firmades ja asutustes, kui ta reedel 13. mail aktiveerus ja kõikides nakatunud arvutites programmifailid hävitas.

Sellel aastal hakkasid ilmuma ka esimesed antiviirusprogramme loovad firmad. Need programmid olid tegelikult viiruskoodi unikaalse koodijärjestuse avastamiseks kontekstotsingut kasutavad skannerid. Samuti kasutati immunisaatoreid, mis muutsid programme nii, et viirused neid juba nakatunuteks pidasid ja enam ei puutunud. Kuigi seda tüüpi antiviiruseid levitati kas tasuta või müüdi väga väikse hinnaga, ei olnud nad eriti populaarsed ning seega ei aidanud viirusepideemiaid vältida.

22.aprillil toimus esimene antiviiruste võrgufoorum. Konverentsi Virus-L lõi Fred Coheni kolleeg Ken van Wyk.

Novembris toimus massiline võrguviiruse Morrise uss epideemia. Viirus nakatas üle 6000 USA arvutisüsteemi, praktiliselt halvates nende töö. Vea tõttu viiruse koodis

saatis ta võrgu teistele arvutitele oma koopiad ja need käivitanud võttis täielikult enda alla kõik võrgu ressursid.

Samal aastal loodi suurt populaarsust ja kuni 1998. aastani eksisteerinud tuntud antiviirusprogramm Dr. Solomon's Anti-Virus Toolkit.

2.10 1989. aasta

Ilmusid uued viirused – Datacrime, FuManchu ja viiruste perekonnad Vacsina ning Yankee. Ohtlikem neist oli Datacrime, mis 13. oktoobrist 31. detsembrini vormindas kõvaketta hävitades nii taastamatult kõik sellel olnud andmed.

Seda aastat võib samas nimetada ka antiviiruste aastaks, sest just siis hakati suurt tähelepanu neile pöörama.

Aprillis tulid Oxfordis asuva inglise antiviiruskompanii Sophos juhid J. Hruska, P. Lammer ja E. Wildin mõttele luua sõltumatu, antiviirustest tõepärast ja kontrollitud informatsiooni avaldav väljaanne ning juulis hakkaski ilmuma uus ajakiri „Virus Bulletin". Ajakirja kriteeriumiks sai sõltumatus ja professionaalne lähenemine antiviiruskaitse probleemide valgustamisele. Artiklite autoriteks ja toimetusnõukogu liikmeteks on tänapäevani kõige hinnatumad antiviiruseksperdid – juhtivate antiviirustarkvara arendusfirmade esindajad.

Peale juhtumit Datacrime'iga, mis pälvis suurt üldsuse ja massiteabevahendite tähelepanu, ja turuuuringut , otsustas IBM oma kompaniisiseselt kasutatud antiviirusprojekti avalikustada ning kommertstooteks muuta. Nii juhtuski, et 4. oktoobril ilmus müügile IBM Virscan, mis maksis kõigest 35 dollarit.

Oluliseks teetähiseks said ka „Virus Bulletini" poolt korraldatavad iga aastased konverentsid. See üritus oli edukas ühendades antiviirusspetsialistid ja erinevate maade suurkasutajad ühiseks võitluseks XX sajandi arvutikatkuga.

Konverentsidega alustati septembris ja need soodustasid juhtivate antiviirustarkvara arendajate omavahelist info- ja kogemustevahetust, aidates kujundada ühiseid seisukohti võitluseks arvutivandalismiga, süstematiseerida arvutiviiruste alaseid uuringuid jne.

Ilmumist alustas ka tänapäeval üks populaarsemaid infokaitse alaseid ajakirju – „Secure Computing", tolleaegse nimega „Virus Fax International". See ajakiri ei

käsitle mitte ainult antiviirusprogramme vaid ka kogu arvutiturvalisusega seotud tark- ja raudvara.

16. oktoobril puhkes SPAN võrku ühendatud arvutitel viirusussi WANK Worm epideemia. See uss kasutas levimiseks DECNet protokolli ning asendas süsteemsed teated ja süsteemse kasutajaparooli juhusliku sümboliga, saate selle GEMPAKI nimele SPAN võrgus.

Sellel aastal alustas oma antiviiruseksperdi karjääri ka Jevgeni Kasperski peale seda kui ta oktoobris oma arvutist Cascade viiruse avastas.

2.11 1990. aasta

Ilmus uus põlvkond viiruseid – polümorfsed viirused. Esimesed seda tüüpi viirused olid Viennast ja Cascadest arenenud viiruste perekond Chameleon. Viruste autor, Mark Washburn, võttis viiruse aluseks Burgeri raamatus toodud Vienna kirjelduse ja lisas Cascadest tuntud šifreerimise. Seetõttu oskas Chameleon muuta nii viiruse keha kui ka desifraatorit. Seetõttu ei suutnu tolleaegsed antiviirus programmid viirust ka avastada.

