Počítačový vir jménem Černobyl

aneb …a zbyly jen oči pro pláč…

Ne, nemusíte se děsit, nechvalně známá ukrajinská jaderná elektrárna je v tom tentokrát nevinně. To jen neznámý počítačový „nadšenec“ stanovil 26. duben jako „Den D“, tedy den, kdy se probudí k životu virus CIH. A protože na tentýž den připadá výročí okamžiku, kdy se v roce 1986 stala černobylská jaderná elektrárna nechvalně známou po celém světě, dostal virus přezdívku Černobyl. A ne neprávem.

Mnoho počítačových uživatelů se domnívalo, že virus CIH se jich jaksi netýká a že „to už tady bylo“. Bohužel, neměli pravdu. Počítačový virus CIH byl poprvé byl detekován na Taiwanu, a to 2. června 1998. Postupně se na světlo světa dostalo několik verzí tohoto viru, z nichž jsou nejznámější varianty1.2, 1.3 a 1.4. První dvě z nich se aktivují vždy 26. každého měsíce, kdežto třetí čeká na svou příležitost do 26. dubna (a pozor - každého roku, takže pokud jste letošek „přežili“ ve zdraví, radujete se předčasně; „Černobyl“ se za rok vrátí!). Důležitá je přitom i skutečnost, že vir CIH je „doma“ v prostředí Windows-95 a –98. Čili: Pracujete-li v jiném operačním systému, nemusíte mít z CIH obavu.

Především varianta 1.4 se dočkala velmi masového rozšíření, a to poněkud paradoxně zásluhou jindy „důvěryhodných“ zdrojů. Na webu bylo možné jeden čas najít infikované demo populární hry Wing Commander – a to přímo na stránkách výrobce! Časopisy, které „rozdávaly“ vir CIH na všechny strany na svých CD-přílohách bylo jen v Evropě několik desítek. A to nemluvíme o aktualizovaných ovladačích, které byly i u mnoha renomovaných výrobců jako standardně „vybaveny“ virem CIH.

Do úplného výčtu „distributorů“ CIH je nutné započítat i jistou portugalská společnost dodávající software všem lékárnám v zemi, která vir distribuovala společně se svými programy.

Ještě štěstí, že mnoho portugalských lékáren stále ještě pracuje pod DOSem, jinak hrozilo zhroucení zdravotnictví v této zemi… Paradoxní je, že portugalský dodavatel software se v prvních chvílích snažil veškerou vinu hodit na nadnárodní Microsoft tvrzením, že vir CIH byl distribuovaný v jeho operačním systému. Tentokrát v tom ale byl počítačový gigant skutečně nevině, neb inkriminovaný operační systém je o pár let starší než CIH.

Také v Indii se počítačoví uživatelé „radovali“ z cédéčka, které bylo volně šířeno na autosalónu v Novém Delí. Že obsahovalo virus CIH, jistě netřeba zdůrazňovat.

Virus CIH je specifickým parazitním virem infikujícím PE soubory (Portable Executable). Při napadání souboru virus sám sebe rozdělí na několik částí (jejich počet se liší případ od případu), přičemž tuto informaci zapíše do „Hlavičky viru“ (viz obrázek). Díky této hlavičce je pak vir schopen své jednotlivé části, jimiž vyplňuje mezery v souboru, spojit v jeden fungující celek.

Virus se sám instaluje do paměti Windows, kde vyčkává na příkaz ke spuštění souboru a infikuje soubory s koncovkou EXE, které jsou otevírané. (Ve viru se ovšem vyskytují chyby a v některých případech počítač „zatuhne“ – to je ostatně nešvar mnoha virů, neboť autoři je zpravidla netestují.). Trigger rutina viru pracuje s Flash BIOS porty a snaží se přepsat Flash paměť „nesmysly“. Toto je možné, pokud motherboard a chipset dovolují zapisování do Flash paměti. Normálně se dá zapisování do Flash paměti zablokovat DIP vypínačem, avšak toto závisí na designu motherboard. Bohužel existují moderní motherboardy které nemohou být ochráněny DIP vypínačem - některé z nich ignorují pozici vypínače a tato ochrana nemá vůbec žádný efekt, u jiného hardware může být ochrana proti zápisu zablokována/přepsána softwarem. Trigger rutina viru CIH v tom případě přepíše data na všech instalovaných pevných discích. Virus používá příkazy přímého zápisu na disk a obchází standardní BIOS virovou ochranu, zatímco přepisuje MBR a boot sektory.

