Matej Kostrec

História počítačových vírusov

Vznik vírusov

Historici presne nevedia, kedy sa objavil prvý počítačový vírus. Jediné, čo je isté, je skutočnosť, že prvý počítač vynájdený Charlesom Babbadge nebol nikdy napadnutý žiadnym vírusom. V polovici 70-tych rokov minulého storočia však už počítače Univax 1108 a IBM 360/370 takéto šťastie nemali. To znamená, že pojem počítačového vírusu vznikol ešte predtým. Mnohí špecialisti sa domnievajú, že vznik tohto pojmu sa spája s prácami Johna von Neumann na matematických automatoch na automatické kopírovanie. Už v roku 1951 Neumann navrhol viaceré metódy, ako vytvoriť takéto automaty. Britský matematik Lionel Pendrose predstavil v roku 1959 jednoduchý dvojdimenzionálny model samokopírovacích automatov, ktoré sa mohli aktivovať, množiť, mutovať a napádať. O niekoľko mesiacov neskôr prepísal Frederick G. Stathl tento model do strojového kódu na počítač IBM 650. Cieľom týchto vedcov v ich výskumoch nebol vývoj počítačového vírusu, ale naopak, zlepšenie podmienok ľudského života.

V roku 1962 vytvorila skupina inžinierov v laboratóriách spoločnosti Bell Telephone počítačovú hru s názvom *Darwin*. Hra bola zostavená okolo *„sudcu“* umiestneného v pamäti počítača, ktorý definoval pravidlá a herný poriadok medzi konkurenčnými programami vytvorenými hráčmi. Tieto programy mohli sledovať a ničiť programy konkurentov, ale aj znásobovať svoju existenciu. Hra spočívala v likvidácii programov konkurentov a kontrole bojového poľa. Táto pôvodne neofenzívna hra, napísaná vedcami a inžiniermi, sa stala námetom na počítačové vírusy, pretože ľudia pochopili, že teória automatického kopírovania a reprodukcie by mohla byť úspešne aplikovaná aj na úplne iné ciele.

70. roky minulého storočia

Začiatkom 70-tych rokov bol odhalený v americkej armádnej počítačovej sieti ARPANET, ktorá bola predchodcom INTERNETU, počítačový vírus *Creeper*. Bol naprogramovaný pre systém *Tenex,* prevádzkovaný a využívaný verejnosťou, a tento vírus bol schopný sám pristupovať do vzdialeného systému prostredníctvom modemu a nakopírovať sa tam. Na napadnutých systémoch sa objavovalo hlásenie : *„I´M THE CREEPER : CATCH ME IF YOU CAN“*. O niekoľko týždňov neskôr bol neznámymi autormi vytvorený program *Reaper*, ktorý ničil vírus Creeper. Samotný Reaper je vírusom, šíri sa po počítačoch pripojených na sieť a zničí Creepera vždy, keď ho nájde. Dodnes nie je jasné, či Reaper vytvorila osoba alebo skupina osôb, ktorí boli autorom Creepera, aby opravili svoju chybu, alebo impulzom na jeho vytvorenie bola reakcia proti útokom Creepera.

V roku 1974 sa objavil vírus nazvaný *Rabbit (zajac)*, ktorého cieľom bolo iba množiť sa a prenikať do iných počítačov. Meno dostal ako paralelu rýchleho zvieraťa, pretože sa množil neuveriteľnou rýchlosťou. Zahlcoval systém svojimi vlastnými kópiami, čím značne spomaľoval výkon počítača. Ak Rabbit dosiahol určitú úroveň zahltenia napadnutého počítača, tak sám zastavil svoje ďalšie množenie sa.

V roku 1975 vznikla nová počítačová hra napísaná pre počítač Univac 1108, ktorá dostala meno *Pervading Animal (prenikajúce zviera)*. Počítačoví experti si ešte dnes lámu hlavy nad tým, či išlo len o iný počítačový vírus alebo prvého *trójskeho koňa.* Pravidlá hry sú veľmi jednoduché. Hráč musí myslieť na nejaké zviera a program mu kladie otázky, aby uhádol, na ktoré zviera hráč myslí. Hra je vybavená automatickou opravnou funkciou. Ak sa programu nepodarí uhádnuť zviera, zaktualizuje sa a začne klásť nové otázky. Aktualizovaná

verzia potlačí pôvodnú, ale navyše na nakopíruje do iných registrov a súborov. Po určitom čase obsahujú všetky registre a súbory kópie *Pervading Animal* a objem kópií hry zaberá obrovský priestor na počítačových diskoch.

80. roky minulého storočia

V tomto období rástla popularita využívania počítačov a s ňou narastal aj počet ľudí, ktorí začali písať vlastné počítačové programy. Moderné telekomunikačné technológie ponúkali kanály umožňujúce sprostredkúvať programy pomocou serverov s otvoreným prístupom, napríklad servery BBS – Bulletin Board System. Priekopníkmi v používaní serverov BBS sa stali univerzity a ich prostredníctvom vznikala svetová databáza údajov prístupná vo všetkých rozvinutých krajinách. Začiatkom 80-tych rokov sa objavili prvé trójske kone a ich počet neustále rástol. Tieto programy sa nekopírovali a nenapádali systémy, ale poškodzovali systémy, ak boli na počítač nainštalované alebo prenášané po sieti.