Kuna polümorfsetel viirustel puudus alaline viiruskood, sai esmatähtsaks ülesandeks uute antiviiruskaitsete väljatöötamine. Antiviirusekspertidel see ka õnnestus ning leiutati algoritmilised keeled, mis suutsid nakatunud failides ära tunda ka polümorfsed viirused.

Teiseks tähtsaks sündmuseks oli Bulgaaria „viiruse tehase” ilmumine. Nii selle, kui ka järgnevatel aastatel avastati suur hulk uusi Bulgaaria päritolu viiruseid: viiruste perekonnad Murphy, Nomenclatura, Beast, viiruse Eddie uued modifikatsioonid jt. Väga aktiivne oli aastas mitu uut viirust välja laskev ning uusi nakatamis- ja varjumisalgoritme kasutav Dark Avenger.

Bulgaarias avastati ka viirusekirjutajate omavaheline viiruste- ja infovahetusele spetsialiseerunud teatetahvlisüsteem VX BBS. Seal said kasutajad viiruseid vahetada ning huvitava viiruse edastajale võimaldati ligipääs andmebaasis olevatele viirustele ja infole. See teadetetahvel oli võimsaks tõukeks viirusliikumise arengule kuna sellele oli võimalik ligipääseda igast maailma nurgast.

Juulis toimus väga tõsine juhtum ajakirjaga „PC Today”. Igale ajakirjale oli lisatud diskett, mis nagu selgus oli nakatunud viirusega DiskKiller. Ajakirja müüdi üle 50 000 eksemplari.

Ilmusid kaks nähtamatut (stealth) viirust Frodo Whale. Need viirused kasutasid oma kohaloleku varjamiseks väga keerukaid algoritme. Samuti avastati esimesed vene päritolu viirused: Peterburg, Voronezh, LoveChild.

Detsembris loodi Saksamaal Hamburgis European Institute for Computer Anti-Virus Research (EICAR), mis on tänapäeval üheks kõige olulisemaks peaaegu kõiki suuri antiviiruskompaniisid ühendavaks rahvusvaheliseks organisatsiooniks.

2.12 1991. aasta

Arvutiviiruste arv ulatus juba sadadeni. Kuna arvutikasutajate ja ajakirjanduse huvi oli suur hakkasid tarkvaraarenduse firmad tegutsema. Ilmavalgust nägi terve rida uusi antiviirustooteid: Symantec Norton AntiVirus, Central Point AntiVirus, Fifth Generation Systems.

Viiruste levikust tooks välja polümorfse faili-buudiviiruse Tequila poolt tekitatud epideemia. Viirus loodi uurimiseesmärkidel, kuid levima hakkas ta peale vargust ning tahtlikku vabastamist. Septembris toimus sarnane juhtum teise polümorfse viiruse Amoebaga.

Tervikuna oli see aasta väga vaikne ning viiruste vaene.

2.13 1992. aasta

Sellel aastal olid teistele arvutitele ja operatsioonisüsteemidele peale IBM PC ja MS-DOS-i kirjutatud viirused unustatud. Suletud olid „augud” globaalsetes võrkudes, vead parandatud ning võrguussid ja –viirused kaotasid oma leviku võime. Juhtpositsioonile tõusid IBM PC arvutitel kasutatavale operatsioonisüsteemile MS-DOS kirjutatud faili-, buudi- ja faili-buudiviirused. Arengut jätkasid antiviirusprogrammid, avaldati raamatuid viirustest ning ilmusid mõned ajakirjad.

Ilmus esimene polümorfik-generaator MtE. Need programmid ei sisalda iseenesest paljunemisfunktsiooni, sest nende peamiseks ülesandeks on viiruskeha ja vastava dešifreerimisgeneraatori šifreerimine.

Ilmusid ka esimesed anti-antiviirus klassi kuuluvad viirused. Esimene neist oli Peach, mis eemaldas kettamuutuste revidendi Central Point AntiVirus andmebaasi, mistõttu antiviirusprogramm, leidmata andmebaasi arvas, et on esmakordselt käivitatud ja palus kasutajat uus andmebaas luua. Sedasi möödus viirus kaitsest ja nakatas kogu süsteemi.

Kogu maailma õiguskaitse organite juurde tekkisid spetsiaalsed üksnes arvutikuritegevusega tegelevad ametkonnad ning avalikkuseni hakkas jõudma üha enam teateid edukast võitlusest viiruseloojatega.

Leidis aset esimene juhtum, kus antiviiruskompanii kommertskasu nimel oma toodetele viiruste ümber paanikat tekitades tähelepanu tõmbas. Juhtum leidis aset viiruse March6 epideemiaga seoses. Üks Ameerika antiviiruskompanii teatas, et 6. märtsil rikub viirus informatsiooni 5 miljonil arvutil. Tegelikult tabas rünnak ainult mõnda tuhandet masinat, samas kui antiviirusfirmade tulud mitmekordistusid.

Avastati esimene Windowsile kirjutatud ja selle täitmisfaile nakatav viirus Win.Vir_1_4, mis avas arvutiviiruste loomise ajaloos uue lehekülje.