Jak je možné, že vir, který je známý již deset měsíců, natropil škodu srovnávanou s útokem legendárního viru Michelangelo? Důvodů bylo několik. Především uživatelé jeho nebezpečí podcenili – a ruku v ruce s nimi i distributoři, kteří nevěnovali dostatečnou pozornost obsahu svých CD. Virus CIH se totiž na napadeném souboru neprojeví růstem velikosti, takže není na „první pohled“ patrný. Mnozí uživatelé antivirových programů navíc podcenili aktualizační soubory.

Podtrženo, sečteno – morová ránu viru CIH byla vpravdě smrtící. Ale mohlo být ještě hůř. Ve Spojených státech se o měsíc dříve objevil vir Melissa následovaný virem Papa, které sice nic neničily, zato však zahlcovaly počítačové sítě dopisy s hesly k pornografickým stránkám. A tak si uživatelé pořídili antivirové programy, aby společně s dvojicí Melissa/Papa „vyčistili“ počítače zároveň i od viru CIH (samozřejmě neúmyslně). Díky tomu byly škody napáchané v USA relativně malé – celkem se hovořilo o deseti tisících zasažených počítačích.

Jinde to bylo horší. Mnohem horší. Jihokorejská vláda ohlásila, že napadeno bylo 240 tisíc počítačů. „Dvě až tři procenta z osmi miliónů PC v naší zemi byla zasažena,“ stojí doslova ve vládním prohlášení. Společnosti zabývající se antivirovými produkty však hlásí minimálně dvoj- až trojnásobně větší rozsah škod. Sto tisíc počítačů se proměnilo v prázdné bedny bez informací také v Číně (plus dalších 250 tisíc v Hong Kongu). V Turecku splakalo nad výdělkem tři sta tisíc počítačových uživatelů. Desítky portugalských bank a pojišťoven dodnes zoufale obnovují své data. V Malajsii vinou viru CIH poklesla úroveň obchodu o deset procent. Atakdále…

A u nás? Kalamita obřích rozměrů se nekonala, přestože žádná oficiální statistika neexistuje. Odhaduje se, že zasaženo bylo několik málo tisíc počítačů, především z řad domácích uživatelů. Stalo se tak zásluhou dostatečné osvěty a také vysoké kvality antivirových programů používaných v českých zemích.

Dnes už známe také autora (či spíše „pachatele“) počítačového viru CIH. Je jím Chen Ing-Hau (jeho jméno správně přepsané do češtiny zní Čen Jing-Chau; anglickou variantu jeho jména však uvádíme přednostně, neboť pojmenování viru je odvozeno od jeho iniciálů), bývalý student informatiky. Proč bývalý? Ze školy byl „odejit“ loni v dubnu poté, co jím napsaný virus (agentury nesdělily, zdali šlo o prototyp CIH nebo nějaký jiný „výtvor“) poškodil data ve školním informačním systému.

Přitom je zajímavá skutečnost, že Chenovi spolužáci a profesoři o viru CIH věděli a od připravovaného „vypuštění“ do světa jej varovali. Chen totiž společně s virem nevytvořil i odpovídající detekční software. Bývalý student informatiky nyní absolvuje dvouletou základní vojenskou službu. Policie už jej vyslechla a zadržela.

Jednoho se ale Chen bojí více než trestu odnětí svobody – setkání se statisíci uživateli osobních počítačů, k nimž „zavítal“ vir CIH a veškerá data z pevných disků odeslal do věčných lovišť…

Tomáš PŘIBYL

tomas.pribyl@aec.cz

Na obrázcích:

CIH12.GIF – To je on, virus CIH ve verzi 1.2.

CIH.BMP – Ilustrace znázorňující umístění viru CIH v napadeném souboru.