

ZGODOVINA ZLONAMERNIH RAČUNALNIŠKIH PROGRAMOV

1949

Razvijejo se teorije o programih, kateri naj bi se sami množili.

1981

Applovi Virusi 1, 2, in 3 so med prvimi virusi, ki so se razširili v javnost. Našli so jih na Apple II operacijskem sistemu, množili so se preko Texas A&M, s pomočjo piratskih iger.

1983

Fred Cohen, je v svoji razpravi definiral računalniški virus kot "računalniški program, ki lahko vpliva na ostale računalniške programe, in jih spreminja tako, da v njih vključi tudi (razvitejšo) svojo kopijo."

1986

Programerja Basit in Amjad sta tega leta zamenjala izvršilno kodo boot (zagonskega) sektorja mehke (disketne) enote, z njuno kodo, katere namen je bil okužiti 360kb disketo, do katere smo dostopali. Okužene diskete so imele oznako "© Brain" (dandanes A:/).

1987

Virus z imenom Lehigh je eden prvih virusov, ki okuži datoteke. Ta virus okužuje command.com datoteke.

1988

Eden najpogostejših virusov, Jerusalem (Jerusalem), je lansiran. Virus se aktivira vsak petek 13., okuži .exe in .com datoteke in zbriše vse programe, ki delujejo na ta dan.

MacMag in Scores virus sta povzročila prvi večji naval na Macintoshe.

1990

Symantec sprogramira Norton AntiVirus, prvi med antivirusnimi programi, za katerimi stojijo velika podjetja.

1991

Tequila je prvi »mnogolični« virus. Polimorfizne (»mnogolične«) viruse antivirusni programi težko zaznajo, saj ob vsaki novi infekciji spremenijo svoj videz.

1992

Obstaja 1300 virusov, 420% rast v primerjavi z decembrom, 1990.

Dark Avenger Mutation Engine (DAME) je narejen. To orodje spreminja navadne viruse v polimorfizne. Virus Creation Laboratory (VCL) postane dostopen. To je dejansko prvo orodje za izdelavo virusov.

1994

Good Timesova email potegavščina se širi po računalniških skupnostih. Potegavščina opozarja na to, da kroži nevaren virus, ki bo izbrisal cel trdi disk, v primeru, da odpremo email sporočilo z naslovom "Good Times." Čeprav so ugotovili, da gre za potegavščino, pa se je le-ta še vedno pojavljala na 6-12 mesecev.

1995

Word Concept postane prevladujoč virus v sredini 90-ih. Širi se s pomočjo Wordovih dokumentov.

1996

Baza, Laroux (makro virus) in Staog virusi so prvi, ki okužujejo Windows95 datoteke, Excel in Linux.

1998

Zaenkrat še nenevaren virus, StrangeBrew, je prvi virus, ki okužuje Java datoteke. Virus spremeni CLASS datoteke tako, da vsebujejo njegovo kodo med programsko kodo.

Chernobyl (Černobil) virus se začne hitro širiti preko .exe datotek. Kot nam že ime pove, je virus zelo nevaren, saj poleg datotek, napada tudi določene čipe v okuženih računalnikih.

2 kalifornijska najstnika vdreta in prevzameja nadzor nad več kot 500 vojaškimi, vladnimi in zasebnimi računalniškimi sistemi.

1999

Melissa virus, W97M/Melissa, vgradi makro (Word/Excel – Tools(Orodja) – Macro (Makroji)) v datoteko, pripeto email sporočilu, in pošlje ta dokument še 50 naslovom, ki jih imamo v Outlooku. Virus okuži tudi ostale Wordove datoteke in jih pošilja kot priponke. Melissa se širi hitreje kot katerikoli virus dotedaj, okužila je približno 1 milijon računalnikov.

Bubble Boy je prvi računalniški črv, ki za okužbo ne potrebuje prejemnikovega klika na priponko. Takoj ko se sporočilo odpre, se Bubble Boy zažene.

Tristate je prvi večprogramski makro virus; okužuje Wordove, Excelove in PowerPointove datoteke.

2000

Love Bug, znan tudi kot ILOVEYOU virus, se pošilja sam sebe preko Outlooka, podobno kot Melissa. Virus dobimo kot VBS (Visual Basic Script) priponko, nato pa pobriše datoteke, tudi MP3, MP2, in .JPG datoteke. Iz okuženih računalnikov pošilja avtorju virusa uporabniška imena in gesla.

W97M.Resume.A, spremenjen Melissa virus, pride na »Wildlist« (www.wildlist.org – stran, ki nam prikaže informacije o vseh virusih, ki trenutno krožijo po okuženih računalnikih). Ta virus deluje podobno kot Melissa, saj s pomočjo makra okuži Outlook in se pošilja naprej.

“Stages” (stopnje) virus, skrit kot zabavni email joke o stopnjah življenja, se začne širiti preko interneta. Za razliko od prejšnjih virusov, se Stages skriva v priponko z lažno “.txt” končnico, ki prevara prejemnika, da jo odpre. Do takrat je veljalo, da so tekstovni dokumenti (.txt) varni.

“Distributed denial-of-service” (DDoS) hekerski napadi na Yahoo, eBay, Amazon in nekaj ostalih večjih strani, so imeli za posledico večurno nedelovanje teh strani.