2.14 1993. aasta

Viiruste kirjutajad asusid tõsiselt tööle. Kirjutati sadu äravahetamiseni sarnaseid tavaviiruseid, terve rida uusi polümorfik-generaatoreid ja viiruste konstruktoreid, loodi uusi viirustekirjutajate elektronväljaandeid. Üha rohkem ilmus aga ka uusi ebatavalisi failide nakatamise, süsteemi tungimise, varjumise ning hävitamise tehnoloogiaid kasutavaid viiruseid.

Kevadel tuli oma antiviirusega Microsoft AvtiVirus turule Microsoft. Antiviirus baseerus Central Point AntiVirusel ning kuulus MS-DOS ja Windows standardpaketti. Kuigi algul näitas programm ennast heast küljest hakkas tema kvaliteet varsti langema ning Microsoft sulges projekti. Selle peale ohkasid teised antiviiruste tootjad kergendatult.

2.15 1994. aasta

Populaarseimaks infokandjaks said CD-plaadid ja ühtlasi ka viiruste peamiseks levikuallikaks. Leidis aset mitu juhtumit, kus plaatide ettevalmistamisel

paljundamiseks sattus originaalplaatidele viirus. Seega jõudsid arvutiturule kümned tuhanded nakatunud plaadid.

Inglismaal nägid ilmavalgust kaks väga keerulist polümorfset viirust SMEG.Pathogen ja SMEG.Queeg, mida isegi tänapäeval kõik antiviirusprogrammid sajaprontsendilise usaldusväärsusega avastada ei suuda. Viiruste autor paigutas nakatunud failid BBS-idele, põhjustades nii epideemia ja massiteabevahendeid haaranud paanika.

Järgmise paanikalaine põhjustajaks oli arvuteid nakatava viiruse GoodTimes eest hoiatav viirusmüstifikatsioon. Hoiatus sai kiiresti rahvusvahelise ulatuse ja tõlgiti ümber paljudesse keeltesse.

Ilmus mitu uut ja võrdlemisi ebatavalist viirus. Esimene neist oli C ja Pascal keeltes kirjutatud programmide lähtetekste nakatav viiruste perekond SrcVir. Teisena ilmus massilise epideemia põhjustanud ohtlik ja keeruline polümorfne viirus OneHalf, mis veel praegugi maailma arvutikasutajale muret valmistab. Järgmise epideemia tekita faili-buudiviirus ZARAZA.

Tähtsad sündmused toimusid aga ka antiviiruste vallas. Juunis lõpetas oma olemasolu selle aja antiviirusliider Central Point, mille ostid Symantec. Septembris osales Hamburgi Ülikooli Antiviirusuuringute Keskuse korraldatavates sõltumatutes testides esmakordselt Jevgeni Kasperski juhitud tarkvaraarendajate rühma loodud programm AntiViral Toolkit Pro (AVP), saavutades absoluutse võidu kõigis kategooriates.

2.16 1995. aasta

DOS-viiruste valdkonnas märkimisväärseid sündmusi ei olnud. Ilmusid mõned keerulised viirusmonstrumid nagu NightFall, Nostradamus, Nutcracker ja mõned naljakad nagu „kahesooline” viirus RMNS ja BAT-viirus Winstart. Peaaegu üle kogu maailma levisid viirused ByWay ja DieHard2

Veebruaris leidis aset vahejuhtum kompaniiga Microsoft. Üks operatsioonisüsteemi Windows 95 160-st beetatestijast otsustas kontrollida saadud demoversiooni sisaldavat plaati antiviirusega ning avastas sellelt buudiviiruse Form.

Kevadel asusid ühtset antiviirusprogrammi arendama kaks küllalt tugevaid antiviiruseid tootvat kompaniid EsaSS (ThunderByte Anti-Virus) ja Norman Data Defence Systems (Norman Virus Control).

Sellel aastal ilmusid ka makroviirused, mis panid oma tulekuga antiviiruste tootjad taas tõsiselt pead murdma, kuna kaitseks seda tüüpi viiruste eest tuli luua antiviiruse programmituumale spetsiaalne täiendus, mis oleks suuteline otsima makroviiruseid Wordi dokumentidest ning hiljem ka Exceli, Accessi, PowerPointi ja teiste rakenduste failidest.

15. novembril mõisteti Inglismaal 26 aastane Christopher Pile süüdi viiruste Queeg ja Pathogen ning polümorfik-generaatori SMEG loomises ja määrati 18 kuuks vangi.

2.17 1996. aasta

Jaanuaris toimus kaks tähelepanuväärset sündmust: ilmus esimene operatsioonisüsteemile Windows 95 kirjutatud viirus Boza ja puhkes Sankt-Peterburgist pärit vene programmeerija Denis Petrovi poolt loodud äärmiselt keeruka polümorfse viiruse Zhengxi epideemia.

