Software z šedé zóny

Vista, Office i Photoshop jsou na webu zadarmo. Zda jsou Crackz a Serial Numbers zakázány, to není úplně jasné. Jasné je však jedno: stránky nabízející takové downloady jsou nebezpečné.

Andreas Hentschel, autor@chip.cz

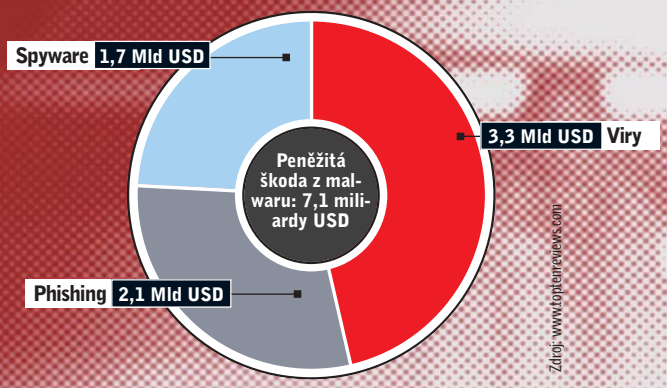
To, co jsme očekávali, přišlo po čtvrthodině. Abychom našli „kreknuté“ Nero 8, hledali jsme na seznamu warezu a serialz Astalavista, pomocí UnderSearch a New-Warez. Virový skener už zaregistroval přes 400 cookies a Firefox marně bojoval s několika „pop-upy“, když tu se při vyvolání GreatCracks náhle otevřelo okno, které alarmujícím tónem varovalo před spywarem a doporučovalo nainstalování nástroje „WinAntiVirus 2007 Pro“ – údajně antispywaru, který spolehlivě odstraní veškerý špionážní software. „Klikněte na OK!“.

WinAntiVirus 2007 Pro, to nevypadá nijak podezřele – kdo se ale ve věci vyzná, zaručeně nechá tlačítko OK bez povšimnutí. Jde totiž o tzv. „rogue antispyware“, tedy falešný antispyware, který místo aby počítač chránil, nainstaluje na něj celou armádu škodlivých programů. Podvodnický nástroj nejdříve varuje před trojským koněm zvaným „Trojan SPM/LX*“. Ten, kdo neví, že nic takového neexistuje, si nejspíš stáhne další doporučené komponenty WinAntiViru. Ty pak deaktivují virový skener, natáhnou další rozšíření, zobrazují reklamy, čenichají na pevném disku, hledají čísla kreditních karet, hesla a jiná důvěrná data. Kdo padne do této pasti, tomu může návštěva na stránce warezu přijít draho: při příštím výpisu ze svého bankovního konta by se také mohl podivit, že jeho kreditní karta byla využita až na doraz. Legální Nero 8 přitom přijde na necelých 2000 Kč.

Infekce už při otevření webové stránky

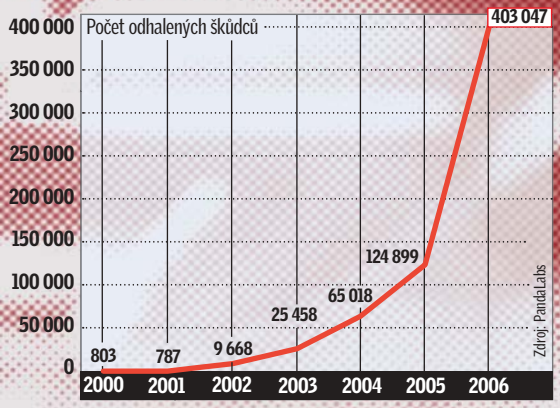
Jakkoli to zní paradoxně, program, který se nám webová stránka Great Cracks pokoušela vnutit, je stále ještě poměrně nevinný malware. Neustále se zdvořile ptá, zda se smí nainstalovat. A jelikož je starý už několik měsíců, dnes samozřejmě figuruje v seznamu virových signatur každého jen trochu slušného antivirového programu. Existují i podlejší způsoby: velké virové laboratoře v posledních měsících zaznamenaly neobvyklý nárůst webově orientovaného malwaru. Do této kategorie řadí bezpečnostní experti zavirované webové stránky, které bez vědomí a souhlasu uživatele instalují programy na pozadí. Cesty do počítače oběti jsou takřka nevypátratelné, jak také uvádí aktuální „White Paper“

Finanční ztráty způsobené malwarem



Soukromým domácnostem v USA způsobilo počítačové záškodnictví velké finanční ztráty. Srovnatelné údaje pro Českou republiku nejsou známy.

