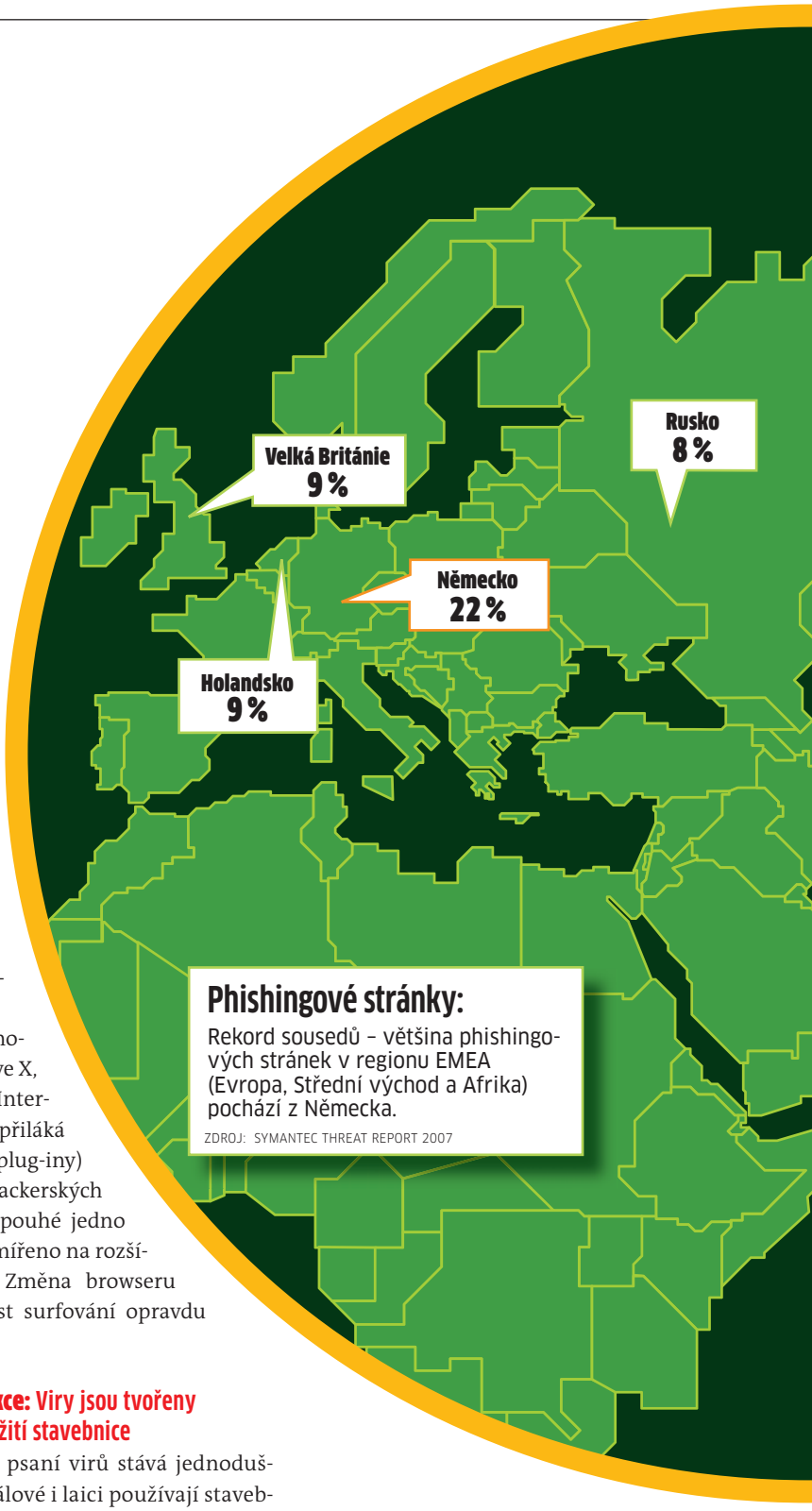
Zaostřeno na: Nebezpečí z webu

Malwarový útok

Je to **JAKO ZÁPLAVA:** číslo udávající počet malwarových útoků se v roce 2007 zdvojnásobilo. Čím dál tím častěji infikují vykradači dat počítače svých obětí.