Märtsis registreeriti Windows 3.x viiruse Win.Tentacle esimene epideemia. Oluline oli sündmus sellepoolest, et see oli esimene vabadusse pääsenud Windows viirus. Sinnamaani olid kõik Windowsi viirused eksisteerinud üksnes viirusekirjutajate elektronajakirjades. Kohata võis vaid buudi-, DOS-i ja makroviiruseid.

Juunis ilmus esimene operatsioonisüsteemile OS/2 kirjutatud EXE-faile nakatav viirus OS2.AEP. Selle ajani olid vaid faile ülekirjutavad ja hävitavad võis siis „kompanjoni" meetodit kasutavad viirused.

Juulis nägi ilmavalgust esimene Microsoft Exceli tabeleid nakatav viirus Laroux. Selle viiruse tegevus oli rajatud Excelis kasutatavatele makrodele. Selgus, et Excelisse sisse ehitatud Visual Basicuga võis samuti viiruseid luua. Epideemia põhjustas see viirus 1997. aastal Moskvas.

Augustis lasid kaks viirusekirjutajat peaaegu üheaegselt välja makroviiruste konstruktorid MS Wordi saksa- ja inglisekeelsetele versioonidele.

Oktoobris leidis aset järgmine juhtum Microsoftis. Kompanii Šveitsi osakonna tehnilise toe veebilehel avastati ühes Wordi dokumendis makroviirus Wazzu. Veidi hiljem avastati sama viirus ka Šveitsis toimunud arvutitehnoloogia näitusel Orbit Microsofti poolt levitatud CD-plaatidel. Probleem selle viirusega veel ja jätkus ja nii avastatigi see viirus septembris Microsoft Solution Provider CD-plaadilt.

Detsembris ilmus esimene operatsioonisüsteemile Windows 95 kirjutatud residentne viirus Win95.Punch, mis laadides end süsteemi kui VxD-draiver, võttis üle kõik failide poole pöördumised ja nakatas need failid.

Tervikuna võib seda aastat pidada viirusekirjutajate laiaulatusliku pealetungi alguseks Windowsi operatsioonisüsteemidele 95 ja NT ning Microsoft Office'i rakendustele.

2.18 1997. aasta

Veebruaris ilmus esimene operatsioonisüsteemile Linux kirjutatud viirus Linux.Bliss. Sealt edasi on Linuxile mõeldud viirused edasi arenenud ja viirusekirjutajate poolt on loodud ka töövõimelisi Trooja hobuseid.

Microsoft Office 97 ilmumine tõi endaga kaasa ka makroviiruste järk-järgulise ülemineku sellele platvormile. See oli tingitud uue programmeerimiskeele VBA 5.0 kasutusele võtmisest, sest uus keel erines eelnevatest WordBasicu ja VBA 3.0 keeltest. VBA 5.0 juures ei suutnud erinevates keskkondades loodud viirused ühilduda täielikult erinevate tarkvaraversioonidega ja seega ei täitnud neile pandud „ülesandeid". Uued makroviirused osutusid aga oma eelkäijate uude versiooni kopeeritud analoogideks. Peagi aga ilmusid spetsiaalselt MS Office 97 rakendustele kirjutatud viirused.

Märtsis ilmus viirus MS Word 6/7 makroviirus ShareFun, mis avas viirusetööstuse ajaloos uue lehekülje. Nimelt oli see esimene viirus mis kasutas levimiseks elektronposti.

Aprillis ilmus esimene andmeedastusprotokolli FTP (File Transfer Protocoll) vahendusel leviv viirususs Homer.

Juunis põhjustas epideemia vene päritolu isešifreeruv Windows 95 viirus Win95.Mad.

Detsembris hakkasid levima IRC kanaleid kasutavad arvutiussid. Võimalikuks sai see kuna IRC kaudu laetavate failide säilituskaust ja juhtimisfaili SCRIPT.INI paigutuskaust langesid kokku. Nii juhtuski, et ussi levitamiseks piisas SCRIPT.INI faili ülekirjutamisest. Peale vea parandamist unustati primitiivsed IRC-ussid.

2.19 1998. aasta

Jätkusid rünnakud MS Windowsile, MS Office'ile ja võrgurakendustele ning ilmusid ka uued üha keerukaimaid nakatamis-, sissemurdmis- ja levikumeetodeid kasutavad

viirused. Lisaks neile ilmusid ka arvukad Interneti juurdepääsu paroole varastavad Trooja hobuse programmid.

Aasta algul toimus terve viiruste perekonna Win32.HLLP.DeTroie epideemia. Nende viiruste omapära oli see, et na suutsid nakatada Windows 32 täitmisfaile ja olid samas ka võimelised saatma oma „peremehele" ka iseloomustavat informatsiooni nakatunud arvuti kohta. Samas oli see viiruste perekond loodud Windowsi prantsuskeelsele versioonile ning epideemia hõlmas ainult prantsuskeelseid maid.