Rozširujúce sa používanie počítačov Apple podnietilo v roku 1981 záujem tvorcov vírusov aj o túto platformu. Preto neprekvapuje, že v tom istom roku sa prejavila prvá rozsiahla epidémia počítačového vírusu aj na platforme Apple II. Vírus *Elk Cloner* sa šíril tak, že napádal operačný systém Apple nahratý na disketách. Pri štarte operačného systému z nakazenej diskety sa automaticky naštartovala kópia vírusu, ale vírus nezasahoval do fungovania počítača, iba kontroloval prístup na disk a externé médiá. V prípade vloženia nenakazenej, zdravej diskety do počítača sa vírus nakopíroval na ňu a nakazil ju. Takýmto spôsobom sa postupne šíril po disketách, ktoré boli v tom čase hromadne používaným počítačovým médiom.

Rok 1983 bol prelomovým rokom z hľadiska definovania pojmu *počítačový vírus.* 10. novembra 1983 počas seminára o informačnej bezpečnosti, organizovanom Univerzitou v Lehigh, bola praotcom modernej počítačovej virológie Lenom Eidelmen urobená ukážka programu na systéme VAX 11/750, ktorý sa správal ako vírus, t. j. bol schopný sa nainštalovať na všetky ostatné objekty systému. O rok neskôr na 7. výročnej konferencii o informačnej bezpečnosti Eidelman definoval pojem ***počítačový vírus*** ako ***program schopný nainfikovať ostatné programy tým, že ich zmení, aby mohol nainštalovať svoje vlastné kópie.*** **Počítačový vírus je teda program, ktorý sa sám automaticky kopíruje a reprodukuje.**

V roku 1986 bola odhalená prvá epidémia vírusu na platforme IBM. Vírus *Brain* sa v priebehu niekoľkých mesiacov rozšíril po celom svete. Autormi vírusu bol 19-ročný pakistanský programátor Basit Faroog Alvi a jeho brat Amiad. Vírus obsahoval aj riadok textu, na ktorom bolo uvedené meno jeho autorov, ich adresa a číslo telefónu. Obaja pracovali pre spoločnosť, ktorá predávala softvér, a svoj čin vysvetľovali tým, že chceli zistiť úroveň implementácie pirátskych kópií vo svojej krajine. Okrem napadnutia operačného systému a zmeny mena disku na ©Brain nespôsoboval vírus žiadne zmeny v údajoch. Obaja bratia však nad ním stratili kontrolu a vírus sa rozšíril do celého sveta. Vírus Brain je považovaný za priekopníka tzv. *plazivého vírusu*, ktorý sa správa tak, že v prípade pokusu o čítanie dát z napadnutého sektora počítača napadne v počítači aj dovtedy zdravé dáta a automaticky z nich rekurzívne vytvára kópie.

Objavenie sa vírusu *Vienna* v roku 1987 a jeho rozšírenie sa po celom svete bolo predmetom rôznych diskusií, ale najmä záujmu medzinárodnej komunity informatikov o identifikáciu autora tohto vírusu. Autorstvo dodnes nie je jednoznačné, pretože dvaja potenciálni autori Franz Swoboda a Ralf Burger sa navzájom obviňujú z poslania vírusu. Napriek tejto nejasnosti o autorstve je vírus Vienna významným z iného dôvodu. Po prvýkrát v histórii sa podarilo nájsť prostriedok na neutralizáciu vírusu. Bernt Fix, ktorému sa to

podarilo, je považovaný za predchodcu nových špecialistov vytvárajúcich *antivírusové neutralizátory a moduly na ochranu, odhalenie vírusov a dezinfenkciu.*

Svetoznámy vírus *Lehigh*, ktorý sa objavil tiež v roku 1987, vstúpil do histórie ako prvý vírus, ktorý priamo poškodzuje údaje. Vírus ničí dáta uložené na diskoch. Našťastie Univerzita Lehigh v Pensilvánii, kde vírus vznikol a podľa ktorej dostal svoje meno, disponovala viacerými počítačovými expertmi z oblasti analýzy vírusov, a tak vírus v skutočnosti nikdy neopustil múry univerzity. Začal však epochu používania deštruktívnej rutiny, ktorou vírus zničil a zlikvidoval nielen všetky hodnotové údaje z počítača, ale aj sám seba. To podnietilo používateľov, aby sa začali serióznejšie zaoberať problematikou informačnej bezpečnosti a ochrany pred vírusmi.

V roku 1987 bola naprogramovaná neznámym autorom v Izraeli skupina vírusov, ktorá niesla spoločné meno *Suriv (čítané od konca – virus)* a modifikovala inštalačné procedúry súborov rôznych formátov. Verzia s označením Suriv-1 napádala súbory formátov COM, ku ktorým pristupoval v reálnom čase. Pri zapnutí nainfikovaného počítača sa nakopíroval do jeho pamäte, kde zostal aktívnym až do jeho vypnutia. Vírus postupne prerušil všetky bežiace operácie, čím donútil používateľa spustiť súbor COM, ktorý vírus okamžite infikoval. Vírus Suriv-2 napádal súbory formátu EXE a Suriv-3 bol kombináciou prvých dvoch verzií. Suriv-4, ktorý poznáme aj pod menom *Jerusalem,* bol ešte sofistikovanejšou verziou svojich predchodcov a rozpútal svetovú vírusovú epidémiu a v „čierny“ piatok 13. mája 1988 zničil súbory s údajmi na všetkých kontinentoch.