2001

Kmalu po napadu 11. septembra, Nimda virus začne okuževati na tisoče računalnikov po celem svetu. Takrat je bil to najbolj dodelan virus, saj je poznal vsaj 5 različnih metod okuževanja in modificiranja samega sebe. Virus “Anna Kournikova”, kateri se pošilja vsem kontaktom v Outlookovemu imeniku, skrbi analitke, ki so ugotovili, da je ta dokaj nenevaren virus, narejen s pomočjo orodja, ki omogoča tudi najmanj izkušenim programerjem izdelavo virusa. Poveča se število črvov, med najbolj znanimi so Sircam, CodeRed in BadTrans, ki povzročajo tudi največ problemov. Sircam se širi preko dokumentov s pomočjo emaila. CodeRed napada ranljive spletne strani, pričakovali so, da bo napadel tudi spletno stran Bele hiše. Okužil je približno 359,000 strani v 12 urah. BadTrans je narejen za pridobitev gesel in informacij o kreditnih karticah.

2002

Avtor Melissa virusa, David L. Smith, je obsojen na 20 mesecev kazni v zveznem zaporu. LFM-926 virus se pojavi začetek januarja in prikazuje sporočilo “Loading.Flash.Movie” (Nalagam Flash film/animacijo), vendar v resnici okuži Shockwave Flash (.swf) datoteke. Virusi z imenom znanih osebnosti, kot so “Shakira,” “Britney Spears,” in “Jennifer Lopez” se začnejo pojavljati. Črv Klez, kot primer vedno večjega števila črvov, ki se širijo preko emaila, prepriše datoteke (jih napolni z ničlami), naredi skrite kopije originalnih datotek in poskuša onesposobiti anti-virusne programe. Črv Bugbear se pojavi v septembru. To je kompleksen črv z veliko metodami okuževanja sistemov.

2003

V januarju se pojavi dokaj nenevaren "Slammer" (Sapphire) črv, vendar postane črv, ki se najhitreje širi, saj je okužil 75.000 računalnikov v samo 10 minutah. Prvo minuto delovanja se je število okužbo vsakih 8,5 sekund podvojilo. Črv Sobig je med prvimi »spam« (spam=nezaželjena reklamna, potencialno nevarna pošta, ki jo prejemamo v velikih količinah na naš email naslov) črvi. Okuženi računalniki so tako prejeli spam sporočila in jih v velikih količinah pošiljali potencialnim žrtvam naprej.

2004

Računalniški črv z imenom MyDoom ali Novarg, se v januarju začne širiti preko emailov in programov za prenašanje datotek (eMule, Kazaa...), hitreje kot katerikoli virus in črv dotedaj. MyDoom vzbudi prejemniku radovednost, tako da ta odpre priponko, ki omogoča hekerjem dostop do trdega diska okuženega računalnika. **Cilj je "denial of service attack" (DDos) napad na SCO Group, podjetje, ki toži veliko skupin zaradi uporabe njihovega Unix programskega jezika. SCO ponuja \$250.000 nagrade vsakomur, ki ima kakršnokoli informacijo o avtorjih črva.**

Približno milijon računalnikov z Windows operacijskim sistemom (OS) je v maju okuženih z črvom Sasser, ki se izredno hitro širi. Žrtve so tudi podjetja, kot so British Airways, banke, državne ustanove, Britanska obalna straža,... Črv ne povzroča nepopravljive škode datotekam in računalnikom, temveč upočasnjuje njihovo delovanje, povzroča nenadne izklope in ponovne zagone (odpre se okno, ki odšteva 60 sekund, nato se računalnik ponovno zažene). Sasser se od ostalih virusov in črvov razlikuje po tem, da za okužbo ni potrebno odpreti datoteke/emaila/priponke. Namesto tega črv išče varnostne luknje in jih izkoristi. Nemški 18-letnik, ki obiskuje srednjo šolo, je priznal, da je avtor tega črva. Osumljen je tudi izdaje nove verzije črva.

Zaključek

Velik odstotek ljudi, ki redno uporabljajo internet, se še vedno ne zaveda groženj raznih zlonamernih programov.

Dejansko dandanes zasebnosti na internetu ni, saj nas že ob sami povezavi na internet izda IP naslov našega računalnika, kar je dovolj za dostop do vašega računalnika. Nočem vas strašiti, vendar pa je vredno imeti dober antivirusni program (brezplačni Bitdefender 8, AVG, dober plačljiv tak program pa je NOD32), Lavasoftov Ad-Aware SE in SpyBot S&D, ki uničujejo spyware, požarni zid (Zone Alarm), najnovejše popravke operacijskega sistema in predvsem pametna uporaba interneta in emaila. S tem mislim na razne priponke in neznane pošiljatelje, emaila lahko odpirate in brišete tudi preko interneta (webmail), ogledovanje strani s sumljivo vsebino (erotika, warez-piratstvo...), uporaba raznih programov kot so Kazaa, eMule, eDonkey...Vse to je potencialna nevarnost, da se naš sistem okuži. Tudi raznim oknom na internetu v stilu »Your computer is infected with spyware. Click here to remove it!« ne gre zaupati. Na internetu ne klikajte tistega, za česar ne veste, kakšne posledice bo imelo (uporabite X v zgornjem desnem kotu). Računalniških virusov je vedno več, postajajo kompleksnejši in očitno postaja zelo zanimiva širitev virusov na ostale platforme (Symbian-mobilni telefoni). Šušlja se tudi, da avtorji antivirusnih programov velikokrat napišejo kakšen virus za testiranje učinkovitosti programa. Očitno jim kakšen tudi »uide«. Veliko avtorjev virusov se po prestani zaporni kazni, zaposli v kakšnem izmed antivirusnih podjetij. Internet le ni tako nedolžen, kot se nekaterim zdi. Za konec še nasvet za odstranitev Sasserja. Okno z odštevanjem ustavimo tako, da ko se nam prikaže, kliknemo Start -> Run -> »shutdown -a«. Okno se zapre, mi pa moramo namestiti najnovejše popravke in na računalnik naložiti »Sasser removal tool«. Želim vam še veliko uspešnega surfanja in čimmanj virusov!

Klemen Konič