Veebruaris avastati uut tüüpi Exceli tabeleid nakatav makroviirus Excel4.Paix, mis kasutas Exceli tabelitesse juurdumiseks makrode asemel valemeid, mis nagu selgus võivad samuti isepaljunevat koodi sisaldada.

Märtsis avastati esimene Microsoft Accessile kirjutatud viirus AccessiV. Erilist tähelepanu ta aga ei pälvinud, sest selleks ajaks oli juba harjutud, et Microsoft Office'i rakendused langevad üksteise järel viiruste ohvriks. Samal ajal ilmus ka esimene mitmeplatvormiline viirus, mis suutis nakatada nii Wordi kui ka Accessi faile.

Juunis tekitas viirus Win95.CIH globaalse ulatusega epideemia. CIH käitumine oli ohtlik kuna jooksvast kuupäevast sõltuvalt kustutas ta Flash BIOS-e, mille tagajärjeks oli emaplaadi vahetus.

Detsembris langes arvutiviiruste ohvriks MS Office'i rakendustes – PowerPoint. Esimene viirustest oli Attach ja temale järgnesid kohe veel kaks – ShapeShift ja ShapeMaster.

2.20 1999. aasta

Jaanuaris puhkes võrguussi Happy99 globaalne epideemia. See oli esimene ussidest, mis kasutas oma levikuks. MS Outlooki.

26. märtsil vapustas maailma teade esimese võrguussi funktsionaalsust sisaldava MS Wordi makroviiruse Melissa globaalsest epideemiast. Kohe peale süsteemi nakatamist võttis Melissa MS Outlooki aadressiraamatust 50 esimest adressaati ja saatis neile oma koopiad, tehes seda kasutaja nimel, kuid märkamatult.

Melissa autor tabati, selleks osutus 31-aastane New Jerseyst pärit programmeerija David L. Smith. Smith mõisteti 9. detsembril süüdi ja karistati 10-aastase vangistusega ning 400 000 dollarilise trahviga.

Leiti ka viiruse CIH autor – Taiwani Tehnoloogiaülikooli üliõpilane Cheng Ing-hau, kuid kuna kohalikel firmadel tema vastu kaebusi ei olnud puudus politseil alus tema arreteerimiseks.

7. mail tungisid viirused graafikapaketi CorelDraw valdustesse. Skriptikeeles kirjutatud viirus Gala oli esimeseks viiruseks, mis suutis nakatada nii CorelDraw enda, kui ka Corel PhotoPainti ja Corel Ventura faile.

Suve algul puhkes ohtliku võrguussi ZippedFiles epideemia. Viirus kujutas endast EXE-faili, mis peale süsteemi juurdumist hävitas mõningate populaarsete rakenduste failid. Kuigi oma levikult jäi see uss alla Melissale, tekitas ta oluliselt suuremat kahju.

Tähelepanuväärseimaks sündmuseks kujunes augustis huvitava ussviiruse Toadie avastamine, mis peale DOS-i ja Windowsi failide nakatamise lisas oma koopiaid postiprogramm Pegasus vahendusel saadetavaile e-kirjadele ja proovis end levitada ka IRC kanalite kaudu.

Oktoober tõi endaga kaasa kolm arvutimaailma jaoks väga ebameeldivat üllatust. Esiteks avastati esimene operatsioonisüsteemile Windows NT kirjutatud ja selle platvormi kõige kõrgemale turvatasemele ehk süsteemsete draiverite piirkonda juurduv ning seetõttu raskesti ravitav viirus Infis. Teiseks teatasid antiviiruskompaniid kuu lõpus esimese MS Projectile kirjutatud, kuid sisuliselt multi platvormse makroviiruse avastamisest, mis suutis nakatada ühtmoodi hästi nii MS Projecti, kui MS Wordi faile. Kolmandaks ilmutas end juba juulist tuntud ja viirusekirjutajate tähelepanu programmeerimiskeelele Visual Basic Script (VBS) tõmmanud ning üheks kurva kuulsusega viiruse LoveLetter esivanemaks saanud skriptiviirus Freelinks.

Novembris vapustas maailma teade uuest e-posti kaudu levivast „stealth”-usside põlvkonnast, mis ei kasutanud oma koopiate levitamiseks enam kirjadele lisatavaid faile ning juurdusid arvutitele kohe peale nakatunud kirja avamist. Esimeseks selliseks ussiks oli BubbleBoy, millele järgne KakWorm. Eranditult kõik seda tüüpi ussid kasutasid Internet Exploreri turvasüsteemis avastatud auku. Kuigi vead said parandatud on KakWorm siiani üks viiest levinuimast kahjurprogrammist.

7. detsembril avastati Brasiilia viirusekirjutaja Vecna poolt loodud väga keerulise ja ohtliku viirus Babylonia, mis avas uue lehekülje viiruste loomises. See oli esimene viirususs, mis püüdis minutiliste intervallidega ühenduda Jaapanis asuva serveriga, vaadata sealt viirusmoodulite loendit ja juhul, kui loendis juhtus olema mõni

nakatunud arvutile paigaldatust „värskem” moodul, siis laadis ta selle automaatselt alla. Hiljem leidis selline tehnoloogia kasutamist paljudes teiste ussides nagu Sonic, Hybrids jt.

