10 virů, které způsobily NEJVĚTŠÍ ŠKODY

Stačí jen několik bajtů kódu, a z milionů počítačů po celém světě zůstane jen hromádka nepotřebného šrotu. Představíme vám deset nejúspěšnějších virů, které dohromady způsobily škody přes 100 miliard dolarů.

FABIAN VON KEUDELL

1 MYDOOM

$39 mld.

Špionážní virus s mnoha záznamy v „nej" žebříčcích. Mimo jiné šlo o nejrychleji se šířícího a nejvíce rozšířeného červa v IT historii, a to i přesto, že byl naprogramován tak, aby zůstal aktivní pouze dvanáct dnů. V době jeho největšího působení jím byl napaden každý dvanáctý e-mail.

2 BLASTER

$33 mld.

V roce 2003 ovládl tento virus tisíce počítačů a také nainstaloval backdoor, jehož pomocí neustále kontaktoval WWW stránky serverů Microsoftu. Miliony a miliony požadavků tak přetížily prostřednictvím DoS útoku aktualizační servery Windows.

3 CONFICKER

$9 mld.

Šíření viru měla na svědomí chyba související s provozem síťově sdílených adresářů, později se objevily i další varianty viru, využívající jiných chyb. Všechny varianty ale měly společné dvě věci: využívané zranitelnosti umožňovaly spuštění škodlivého programu na počítači bez vědomí uživatele a na všechny zranitelnosti již existovala záplata. Přesto bylo na začátku roku 2009 po celém světě infikováno více než 50 milionů (nezazáplatovaných) počítačů.

4 ILOVEYOU

$8,7 mld.

Tento vir, šířící se v roce 2000 jako hromadný e-mail, lze považovat za jeden z nejzákeřnějších, protože mazal soubory se specifickými koncovkami. Jeho autorem je pravděpodobně Onel de Guzman, filipínský programátor. Ten byl ale propuštěn, protože jeho země neměla žádné zákony proti počítačové sabotáži.

5 SASSER

$3,5 mld.

Kvůli chybě v systémové službě LSASS dokázal malware Sasser v roce 2004 kdykoliv vypnout uživateli počítač. Zanedlouho poté, co Microsoft nabídl odměnu 250 000 dolarů za důkazy vedoucí k odhalení viníka, byl autor objeven. Byl jím osmnáctiletý německý student Sven Jaschan z Rotenburgu, který byl nakonec podmíněně odsouzen na 21 měsíců.

6 CODE RED

$2,6 mld.

V roce 2001 ovládl počítače červ, který využíval infiltraci pomocí přetečení bufferu. Ovládnuté počítače později použil pro DoS útoky na webové stránky Bílého domu. Zdrojový kód pocházel z Filipín, stejně jako malware Iloveyou.

7 SOBIG.F

$2,5 mld.

Tento červ – botnet je šestou verzí důmyslné rodiny virů z roku 2003. Poslední verze byla považována za zvláště účinnou: dokázala se například rozeslat na všechny e-mailové adresy, které bylo možné najít v systému. Červ prohledával nejen poštovní adresáře, ale i textové soubory. Pro odesílání si navíc malware nainstaloval svůj vlastní poštovní server.

8 SQL SLAMMER

$1,2 mld.

V roce 2003 virus zaútočil na počítače s nainstalovaným SQL serverem a tím způsobil „zamrznutí" všech bankomatů v USA. Polovina z hlavních síťových uzlů na webu byla infikována po patnácti minutách a virus se také dostal do jaderné elektrárny.

9 MELISSA

$1,1 mld.

V roce 1999 se Office makrovirus sám bez vědomí uživatele rozeslal na prvních padesát kontaktů v adresáři oběti, což ve finále vyústilo v přetížení serveru. Američan David L. Smith, který byl za malware zodpovědný, byl odsouzen na dvacet měsíců vězení a k zaplacení 5 000 dolarů. Podle Smitha byl virus pojmenován po striptérce.

10 NIMDA

$590 mil.

Načasování útoku backdoor malwaru Nimda na 11. září 2001 ukazovalo na organizaci al-Káida, experti z firmy F-Secure však ve zdrojovém kódu nalezli text „Concept Virus (CV) V.5, Copyright(C)2001 R.P. China". Podle Petera Tippetta, autora Norton Antiviru, se Nimda stala nejrozšířenějším virem své doby za pouhých 22 minut.