Prvá veľká epidémia na lokálnej sieti vypukla v decembri 1987. Červ *Christmas Tree (Vianočný stromček)* napadol operačné systémy VM/C MS-9. Červ bol pustený do siete Bitnet z univerzitnej siete v Nemecku cez portál EARN (Európska akademická a výskumná sieť) a následne aj cez IBM sieť Vnet. Štyri dni po jeho spustení vírus zahltil sieť. Ihneď po napadnutí počítača zobrazil vírus na jeho obrazovku vianočný stromček a poslal jeho kópie všetkým užívateľom, ktorých adresy sa nachádzali v adresároch systémov zapojených na sieť.

Rok 1988 sa zapísal do histórie objavením sa prvého šifrovaného vírusu *Cascade*. Hneď ako bol vírus aktivovaný, začali ikony na obrazovke počítača padať smerom nadol. Vírus pozostával z dvoch častí, a to tela vírusu a šifrovacieho programu. Tento program zakódoval telo vírusu, aby mu dal v každom napadnutom súbore iný vzhľad. Pri aktivovaní vírusu bolo najprv telo vírusu dekódované a až následne spustil vírus svoje kaskádové aktivity. Cascade je považovaný za predka polymorfných vírusov, ktorý kódoval iba telo vírusu a za dekódovací kľúč používal dĺžku napadnutého súboru. Dekódovací program sa nemenil, a preto umožnil moderným antivírusovým prostriedkom ľahkú detekciu vírusu. Princíp automatického šifrovania používaný pri víruse Cascade a informácie o neutralizácii vírusu Vienna sa stali podkladom pre Marka Washburn na vytvorenie prvej skupiny polymorfných vírusov *Chameleon.*

Ďalší červ, ktorý poznáme pod menom jeho autora *Morris*, využíval slabiny operačného systému UNIX na platformách VAX a SUN. Používal aj viaceré inovatívne metódy prístupu k systémom s cieľom získať heslá. Straty, ktoré v roku 1988 spôsobil tento červ, boli odhadnuté na 96 miliónov amerických dolárov, čo bola v tom období značná čiastka.

V roku 1989 sa objavili vírusy *Datacrime* a skupina vírusov *Vacsina a Yankee.* Vírus Datacrime bol zvlášť nebezpečný. Preformátovával cylinder pevného disku, čo vyvolalo deštrukciu údajov uložených v súboroch FAT, ktoré nebolo možné obnoviť. V Spojených štátoch spôsobil paniku, napriek nie veľmi závažným škodám, ktoré spôsobil. Nazvali ho *Columbus day*, pretože si veľa ľudí myslelo, že vírus bol naprogramovaný nórskymi teroristami, ktorí chceli potrestať Američanov za to, že prisúdili objavenie Ameriky Krištofovi Kolumbovi, a nie Erikovi Červenému, vikingovi nórskeho pôvodu, ktorý sa prvý vydal na západ objavovať nové krajiny.

V Holandsku sa v roku 1989 rozhodla miestna polícia začať aktívny boj proti počítačovej kriminalite. Vyvinula antivírusový program schopný neutralizovať *Datacrime* a predávala ho priamo miestnym komisariátom za symbolický 1 dolár. Dopyt po tomto softvéri bol veľmi vysoký, ale neskôr sa zistilo, že antivírusový program nebol vierohodný a vyvolával falošné poplachy. Následne bola publikovaná druhá verzia, ale aj tá obsahovala početné chyby.

V decembri 1989 bola poslaná na 20 000 adries po celom svete informačná disketa o AIDS obsahujúca trójskeho koňa. Adresy boli odcudzené z databázy odborného časopisu PC Business World. Hneď ako bola nakazená disketa prečítaná, trójsky kôň sa automaticky nainštaloval do systému, vytváral svoje vlastné skryté súbory a adresáre a modifikoval systémové súbory. Po 90 vykonaných zmenách zakódoval operačný systém mená všetkých súborov, čo znamenalo, že nebolo možné sa k nim dostať a ponechal iba jediný súbor, ktorý vyzýval používateľa, aby zaplatil peniaze za používanie počítača na určitý bankový účet. Táto skutočnosť pomohla odhaliť autora tohto trójskeho koňa, taliana Josepha Poppa, ktorý bol vyhlásený za blázna a odsúdený v neprítomnosti talianskou justíciou.

Koncom 80. rokov sa aktivizovali aj autori antivírusových programov a svetlo sveta uzreli predchodcovia Kasperského antivírusového balíka *AVP Antiviral Toolkit Pro,* ale aj neutralizačné programy *F-Prot, ThunderBYTE, Norman Virus Control a Virscan.* Rok 1989 bol prelomovým aj prvými publikáciami venovanými boju proti vírusom. Vydavateľstvo Sophos začalo vo Veľkej Británii vydávať časopis Virus Bulletin, ktorý existuje až dodnes, a vydavateľstvo Dr. Solomon´s uviedlo na trh odborný časopis Virus Fax International, ktorý bol neskôr premenovaný najskôr na Virus News International a potom na Secure Computing, ktorý je momentálne považovaný za najpopulárnejší zdroj informácií v oblasti informačnej bezpečnosti.