Rozšířenost škodlivých kódů



Počet celosvětově odhalených škodlivých programů (trojské koně, viry, spyware atd.) v loňském roce explozivně vzrostl.

bezpečnostní firmy Trend Micro: tzv. „web-threats" propašují škodlivý kód například využitím slabin v multimediálních souborech reprodukovaných přímo v browseru – jako je tomu u YouTube nebo u MySpace. Používají řídicí prvky ActiveX, vynucují si stahování domněle chybějících kodeků nebo programových komponent, využívají neopravené bezpečnostní mezery v prohlížečích nebo v jiných s webem svázaných programech (například QuickTime nebo Acrobat Reader) – a infikují počítač, v těch nejhorších případech už při pouhém navštívení webové stránky.

Nebezpečnější než pharming, phishing a spam

Jakmile je počítač jednou infikován, následují obvyklé scénáře: PC se stane součástí sítě „botů" a tím i šiřitelem spamu; hijacky v prohlížečích zavádějí na falešné webové stránky, spyware shromažďuje důvěrná data. Rainer Link, bezpečnostní expert firmy Trend Micro, sleduje mj. globální vývoj malwaru a ve web-threats spatřuje obrovské nebezpečí: „V seznamu největších rizik zaujímají podle našeho názoru třetí místo za viry a trojskými koňmi. Ohrožení z internetu považujeme za nebezpečnější než pharming, phishing nebo spam." A tento názor potvrzuje i konkurence: „E-maily jsou sice dosud nejoblíbenější cestou šíření škůdců," říká Markus Mertes, marketingový ředitel Panda Security, „ale bezpečnostní chování uživatelů se už změnilo a hrozbu ze spamu si stále více uvědomují. Internetoví podvodníci jsou proto odkázáni na nové způsoby šíření svých nástrah."

Nejlepší návnady: Filmy a software z Crackz

Jedna z cest, které pro šíření malwaru slibují největší úspěšnost, vede přes pirátské kopie – jsou totiž velmi žádané a pro každého snadno dostupné. S prvními kroky do světa warezu ochotně pomůže Google: po zadání vyhledávacích pojmů jako serialz, warez, moviez, crackz nebo downloadz vedou odkazy už na první nalezené stránce k odpovídajícím adresám. Kdo se tam ještě „prokliká" internetovými fóry, zaručeně přistane na tzv. DDL stránkách (Direct Download) nebo v torrentových seznamech. Odtud už jsou Vista, Photoshop i všechny další myslitelné programy vzdáleny jen na kliknutí myší – a se sériovými čísly ze stránek Serialz lze pak demoverze drahých programů uvolnit pro neomezené používání.

Jak často se software, filmy a hudba z internetu stahují, to nelze přesně říci. „Výměnné burzy a stránky s downloady nepatří mezi podniky kótované na burze," říkají odborníci z organizací zabývajících se sledováním porušování autorských práv. Odborníci však odhadují, že po webu se šíří daleko více ilegálních kopií než na konvenčních datových nosičích.

Šíření nelegálních kopií je starší než samotný komerční internet. Pirátské skupiny, které si s oblibou říkají „release groups", krekovaly už hry pro Commodore C64 – příslušné diskety se tehdy dodávaly na objednávku poštou. Takové skupiny zásobují svět programy, filmy a hudebními alby (viz schéma) i dnes, jenomže po internetu. Na celém světě nyní existuje asi stovka release groups, a svým způsobem představují téměř sympatický jev.

„Na spam už málokdo naletí. Podvodníci proto hledají nové cesty."

Markus Mertes, Panda Security

Crackeři v nich organizovaní považují svou činnost za jakýsi druh sportu. Při překonávání mechanismů na ochranu proti kopírování se poměřují s vývojovými pracovišti softwarových koncernů, při krekování her se sobě rovnými. Skupina, která dodá nejrychlejší a nejlepší cracky, se uvnitř této komunity těší největší vážnosti. Komerční zájmy jsou zde ovšem zapovězeny. Takzvaní „first seeder", kteří cracky z této scény umístí na výměnné burzy, upadají v opovržení. Ale z práce „počestných" i tak profitují ti nejhorší hackeři.