Alates aasta keskpaigast jagunes antiviirustööstus formaalselt kaheks vastavalt oma suhtumisele aastavahetusega 1999-2000 kaasnevatesse vahejuhtumitesse. Üks osa toetas innukalt nägemust sellest, kuidas kräkkerid ja kogu maailma viirusekirjutajad ülejäänud ühiskonnale sajandivahetusel tuhandete eriti ohtlike viiruste näol inimtsivilisatsiooni aluseid proovile paneva „üllatuse” valmistavad. Selliste seisukohtade peamiseks mõtteks oli oma toodete, kui „ainsate päästevahendite” läbimüüki suurendada. Teine osa antiviiruskompaniisid püüdsid aga hirmunud kasutajaid igati rahustada ning asjatut ja ohtlikku paanikat vältida. Hiljem osutusidki hüsteerilised avaldused „Viiruseohust 2000” alusetuks ja see aastavahetus erines ülejäänutest vaid suurejoonelistemate pidude poolest.

2.21 2000. aasta

Aasta algas ootamatult: arvutiviiruste ohvriks langesid üksteise järel Windows 2000 ja populaarne diagrammide ja plokkskeemide loomise rakendus Visio. Veel enne, kui Microsoft jõudis turule tulla Windows 2000 täisfunktsionaalse kommertsversiooniga, tulid põrandaaluse rühmituse 29A liikmed „turule” seda nakatava viirusega Inta ning natuke hiljem tõnbasid peaaegu üheaegselt ilmunud viirused Unstable ja Radiant risti peale ka visiole.

5. mail puhkes Guinessi rekordite raamatusse sattunud skriptiviiruse LoveLetter epideemia. Naiivsed arvutikasutajad ei osanud isegi kujutleda, et süütutes VBS-failides, mis olid veelgi süütumateks tekstifailideks maskeeritud, võib asuda ohtlik viirus, mis kohe peale käivitamist hävitas ketastelt kõik teatud laienditega failid ja saatis märkamatult oma koopiad kõigile MS Outlooki aadresssiraamatust leitud adressaatidele. Tänu skriptiviiruse lähtekoodile on järgnevatel aastatel ilmunud hulgaliselt LoveLetteri modifikatsioone.

Suvi kujunes palavaks just arvutiviiruste osas. Kuigi tavaliselt peetakse suve puhkuse ajaks ja seda eeldatakse ka nii viirusekirjutajatelt, kui ka antiviirusekspertidelt, otsustasid esimesed teistele ootamatu üllatuse valmistada. Juulis esitles rühm Cult of death Cow tuntud sanktsioneerimata kaugadministreerimisutiliidi Back Orifice 2000 (BO2K) uut versiooni. See leidis aset iga-aastasel konverentsil DefCon.

Tegelikkuses ei olnud programmi uus versioon sugugi ohtlikum oma eelkäijast ning oli operatiivselt lisatud juhtivate antiviiruste andmebaasi.

Juulis ilmus kolm huvitavat viirust. Star, mis oli AutoCADi viirus, seejärel aga korraga viie erineva viiruse, sealhulgas CIH-i, SK, Bolzano jt. koodi sisaldav Dilber, mis sõltuvalt jooksvast kuupäevast aktiveeris ühe või teise komponendi destruktiivsed funktsioonid, teenides sellega nimetuse – viirustega täidetud kosmosesüstik. Kolmandana avastati arvutisse tungimiseks „kirvemeetodit" kasutav võrguuss Jer. Veebilehele lisati selle avamisel automaatselt aktiviseeruv skriptiprogramm, mis palus luba enda kopeerimiseks kasutaja arvutisse. Arvestus oli rajatud sellele, et kasutaja vajutab tüütust skriptiprogrammist vabanemiseks automaatselt „Yes" nupule ning lubab tundmatut faili kopeerida.

Sellise ussi ilmumine tähistas uut tehnoloogilist moesuunda viiruste Internetti sokutamisel. Algul paigutatakse uss veebilehele, siis tehakse aga kasutajate ligimeelitamiseks massiline reklaamikampaanioa. Arvestus osutus täpseks, sest paljude külastajate seas leidus ikka mõnikümmend lihtsameelset, kes ussi oma arvutisse lasid.

Augustis avastati esimene pihuarvutile Palm Pilot operatsioonisüsteemile PalmOS kirjutatud Trooja hobuse tüüpi kahjurprogramm, mis käivitamisel kustutas arvutist failid, kuid ei omanud paljunemisvõimet.

Septembris täiendas seda uut kahjurprogrammide liiki esimene tõeline PalmOS viirus Phage. See oli klassikaline parasiitviirus, mis nakatatavasse failidess juurdumise asemel need lihtsalt oma koodiga asendas.