Roky 1990 – 1995

V roku 1990 prišlo k rozmachu prvých polymorfných vírusov. Objavila sa veľká skupina vírusov *Chameleon,* v ktorých sa kryptovaný kód menil pri každom nakazenom počítači. Táto vlastnosť ich chránila pred vtedajšími antivírusovými programami, ktoré boli založené na vyhľadávaní kódu známeho vírusu. Chameleón však neobsahoval stály kód, preto bolo potrebné vyvinúť nový rad špeciálnych algoritmov schopných identifikovať polymorfné vírusy. V roku 1992 Eugen Kaspersky objavil emulačný procesor schopný dešifrovať kódy, ktorý bol účinný na neutralizáciu tohto typu vírusov. Jeho technológia sa stala neoddeliteľnou súčasťou moderných antivírusových programov.

Začiatkom 90. rokov sa veľmi aktivizovala bulharská liaheň vírusov. Najaktívnejším autorom bol Dark Avenger, vďaka ktorému sa 15. BBS (Bulletin Board Service), konané v 1990 v Bulharsku, stalo prvým fórom, kde sa vymieňali vírusy. Filozofia bola veľmi jednoduchá. Ak sa používateľovi fóra podarilo poslať vírus do siete, mohol si ako výmenu zaň vybrať iný vírus z katalógu fóra. Ak používateľ ponúkol nový zaujímavý vírus, dostal pridelený úplny prístup k zdrojom fóra a mohol posielať neobmedzený počet vírusov zo zbierky fóra. Je jasné, že po tomto fóre sa výskyt vírusov v počítačovom svete mnohonásobne zvýšil. Objavili sa aj prvé ruské vírusy *Peterburg, Voronež a LoveChild.*

Britský informatický magazín *PC Today* v roku 1990 vo svojom júlovom čísle distribuoval ako súčasť magazínu aj bezplatnú disketu nainfikovanú vírusom *DiskKiller.* Toto číslo sa predalo v počte vyššom ako 50 000 exemplárov. Epidémia, ktorá vďaka tomu vznikla, je považovaná za školu virológie.

V decembri 1990 bol v Hamburgu zriadený *European Institute for Computer Antivirus Research* (EICAR – Európske centrum výskumu boja proti počítačovým vírusom). Táto inštitúcia je dodnes považovaná za jednu z najrešpektovanejších medzinárodných organizácií

v informatickom svete. Zoskupuje vybraných odborníkov a najznámejších autorov antivírusových programov.

Vzhľadom na skutočnosť, že v roku 1991 existovalo už viac ako 300 rôznych druhov vírusov, začali sa viac aktivizovať autori antivírusových programov. Na počítačových trhoch sa objavili *Norton Antivirus, Central Point Antivirus a Untouchable* od spoločnosti Fifth Generation System, ktorú neskôr odkúpila spoločnosť Symantec. Spomedzi vírusov, ktoré uzreli svetlo sveta v tomto roku, môžeme spomenúť polymorfný vírus *Tequila*, ktorý napádal sektor zavádzania a spúšťania operačného systému počítača, a vírus *Dir_II*, používajúci úplne novú metódu nakazenia súborov, a to technológiu presmerovania pointrov. Tento vírus zostal až do dnešného dňa jediným exemplárom takéhoto typu.

Začiatkom roka 1992 vyvinul jeden z najznámejších autorov vírusov Dark Avenger polymorfný generátor *MTE*, ktorého funkcia spočívala v integrácii do iných polymorfných vírusov, aby im uľahčila ich prieniky do dátových súborov. Generátor bol dodávaný vo forme modulu, ktorý bol okamžite spustiteľný a obsahoval aj dokumetáciu na jeho použitie. V tom istom roku sa objavil nielen silne medializovaný vírus *Michelangelo*, ale aj prvé anti-antivírusové programy, ktoré ničili databázy kontrolných mechanizmov antivírusových programov. Ak antivírusový program nenašiel takúto databázu, začal si ju budovať od začiatku, a tak existujúce vírusy neboli odhalené a mohli napádať systém.

Aj policajné a súdne orgány na celom svete začali zriaďovaním špecializovaných oddelení určených na boj proti počítačovej kriminalite, klásť dôraz na odhaľovanie tohto typu kriminality. V roku 1992 zlikvidoval policajný oddiel počítačovej kriminality New Scotland Yard skupinu britských autorov vírusov. Zdá sa, že aktivita tohto oddielu až do dnešného dňa bráni novému združovaniu sa tvorcov vírusov vo Veľkej Británii.

V roku 1993 sa aktivizovala spoločnosť Microsoft a uviedla na trh svoj prvý vlastný antivírusový produkt *Microsoft AntiVirus*, ktorý bol súčasťou štandardných verzií MS DOS a Windows. Prvé užívateľské pokusy naznačovali vysokú účinnosť, avšak neskôr sa kvalita znižovala a spoločnosť od projektu vlastnej tvorby antivírusových programov ustúpila.