AXEL SCHOEN



Jednou si na to snad zvykneme: na divoce blikající bezpečnostní skenery při surfování na internetu, na bezpečnostní soupravy, které si „na pozadí" zaberou polovinu z výpočetního výkonu PC, a na obtěžující výzvy operačního systému. Proč tolik pesimismu? Protože jsme si jisti, že současná záplava virů na webu jen tak neustoupí. Podle firmy F-Secure ohrožovalo v roce 2007 bezpečnost počítačů více než 500 000 malwarů. Dokonce ani počítačoví programátoři bezpečnostních firem nemají šanci udržovat se zločinci tempo, takže mají občas problémy s aktuální obnovou signatur pro detekční nástroje. Moc toho nelze udělat ani pro zajištění bezpečnosti surfařů. Samozřejmě lze použít některý z exotických operačních systémů nebo prohlížečů, jako jsou Apple Mac OS nebo Safari či Opera. Podle většiny internetových statistik mají webové prohlížeče typu Opera a Safari (Mac) podíl na trhu do pěti procent. Při tak malém rozšíření to hackerům ani nestojí za pokus o jejich napadení.

Brána: Útoky přitahují především Windows XP a Internet Explorer. Podle firmy F-Secure jsou v současné době nejoblíbenější obětí hackerských útoků stále Windows XP (s podílem na trhu větším než 75 procent). Podle nejnovějších prognóz jsou však Windows Vista (se svým vzrůstajícím obratem – přibližně 12 procent) na nejlepší cestě vypracovat se na ještě významnější cíl útoků. V případě většiny uživatelů však bohužel platí, že jen málokdo si změní svůj vyzkoušený browser nebo odinstaluje oblíbený operační systém jen proto, že má problémy s bezpečností...

Čísla však hovoří jasně: Active X, komponenta Internet Exploreru, přiláká (ve srovnání s plug-iny) 89 procent hackerských útoků, ale jen pouhé jedno procento je namířeno na rozšíření Firefoxu. Změna browseru tedy bezpečnost surfování opravdu ovlivní...

Masová produkce: Viry jsou tvořeny snadno – za použití stavebnice

Den od dne se psaní virů stává jednodušším: profesionálové i laici používají stavebnicové systémy, jako je např. MPack, které jsou na pochybných fórech nabízeny přibližně za 1 000 dolarů. Především čínští hackeři vytvářejí stále více nových variant podobného malwaru. Je to rychlé, levné a s minimálním úsilím – něco jako „tovární" výroba.

Bezpečnostní agentury i firmy reagují na tuto záplavu virů jen s obtížemi: nově by měly bezpečnostní programy především identifikovat chování malwaru, analyzovat je, a teprve pak je zastavit. Takzvaná „Behaviour Control" dokáže identifikovat i nebezpečné nástroje, které nebyly a nejsou zahrnuty v databázi výrobců bezpečnosti.

HISTORIE VIRU

Termín „vir" poprvé použili v roce 1981 ve svém rozhovoru Dr. Fred Cohen a profesor Leonard M. Aleman.

John von Neumann rozvinul teorii „self-reproducing automates" a vybudoval teoretické základy pro všechny viry.

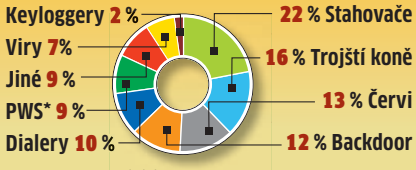
1949

Dokonce i námi oslovený bezpečnostní expert firmy Symantec je přesvědčen, že „většina virů bude odhalena prostřednictvím chování“. Tímto způsobem lze snadno odhalit na první pohled neškodnou techniku „Drive-by-Downloads“, která vždy dodržuje stejný vzor. Webová stránka nejdříve způsobí pád Internet Exploreru a poté nainstaluje downloader. Teprve ten nahraje škodlivá data z internetu. Toto chování lze zmiňovaným způsobem snadno odhalit a zastavit. Je tu jen jeden malý problém týkající se jednoduchého, téměř prastarého malwaru: vir musí něco učinit, např. vymazat několik souborů, abyste ho mohli detekovat na základě chování. To by ale mělo být ochráněno antivirovým programem.

