Časová osa Chipu: Počítačové viry

Hrozby jako Mydoom, CodeRed a I-Love-You brzdí internet a způsobují **ŠKODY V ŘÁDU STOVEK MILIONŮ EUR**. Počítačové viry nyní slaví 25. výročí své existence...

Když Fred Cohen poprvé představil své výzkumy, nikdo určitě neušil, že položil základy oboru s obratem přes tři miliardy eur. Ano, právě Fred Cohen zveřejnil v roce 1984 práci s názvem „Počítačové viry – teorie a experimenty“. V ní detailně popsal strukturu programu, který se sám dokáže „rozmnožovat“ a řídí se určitými příkazy i bez zásahu uživatele – to je první stručný popis viru. Jen o pět let později začaly specializované firmy zkoušet dostat podobné škůdce pod kontrolu pomocí antivirových programů.

Ještě v polovině osmdesátých let vypadalo vše růžově – pokud vám z počítače zmizel

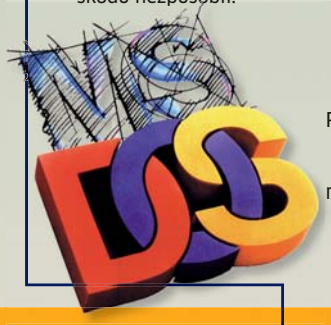
Historie počítačových škůdců

1949 – Teorie virů
V jedné ze svých prací zveřejnil John Neumann teorii, podle které se může počítačový program sám replikovat.

1982 – Nezávislé nástroje
Patnáctiletý student Rich Skrenta napsal program jménem Elk Clonek, který se šířil ze systému na systém pomocí disket. Tento program ale neobsahoval žádné „škodlivé“ funkce.

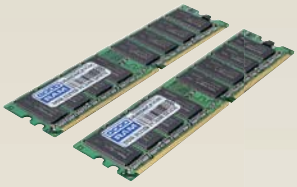
1984 – První vir
Fred Cohen představil ve své práci první funkční vir. Škůdce byl vytvořen pro operační systém Unix.

1986 – Pákistánská spojka
Prodejci softwaru ze Středního východu rozšířili první vir pro DOS. Program přejmenovával disky, ale žádnou velkou škodu nezpůsobil.



1987 – Mazací vir
První vir, který způsoboval trvalé poškození. V pátek třináctého mazal z disku všechny soubory s příponou COM a EXE.

1987 – Skrytý v RAM
Kaskádový vir skrýval sám sebe v zašifrované podobě do paměti RAM. Vypnutím počítače byl vir odstraněn.



1988 – Virový konstrukční balíček
První virový konstrukční balíček se objevil pro populární počítač Atari ST. Pomocí tohoto nástroje mohli i začátečníci bez programátorských zkušeností vytvářet obtížně identifikovatelné škůdce.

1989 – Antivirové nástroje
Na trhu se objevily první nástroje na ochranu proti nebezpečným škůdcům.

soubor, ve většině případů šlo o chybu programu nebo o nedbalost uživatele. Jen o několik let později se však už dokázaly polymorfní viry měnit a šifrovat vlastní kód. A právě to byl důvod, proč v právě se rozvíjejícím antivirovém průmyslu hodila celá řada firem „ručník do ringu“. Morfia, Jerusalem, Datacrime, OneHalf… – zkrátka zlatá doba pro autory virů, hodiny zoufalství pro běžné uživatele a škody v řádech milionů dolarů.