Problematika vírusov na CD nosičoch zaznamenala v roku 1994 veľký rozmach. Extrémna popularita tohto nosiča dát sa stala jedným z hlavných cieľov šírenia vírusov. Ani nové služby v podobe využívania internetu a elektronickej pošty neodolali vírusovým epidémiám. Ako príklad si uvedieme len niektoré typovo najvýraznejšie, ktoré sa objavili v roku 1994. *Shifter* - prvý vírus napádajúci súbory OBJ, *Phantom 1*- prvý polymorfný ruský vírus, skupina vírusov *ScrVir* – napádajúca zdrojové programy napísané v jazyku C a Pascal, *OneHalf* – ktorý je do dnešného dňa aktívny a spôsobuje značné škody a *Zaraza* – používajúci unikátnu metódu inštalácie systému MS DOS.

V roku 1995 mali problémy s vírusmi viaceré veľké počítačové spoločnosti. Spoločnosť Microsoft poslala svojim testovačom nainfikované beta verzie Windowsu 95. Iba jeden z nich však pristúpil k antivírusovej analýze a na disketách objavil vírus *From*. Napriek tomu, že Microsoft zvýšil úroveň antivírusovej kontroly, už v auguste toho istého roku bol operačný systém MS Windows napadnutý vírusom *Concept*, ktorý zaberá jedno z popredných miest v zozname najrozšírenejších vírusov, ktorý vedú autori antivírusových programov. Ani spoločnosť Digital Equipment Corporation, významný výrobca hardvéru, sa nevyhla napadnutiu svojich produktov vírusom *Concept*, ktorý nešťastnou náhodou distribuovala účastníkom medzinárodnej konferencie v Dubline. Vírus bol však veľmi skoro odhalený a Digital sa ešte na konferencii ospravedlnil. Aj objavenie sa prvých makrovírusov, napádajúcich makrá v MS Office, spôsobilo vrásky na tvárach producentov antivírusových programov.

Rok 1995 bol krutý, ale aj úsmevný pre počítačovú revue PV Magazine, ktorý predával jedno zo svojich čísiel aj s disketou napadnutou vírusom *Sampo*. Tento omyl bol čoskoro odhalený, ale iróniou osudu je, že disketa bola dodatkom k číslu venovanému

problematike antivírusových testov. Aj súdne orgány posilnili boj proti počítačovej kriminalite. 16. januára 1995 poslal oddiel počítačovej kriminality New Scotland Yard pred súd Christophera Pile, nezamestnaného autora a distribútora viacerých vírusov. Pile vykonával svoje nekalé aktivity pod pseudonymom Čierny Barón a bol obvinený z napísania polymorfných vírusov *Queeg, Pathogen a SMEG*. Po 10 mesiacoch bol Pile uznaný za vinného a odsúdený na 18 mesiacov väzenia.

Roky 1996 – 1999

V marci 1996 napadol vírus *Win.Tentacle* počítačovú sieť v nemocnici vo Francúzsku. Tento vírus bol prvým vírusom na operačnom systéme Windows, ktorý bol objavený v reálnom prostredí každodenného života. Do tohto obdobia bola väčšina vírusov na Windows posielaná len do katalógov fór organizovaných autormi vírusov alebo do odborných periodík určených pre počítačových nadšencov a špecialistov. Pred objavením sa vírusu *Win.Tentacle* sa v reálnom prostredí vyskytli iba vírusy napádajúce sektor spúšťania operačného systému, operačný systém DOS a makrá.

Rok 1996 je považovaný za začiatok útokov nelegálnej komunity informatikov proti operačným systémom Windows 95 a Windows NT, ako aj proti všetkým aplikáciám Microsoft Office. Objavili sa desiatky vírusov na operačných systémoch a stovky vírusov určených na deštrukciu makier. V tomto období sa začali počítačové vírusy orientovať na 32-bitové operačné systémy, čo samozrejme malo dosah aj na vznik nového typu antivírusových neutralizačných prostriedkov.

Vo februári 1997 sa objavil vírus *Linux Bliss,* prvý vírus napádajúci operačný systém Linux. Aj keď sú vírusy namierené proti Linuxu podstatne zriekavejšie ako tie, ktoré boli vyvinuté pre Windows, ich aktivita má tiež ťažko odhaliteľnú sofistikovanú podobu. V apríli 1997 uzrel svetlo sveta vírus *Homer*, ktorý je považovaný za prvého sieťového červa napádajúceho sieť prostredníctvom protokolu FTP. Rozvoj internetu a chatovania cez internet sa taktiež stal záujmom autorov vírusov. Koncom roka 1997 bol špecialistami pre boj proti vírusom odhalený nový typ počítačového červa, ktorý sa šíril cez kanály Internet Relay Chat. Tento červ menil v adresári, kde sú uložené prenášané súbory, súbor príkazov SCRIPT.INI tým, že automaticky prepisoval pôvodný súbor na vzdialenom počítači tak, aby pri opätovnom prihlásení sa distribuoval červa do počítačov ostatných užívateľov.