Jak si tedy poradit se záplavou malwaru? Většina odborníků se shoduje v tom, že si s ní bez problémů poradí až bezpečnostní programy příští generace. Myšlenkou vývojářů je, že bezpečnostní programy by nejdříve měly spustit stažené soubory v tzv. sandboxu. V této zabezpečené oblasti bude prověřeno, zda soubory obsahují to, co slibují – či zda byly naprogramovány s cílem čmuchat nebo ničit.

Malware trendy

Trojští koně a stahovače nahrazují klasické viry.

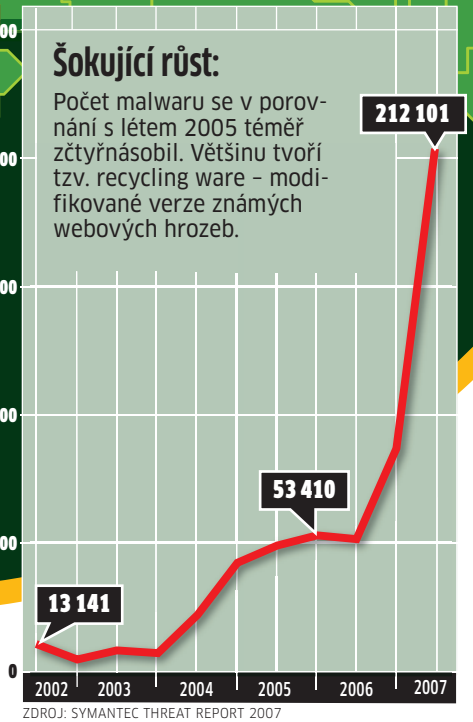


* PWS: MALWARE SLÍDÍCÍ PO HESLECH.
ZDROJ: IBM INTERNET SECURITY SYSTEMS 2006

29 % botnetů pochází z Číny

Šokující růst:

Počet malwaru se v porovnání s létem 2005 téměř zčtyřnásobil. Většinu tvoří tzv. recycling ware – modifikované verze známých webových hrozeb.



ZDROJ: SYMANTEC THREAT REPORT 2007

HLEDANÍ

Největší internetové podvody

Michael Buen
Filipínský student a autor viru „I love You“ .
Vir, který způsobil škodu kolem tří miliard eur a využil pro své rozmnožování Outlook.

David L. Smith
Americký programátor, autor červu Melissa.
Tento škůdce způsobil jen v samotných USA škodu více než 80 milionů dolarů.

Tarik Al-Daur
Příznivec hnutí Al-Káida, autor škůdce jménem Storm.
Tento student vyplenil okolo 37 000 kreditních karet a nakoupil zboží v ceně 2,4 milionu eur.

HLEDAČI

Nejlepší lovci virů

Eugene Kaspersky
Ředitel antivirového výzkumu v Kaspersky Lab
V roce 1997 založil Kaspersky Lab a je členem Computer Antivirus Researcher's Organization (CARO).

Candid Wüest
Bezpečnostní expert a výzkumník Symantecu
Lovec virů u firmy Symantec, testuje nové malwarové nástroje ve výzkumném centru.

Mikko H. Hyppönen
Vedoucí výzkumu u firmy F-Secure
Jeho tým vystopoval červy typu „Sobig.F“, varoval před „Sasserem“ a zastavil „Zotob“.

1983 Badatel Fred Cohen ve své práci „Počítačové viry – teorie a experiment“ jako první definoval základní funkce virů.

1986 Prostřednictvím programů „Brain“ rozšířil prodejce PC první MS-DOS-Virus.

1990 „Chameleon“ byl prvním polymorfním virem. S každou infikací se modifikoval a vzhledem k velikosti 9 Kb ho lze označit za nejmenší „stealth vir“...

2004 18letý student ze severního Německa vypustil na internet červa Sasser. Microsoft dokonce nabídl 250 000 eur za informace vedoucí k pachateli...

2005 „Sober“ byl masovým „mailer červem“, který se šířil pomocí vlastní „SMTP machine“ s falešnými adresami odesilatelů. Deaktivoval antivirové nástroje.