Septembri algul avastati esimene failisüsteemi NTFS täiendavate voogudega manipuleeriv arvutiviirus Stream, mis iseenesest reaalset ohtu ei kujutanud, kuid erakordselt ohtlik oli täiendavatesse voogudesse tungimise tehnoloogia ise, sest ükski antiviirusskanner ei ole võimeline seal kahjurkoodi avastama.

Oktoobris ilmus esimene PIF-failidesse kaevuv viirus Fable ja esimene skriptikeeles PHP kirjutatud viirus Pirus. Samal kuul leidis aset ka laia kõlapinda leidnud skandaal seoses oletatavalt Sankt-Peterburgist pärit tundmatute häkkerite sissemurdmisega neile mitmeks kuuks avatuks jäänud Microsofti sisevõrku. Sissemurdmine oli sooritatud triviaalsel meetodil, võrguuss QAZ abil. Huvitav oli see juhtum ka selle

poolest, asastamise hetkeks oli see uss juba mitmeid kuid praktiliselt kõigi antiviirusprogrammide andmebaasidesse kantud.

Novembris avastati ohtlik ja tehnoloogiliselt täiuslik viirus Hybris, mille autoriks oli hüüdnime Veca all esinev tuntud Brasiilia viirusekirjutaja, kes oma esimese iseuuendava viiruse Babylonia ideed edasi arendas ja varem tehtud vigadest õppust võttis. Hybris kasutas olemasolevate viirusmoodulite tuvastamiseks 128-bitilist RSA elektronvõtit ning levis peamiselt elektronkonverentside kaudu.

Sellel aastal leidis kinnitust tõsiasi, et kahjurkoodide peamiseks trantspordivahendiks oli saanud elektronpost.

Oma tegevuse aktiviseerisid ka Linuxi viiruste loojad ja kokku registreeriti 37 Linuxile kirjutatud uut viirust ning Trooja hobuse programmi, millega Linuxi viiruste üldarv tõusis 43-ni, seitsmekordistudes selle aastaga.

Veel võib äramärkida viiruste edetabelis aset leidnud olulised muutused, kus seni kindlalt esikohta hoidnud makroviirused loovutasid oma positsiooni skriptiviirustel.

3 TUNTUMAD ARVUTIVIIRUSED

3.1 Kurikuulsad viirused

3.1.1 Michelangelo

Aktiveerub Michelangelo Bunarotti sünnipäeval 6. märtsil hävitades kogu boot-ketta info.

3.1.2 Interneti uss (worm) 2.nov. 1988 - USA

Autoriks oli Cornelli Ülikooli üliõpilane Robert Morris. Uss erinev viirustest selle poolest ,et ei haaku mõne olemasoleva peremeesprogrammi külge, vaid levib ja paljuneb arvutivõrgus iseseisvalt. See uss nakatas lühikese ajaga 6200 VAX- ja Sun-arvutit, mis töötasid operatsioonisüsteemi Unix teatud versioonidega. Tagajärjeks oli, et paljud organisatsioonid, sealhulgas suured teaduskeskused olid sunnitud ennast mõneks ajaks internetist lahti ühendama.

3.1.3 Internetiuss „Good Times" dets.1994

Asjatundlikult käimapandud kirjakett, kuid mitte viirus. Autor lasi ringlusse e-maili teemareaga „Good Times". Kirjas oli hoiatus, et mööda e-postisüsteeme liigub ringi ohtlik viirus nimega „Good Times", mis aktiveerub siis, kui lugeda viirust sisaldavat kirja. Kõik kirjad teemareaga „Good Times" kästi kohe ilma lugemata hävitada.

Paljud kasutajad ei mõistnud, et see hoiatus oli nali – üldiselt, ei võimalda elektrooniline kirjasüsteem kirja lugemise peale programmide käivitamist – ja saatsid hoiatuse sõpradele edasi.

3.2 Laastavaimad viirused

3.2.1 Loveletter

Ilmus 4. mail 2000 ja levis e-posti teel. Teemareaga „ILOVEYOU" elektronkirja avades käivitus programm, mis kirjutas Windowsi operatsioonisüsteemis üle teatud registrid, .jpg-laiendiga pildifailid ning .mp3-laiendiga helifailid.

Viirus paljundas ennast, saates kirja edasi kõigil MS Outlooki aadressiraamatusse sisestatud aadressidel.

3.2.2 NewLove

Ilmus 19. mail 2000 ja sarnaselt LoveLetteriga levis e-posti teel. Kirja teema rida varieerub, mis teeb viirust sisaldava kirja avastamise keerulisemaks. Teemarida algab edasisaadetava kirja tähisega „FW:”, millele järgneb arvutist leitud suvalise faili nimi. Saadetis sisaldab .vbs laiendiga faili. Viirus käivituks, kui kasutaja selle avaks.

Nagu LoveLetter, saadab viirus käivitudes end edasi kõigile arvuti aadressiraamatus olevatele aadressidel. Seejärel hävitab ta kõvakettal olevad failid, mille tulemusena arvuti kinni jookseb ja enam ei käivitu.