Rok 1997 je povestný aj rôznymi škandálmi, ktoré sa udiali medzi spoločnosťami zaoberajúcimi sa vývojom antivírusových prostriedkov. Najprv to bol konkurenčný boj spoločnosti McAfee proti Dr. Solomon´s, v ktorom sa navzájom obviňovali z nedokonalosti svojich antivírusových produktov, ako aj z nekalej marketingovej kampane. Potom taiwanský informatik Trend Micro obvinil spoločnosti McAfee a Symantec z krádeže jeho patentu antivírusovej analýzy elektronickej pošty. A o niekoľko týždňov neskôr Symantec obvinil McAfee z používania kódu vychádzajúceho z princípu neutralizačných programov Norton AntiVirus od spoločnosti Symantec.

Aj v roku 1998 pokračuje nárast vírusových útokov na všetky druhy počítačov a operačných systémov. Vírusy využívajú na svoje šírenie nové možnosti technológií a infikujú komplexnejšie počítače svojich obetí. Objavuje sa veľký počet trójskych koní naprogramovaných tak, aby odchytili heslo (rad vírusov *PSW*) a poskytli možnosť ich tvorcom obohatiť sa prostredníctvom elektronických finančných transakcií. Vznikajú aj polyfunkčné vírusy, napríklad *Triplicate*, ktorý napáda súčasne dokumenty Wordu, Excelu i PowerPointu.

V tom istom roku sa objavil aj prvý vírus *Java.StrangeBrew,* infikujúci programovací jazyk Java, ale aj tri vírusy (*VBS)*, schopné nakaziť skripty Visual Basicu používané na tvorbu webových stránok. Kasperského spoločnosť Kaspersky Lab, ktorá bola najrenomovanejšou

spoločnosťou pre oblasť produkcie antivírusových prostriedkov, publikovala hĺbkovú štúdiu o hrozbách, ktoré predstavujú vírusy *VBS*. Mnohí počítačoví špecialisti vyhlasovali, že Kasperského idey sú alarmistické a schválne prispievajú ku kolektívnej hystérii. Vývoj v nasledujúcich mesiacoch mu však dal za pravdu. O šesť mesiacov po publikovaní štúdie zamoril celý svet vírus *LoveLetter* (známy aj pod menom *IloveYou* spôsobil epidémiu aj na Slovensku), ktorý patrí dodnes k najrozšírenejším a najnebezpečnejším.

Je zvláštne, že najvýznamnejšou udalosťou roka 1999 nebolo objavenie sa nejakého supervírusu, ale kúpenie austrálskeho vydavateľa antivírusových programov Cyber spoločnosťou, ktorá je považovaná za giganta informatiky, a to Computer Associates. Ich produkty z oblasti antivírusovej ochrany sa zlúčili pod jednotné názvy *CA Vet Anti-Virus* a *CA InnoculateIT*, ktoré sú používané dodnes. Ale ani objavovanie sa nových vírusov v tomto roku nezaostávalo. Vírus *Happy99* patrí medzi prvé moderné červy, ktoré otvorili novú éru vo vývoji škodlivých a zákerných kódov. Šíri sa prostredníctvom MS Outlooku, ktorý sa stal štandardom elektronickej pošty vo väčšine európskych a amerických podnikov, a ešte stále mu v rebríčku Top 10 najrozšírenejších vírusov patrí popredné miesto. Obdobné vlastnosti mali aj ďalšie vírusy, ako napríklad *Caligula, SK a Melissa.* Zaujímavým bol najmä vírus Melissa, ktorý zlikvidoval zoznam adries uložených v Outlooku, ale ešte predtým poslal na prvých 50 adries svoju vlastnú kópiu. Správal sa tak, ako keby poslanie správy naozaj prichádzalo od skutočného odosielateľa. Napriek tomu, že sa veľmi rýchlo podarilo nájsť adekvátny antivírusový prostriedok proti Melisse, vírus spôsobil značné škody vo viacerých informačných systémoch. Policajné orgány v prípade Melissy reagovali tiež veľmi rýchlo a vypátrali autora vírusu Davida L. Smitha, 31-ročného programátora z New Jersey, ktorý bol odsúdený na 10 rokov väzenia a pokutu 400 000 amerických dolárov.

7. decembra 1999 bol odhalený mimoriadne nebezpečný vírus *Babylonia,* ktorý znamenal obrat v produkcii vírusov. Bol to totiž prvý vírus, ktorý sa sám dokázal na diaľku obnoviť. Každú minútu sa pripojil na jeden japonský server, aby jeho prostredníctvom poslal na nakazené počítače zoznam modulov vírusu. Ak boli vírusy na poslanom zozname novšie ako tie, ktoré sa nachádzali na nakazenom počítači, tak ich ihneď preposlal na tento počítač. Obdobná technika bola neskôr použitá aj inými vírusmi, napríklad *Sonic a Hybris.*

Koniec roka 1999 bol v počítačovom svete spojený s prechodom na rok 2000 a nové milénium. Mnohí ľudia boli presvedčení, že komunita počítačových pirátov a autorov vírusov pripraví pri tejto príležitosti nepríjemné prekvapenie v podobe vytvorenia tisícov vírusov, ktoré položia ľudskú civilizáciu na kolená. Apokaliptické prognózy sa nenaplnili a rok 2000 prišiel rovnakým spôsobom ako predchádzajúce roky.