Viry pro každého: Nákaza přes web

V předinternetovém období nebylo pro tvůrce virů snadné své „produkty“ rozšířit. Jediným médiem v „oběhu“ byly totiž v té době diskety. Zlaté časy nastaly „zlým hochům“ až s příchodem internetu. To už mohli programátoři zákeřných kódů odesílat své nebezpečné „výtvory“ téměř komukoliv i ze svého domova – pokud byli připojeni k síti…

Internet a virové „konstrukční sady“ postavily výrobce antivirů před zcela nový problém. Doposud experti studovali každý jednotlivý vir a obranné prostředky vytvářeli přímo na míru. A zatímco 300 virů denně problém nepředstavovalo, nyní se jejich počet za den přehoupl přes hranici 30 tisíc…

Výsledek: Výrobci antivirových nástrojů začali budovat velká výpočetní centra a vytvářet programy, které by dokázaly automaticky analyzovat vzorky virů a aktualizovat signatury antivirových nástrojů. Nyní probíhá běžná automatická analýza nového škůdce jen několik sekund – přímý „zásah“ odborníků vyžadují jen obtížnější případy.

V současné době už však nejsou cílem útoků jen počítače, ale například také mobilní telefony. Prozatím se objevilo jen několik škůdců útočících na zlomek telefonů (obvykle těch „chytřejších“), experti však očekávají, že tato situace se brzy drasticky změní.

Předpokládá se, že významnou roli zde budou hrát synchronizační služby (jako například Live Mesh nebo Apple mobile), které zajišťují výměnu dat mezi mobilním telefonem a počítačem. Tyto servery mohou plnit roli perfektního distribučního prvku – a fakt je, že proti podobnému typu útoku zatím neexistuje obrana…

Dokonce i Fred Cohen však zakončil svou práci prohlášením, že operační systém může být dokonale bezpečný pouze tehdy, pokud pracuje bez „externích“ programů, není zapojen do sítě a nenabízí žádné jiné „vstupy“. To je ale v době internetu, USB disků a P2P sítí nereálná představa. Nezbývá nám tedy než být opatrní a důvěřovat výrobcům antivirových nástrojů. Ti budou muset pečovat o stále větší počet surfařů a doufat, že v tomto každodenním nekonečném boji udrží alespoň „nerozhodné“ skóre.

AUTOR@CHIP.CZ

FOTO: GDATA; ISTOCKPHOTO.COM; WIKIPEDIA/BILL BERTRAM/JACOPINO DEL CONTE/KSLINKO

Vítězství škůdců
Autoři virů dokáží své výtvory zašifrovat a skrýt je v systému pomocí polymorfního generátoru. Celá řada výrobců antivirů rezignovala na pokusy o jejich odhalení a vyřešení tohoto problému.

Červ jako milostný pozdrav
První velký počítačový „červ“ jménem I love you se šířil pomocí e-mailu a během jednoho dne dokázal napadnout miliony počítačů, na kterých mazal soubory.

Michelangelo
První vir, který si vydobyl pozornost v médiích. Tento škůdce přepisoval v den umělcových narozenin důležité systémové sektory.

BUDOUCNOST

Viry všude kolem nás
Komunikační zařízení, jako například chytré mobilní telefony nebo notebooky, jsou navzájem propojena pomocí internetu. Škůdci útočí na všechny systémy a kradou všechna dostupná data. Ochranu zaručí jen nové, efektivnější antivirové programy.

1992 · 1995 · 2000 · 2002 · 2004 · 2006 · 2009

Makroviry
Byl objeven první škůdce pro Word a spol. Zásluhou časté výměny dokumentů se v oběhu objevilo více těchto „makrovirů“ než virů útočících na operační systémy.

Nezávislé viry
Vir nové generace dokázal kromě aplikací pro Windows napadnout i soubory v Linuxu. Tento komplexní škůdce zahájil novou vlnu „nezávislých“ virů.

Mobilní telefony
Objevili se první škůdci pro kapesní PC. O rok později už škůdci napadli také zařízení s OS Symbian. K jejich většímu rozšíření ale dodnes nedošlo…

Červ Sasser
Německý student vytvořil vir, který vypínal počítače. Celkově způsobil škodu v řádu miliard dolarů…

Rádiový červ
Skupina holandských výzkumníků představila nového červa, který se může šířit pomocí RFID vysílačů.