Viirus on programmeeritud nii, et ta aina oma koodi muudab lisades sellele juhuslikke tekstikatkendeid. See kasvatab viirust levimisel aina suuremaks ja suuremaks.

3.2.3 CIH (Tšernobõli viirus)

CIH paljuneb ja aktiveerub ainult arvutites, kus operatsioonisüsteemiks on Windows 95 või Windows 98. Viirus võib üle kirjutada kõvaketta alguse, kus asuvad olulised andmed kõigi failide paiknemise kohta (FAT). Lisaks üritab CIH üle kirjutada BIOS-kiibi sisu, see õnnestub viirusel vaid teatud tüüpi BIOS’ide korral. Arvuti, kus CIH on BIOSi üle kirjutanud, ei käivitu enam, vaid jääb täiesti tummaks. Halvemal juhul ootab siis ees kulukas emaplaadi vahetus.

KOKKUVÕTE

Arvutiviiruste teemat käsitledes oli üheks läbivaks teemaks hea ja kurja vaheline võitlus ehk siis ühelt poolt viirusekirjutajad ja teiselt poolt antiviiruseksperdid. Vaadeldes seda võitlust jääb mulje, et head kaotavad, kuid tegelikkus on, et arvutiviirusi on kaugelt rohkem võimalik kirjutada, kui seda siiani on tehtud. Võib ju isegi öelda, et me oleme alles jäämäe tippu näinud ja ei tea sedagi kui suur see mägi on. Selliseid asjaolusid arvestades võime öelda, et antiviiruseksperdid teevad väga head tööd.

Praegusel hetkel võime kindlad olla, et epideemiad, mis on tabanud arvuti maailma, ei ole veel lõppenud. Alust on arvata, et need lähevad ainult hullemaks, sest täpselt nii, kuidas antiviiruseksperdid aitavad meil arvutiviirustest vabaneda, kirjutavad viirusekirjutajad neid juurde ning oodata võib ainult uusi ja hullemaid.

Öeldakse ju, et inimvõimetel ei ole piire. Kuna arvutite maailm on mõne koha pealt veel alles täiesti tundmatu ala, siis on viirustekirjutajatel võimalik lasta oma fantaasial lennat. Meie ainus lootus on, et antiviiruseksperdid on neist paremad.

KASUTATUD KIRJANDUS

1. Arvutiviiruste ajalugu „muinasajast” tänapäevani 1
   http://vana.am.ee/3014 (25. veeb. 2006 a.)
2. Arvutiviiruste ajalugu - „muinasajast” tänapäevani 2
   http://vana.am.ee/3712 (25. veeb. 2006 a.)
3. Arvutiviiruste ajalugu - „muinasajast” tänapäevani 3
   http://vana.am.ee/3922 (25. veeb. 2006 a.)
4. Arvutiviiruste ajalugu - „muinasajast” tänapäevani 4
   http://vana.am.ee/4415 (25. veeb. 2006 a.)
5. Arvutiviiruste ajalugu - „muinasajast” tänapäevani 5
   http://vana.am.ee/4974 (25. veeb. 2006 a.)
6. Arvutiviiruste ajalugu - „muinasajast” tänapäevani 6
   http://vana.am.ee/5519 (25. veeb. 2006 a.)
7. Arvutiviiruste ajalugu - „muinasajast” tänapäevani 7
   http://vana.am.ee/5833 (25. veeb. 2006 a.)
8. Arvutiviiruste ajalugu - „muinasajast” tänapäevani 8
   http://vana.am.ee/6256 (25. veeb. 2006 a.)
9. Arvutiviiruste ajalugu - „muinasajast” tänapäevani 9
   http://vana.am.ee/6606 (25. veeb. 2006 a.)
10. Arvutiviiruste ajalugu - „muinasajast” tänapäevani 10
    http://vana.am.ee/6961 (25. veeb. 2006 a.)
11. 2004: viirused ja spämm
    http://vana.am.ee/15437 (25. veeb. 2006 a.)
12. http://www.ut.ee/it/juhendid/viirused (25. veeb. 2006 a.)
13. Arvutiviirused.doc
    http://materjalid.tmk.edu.ee/mati_muinaste/Andmeturve/AT200506/ (25. veeb. 2006 a.)
14. TurvalineArvuti.doc
    http://materjalid.tmk.edu.ee/mati_muinaste/Andmeturve/AT200506/ (25. veeb. 2006 a.)
15. Arvutiviirused ja viirusetorjetarkvara.ppt (25. veeb. 2006 a.)

http://materjalid.tmk.edu.ee/vladimir_kjahrenov/index.php?dir=/Andmeside/Loeng_2 (25. veeb. 2006 a.)
16. http://www.cs.ut.ee/~heli_u/loeng6.htm (25. veeb. 2006 a.)
17. http://www.zone.ee/arvutiajalugu/ (25. veeb. 2006 a.)