Roky 2000 – 2001

Rok 2000 sa začal neočakávaným spôsobom pre užívateľov systému Windows 2000 a Visio- programové vybavenie na tvorbu grafov a diagramov. Len čo Microsoft pustil na trh komerčnú verziu svojho nového operačného systému, členovia záškodníckej skupiny 29A ho nakazili vírusom *Inta*. Len niekoľko dní neskôr sa objavili hneď dva vírusy *Unstable a Radiant*, ktoré napadli Visio a predznamenali zánik spoločnosti Visio Corporation, ktorá bola odkúpená spoločnosťou Microsoft. Zlé jazyky hovoria, že tieto vírusy pustil do obehu Microsoft, aby mohol zrealizovať kúpu jedného zo svojich konkurentov.

Zaujímavá udalosť sa stala aj v apríli 2000. Prvý ruský makrovírus napádajúci makrá MS Wordu bol odhalený v kancelárii britského premiéra na Downing Street 10. Ani máj nezaostal v rebríčku počítačových pikantností. 5. mája bol do Guinesovej knihy rekordov zapísaný rekordný výskyt vírusu *LoverLetter*, ktorý ničil celý rad dátových súborov a automaticky sa rozosielal na všetky adresy zaznamenané v adresároch MS Outlooku nakazených počítačov. V júni sa objavil vírus *Timofonica*, ktorý ako prvý postihol aj mobilné

telefóny. Prejavil sa tak, že posielal z nakazených počítačov správy na mobilné telefóny siete MoviStar, ktorá patrí španielskemu telekomunikačnému gigantovi Telefonica.

Ani v lete roku 2000 si autori vírusov neodpočinuli. Do obehu bol poslaný vírus *Star*, prvý vírus napádajúci systém AutoCad. Osobitnú pozornosť si získal počítačový červ *Jer*. Jeho telo bolo umiestnené na webovú stránku, kde sa aktivoval pri prihlásení sa užívateľa na túto internetovú stránku. Jeho autor využíval metódu sociálneho inžinierstva, psychologického pôsobenia na ľudských jedincov, a to formou masového marketingu na pritiahnutie pozornosti používateľov stránky. Kto klikol na ikonku, pod ktorou sa skrýval vírus, si ho nechtiac natiahol aj do svojho počítača. Treba úprimne povedať, že kampaň bola úspešná, pretože sa dalo nachytať niekoľko tisíc používateľov internetu. Jeseň – naopak – patrila tvorcom antivírusových produktov. Spoločnosť Kaspersky Labs zmenila meno svojho kľúčového produktu, a tak sa z AntiViral ToolkitPro stal Kaspersky Anti-Virus. Vo všeobecnosti je možné potvrdiť, že rok 2000 sa stal rokom šírenia vírusov prostredníctvom elektronickej pošty. Podľa štatistík spoločnosti Kaspersky Labs až 85 % vírusov sa dostalo do počítačov práve touto cestou.

Rok 2001 sa vyznačuje tým, že autori vírusov ustúpili vďaka častejšiemu využívaniu internetu od tvorby klasických vírusov, najmä makrovírusov a skriptových vírusov, v prospech červov. Aj štatistiky útokov červami sa oproti predchádzajúcemu roku zvýšili až na 90 % z celkového počtu registrovaných útokov spôsobených rôznymi formami škodlivého softvéru. Tento rok sa stal prelomovým aj vo vývoji vírusov útočiacich cez internet. Predtým sa väčšina útokov diala prostredníctvom sťahovania nakazených súborov cez internet. Od roku 2001 stačí jednoduchá návšteva napadnutej webovej stránky. Autori vírusov začali nahrádzať zdravé stránky nakazenými. Väčšina používateľov internetu si nakazila svoje počítače škodlivými kódmi vďaka nedostatkom MS Internet Explorera. Ani operačný systém Linux sa nevyhol útokom nových vírusov. Najzaujímavejším je prípad vírusu *Ramen*, ktorý nakazil veľký počet podnikových sietí, pričom jeho obeťou sa stal aj americký Národný úrad pre letectvo a vesmír (NASA).

Najhorším prekvapením a morou roka 2001 boli bezpochyby červy šíriace sa bez prenosu údajových súborov. Tieto červy boli schopné množiť sa a fungovať v pamätiach RAM a šíriť sa ako balík špeciálne konfigurovaných dát. Táto technika spôsobila bolesti hlavy autorom antivírusových programov, pretože väčšina existujúcich prostriedkov bola proti nej neúčinná. Až po mnohých týždňoch vyvinula spoločnosť Kaspersky Lab antivírusový filter schopný nájsť v balíkoch údajov tento typ červa a zlikvidovať ho.

Roky 2002 – 2003

V roku 2002 bolo zaznamenaných 12 vírusových epidémií veľkého rozsahu a 34 epidémií stredného dosahu. Naďalej pretrvávali neutíchajúce aktivity vírusov vypustených do sveta počítačov v predchádzajúcich rokoch. Autori vírusov sa zamerali na nové platformy, nové softvérové aplikácie a nové technológie. Objavil sa vírus *Spida*, ktorý infikoval SQL servery, a *Benjamin*, ktorý zamoroval svojimi kópiami sprostredkované siete. Tento rok priniesol zvýšenú produkciu červov a škodlivých kódov, ktorých cieľom bolo odchytiť heslá, mená používateľov, prístupové dáta a ostatné dôverné údaje, ktoré umožňovali autorom týchto červov získať peniaze vďaka získaným dátam a dopustiť sa finančných podvodov.

Najzávažnejšiu epidémiu roku 2002 spôsobil internetový červ *Klez*. Červ sa objavil v októbri a počas nasledujúcich dvoch rokov mu patrilo popredné miesto v zozname najrozšírenejších vírusov, pričom až 60 % zaregistrovaných útokov sa pripisuje na vrub práve tomuto internetovému červovi. Jeho novým variantom *Klez.e* a *Klez.h* patrí táto pozícia vo svete počítačových vírusov do dnešného dňa.

Situácia v šírení sa škodlivých kódov sa v roku 2002 oproti predchádzajúcim rokom zmenila. Počas predchádzajúcich rokov sa väčšina vírusových útokov spájala s malým počtom vírusov, vo všeobecnosti s 2 alebo 3, zatiaľ čo od septembra roku 2002 bol zaznamenaný rastúci počet infikovaní počítačov vírusmi, ktorým nepatrilo ani miesto v top 20.

Používatelia si čoraz viac začali uvedomovať potrebu zvýšenia úrovne informačnej bezpečnosti a prijímania opatrení na ochranu svojich počítačov, čo bezpochyby zohralo významnú úlohu vo vývoji nových druhov vírusov. Prijaté bezpečnostné opatrenia umožnili znížiť počet incidentov spôsobených individuálnymi vírusmi. V tomto období začínajú narastať útoky, pri ktorých boli vírusy súčasťou iného druhu páchanej počítačovej kriminality.

V roku 2003 boli spustené dva útoky svetového rozmeru na internet. Je možné ich považovať za najväčšie v doterajšej histórii internetu. Prvý bol spôsobený červom *Slammer*, ktorý využil na svoje šírenie sa slabiny MS SQL serverov. Slammer je považovaný za prvého červa bez klasického tela so schopnosťami bleskového útoku. V priebehu niekoľkých minút nakazil stovky počítačov po celom svete a zvýšil objem prenosov po internetovej sieti tak, že viaceré národné úseky siete sa zahltili a zrútili. Podľa počítačových špecialistov stúpla v jednotlivých častiach siete kapacita prenosov o 40 až 80 %. Tento červ napadal počítače prostredníctvom portov 1433 a 1434. Hneď ako sa dostal do počítača, nenakopíroval sa na pevný disk, ale zostal v pamäti počítača a periodicky sa posielal na všetky adresy nachádzajúce sa v adresároch.

Druhá – ešte závažnejšia – epidémia vznikla v auguste 2003. Bola spôsobená červom *Lovesan*, ktorý využil slabiny operačného systému Windows. Na rozdiel od Slammera sa Lovesan množil a využíval na to veľkosť prevádzkovanej služby RPC DCOM Windows 2000/XP. Týmto červom bola zasiahnutá skoro celá populácia užívateľov internetu.

Ďalším extrémnym výskytom sa prejavila skupina červov *Sobig*, a najmä jeho verzia *Sobig.f*, ktorá sa v auguste nachádzala minimálne v jednej elektronickej správe z dvadsiatich. Autori tejto skupiny si prostredníctvom týchto červov vytvárali priestor na posielanie nevyžiadanej elektronickej pošty (spam). September patril červovi *Swen*, ktorý bol jeho autorom prezentovaný na internete ako korektor Microsoftu a neutralizačný prostriedok proti červom, ktoré spôsobili vírusové epidémie v roku 2003. Tento rok bol aj rokom zvýšeného výskytu trójskych koní zneužívajúcich odcudzené porty. Zaujímavá situácia vznikla v prípade trójskeho koňa *Backdoor.Agobot*, keď si jeho autor vytvoril sieť webových stránok, cez ktoré sa za minimálne 150 amerických dolárov mohol ktokoľvek stať majiteľom exkluzívnej verzie *Backdooru*, vytvorenej podľa vlastných požiadaviek a špecifikácií.

Na jeseň 2003 prekročil počet objavených trójskych koní počet odhalených klasických vírusov a táto tendencia trvá do dnešného dňa. Vo svete počítačov a internetu si našiel svoje miesto aj nový druh trójskych koní, tzv. *trójske kone proxy*. Ide o prvý nepopierateľný prípad spolupráce medzi autormi vírusov a šíriteľmi nevyžiadanej elektronickej pošty.

Rok 2003 sa stal prelomovým v šírení počítačových vírusov. S prudkým rozvojom moderných počítačových a komunikačných technológií vznikali nové možnosti ich zneužívania, a tým aj nové druhy páchania počítačovej kriminality. Nie je možné povedať, že by počítačové vírusy vymizli zo sveta počítačov, zmenila sa však forma ich využívania. Prestali byť púšťané do sietí samostatne a začali byť využívané ako súčasť spamingu, phishingu, pharmingu, cardingu a iných typov zneužívania počítačov na obohacovania sa počítačových pirátov.

Mgr. Matej Kostrec
Akadémia Policajného zboru v Bratislave
Katedra manažmentu a informatiky
e-mail: matej.kostrec@minv.sk