Každá desátá stránka infikována škodlivým kódem

Stahovat drahé programy, nové filmové trháky v kvalitě HD nebo americké televizní seriály, to už se pro mnohé stalo stejnou samo- →

Od originálu k hromadné kopii

Hrané filmy a softwarové tituly jsou díky přísně organizovaným gangům často k dostání na webu ještě před oficiálním uvedením na trh. Podvodníci využívají obliby warezu a příslušné stránky infikují škodlivými programy.

→ zřejmostí jako nákup v pekařství. Ale zatímco při nákupu rohlíků obezřetně přepočítáváme drobné, na webu se pohybujeme zcela bezstarostně. Ať se jedná o ruské servery, nebo o webové stránky ze souostroví Tonga, z Arménie či ze Samoy: při pátrání po atraktivních programech zadarmo se surfuje na cracks.ru, hledá se u Serialz.to nebo Cracks.am – tedy v těch nejpochybnějších zákoutích webu.

Přitom existují docela konkrétní varování před takovými webovými stránkami a na nich číhajícím nebezpečím. Například firma McAfee ve své na jaře uveřejněné studii vypočítala, jak velká je pravděpodobnost, že při návštěvě určitých stránek hrozí zavirování. Podle této studie jsou ruské servery infikovány s pravděpodobností 4,5 %, u stránek z Rumunska nebo Samoy je to 5,6, respektive 5,8 %. Největší nebezpečí hrozí v doméně nejvyšší úrovně „.tk". U webových stránek hostujících na pacifických ostrovech Tokelau představuje toto riziko dokonce 10,1 %. Pro hackery jsou tyto stránky skoro ideální: poplatky za hostování jsou v těchto zemích zanedbatelné, provozovatelé serverů právně téměř nepostižitelní – a zájem o obsahy takových stránek je obrovský. „Autoři malwaru si vždy dokážou najít médium, které je nejvíce používáno a nejméně chráněno," říká Rainer Link. Vývoj útoků založených na webu pak nastiňuje takto: „Kyberkriminální živly nejdříve naprogramovaly viry, které byly umístěny ve spustitelných souborech, potom makroviry schované v dokumentech, později pak e-mailové viry. Nyní tedy jako transportní médium zneužívají web."

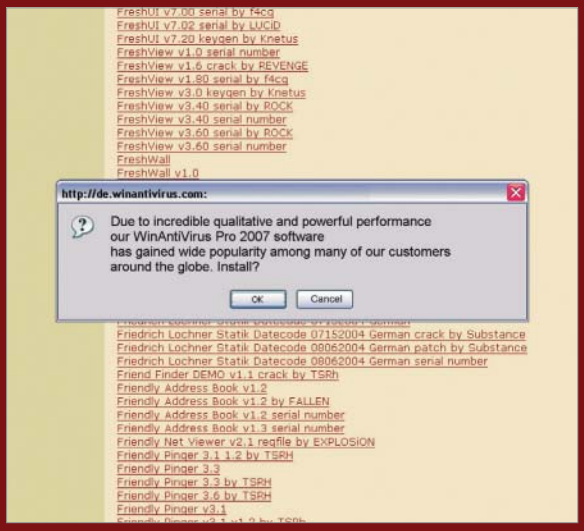
Kolik infikovaných stránek skutečně existuje, to lze jen těžko vyčíslit. Webová služba stopbadware.org uváděla uprostřed září ve svém rejstříku skoro 230 000 stránek, které se svým návštěvníkům pokusily podstrčit nějaký malware. Evidentně jich však bude mnohem více, vždyť v seznamu chybí například v úvodu zmíněný portál GreatCracks. Jinak celé spektrum sahá od portálů pro stahování spořičů obrazovek přes hackerská fóra až po warezové stránky či „serialz" sbírky s bezplatnými downloady a uvolňovacími kódy všech myslitelných programů.

K infikování webové stránky škodlivým kódem nemusejí hackeři vynaložit nijak zvlášť velkou námahu. K dispozici mají hotové stavebnice, které „exploity" vytvářejí samočinně a prostřednictvím iFrames je zapojí do zvolené webové stránky. Jedna z těchto stavebnic se jmenuje MPack a je mezi internetovými gaunery natolik oblíbená, že se její cena během jediného roku téměř zdvojnásobila. Taková stavebnice webové útoky do velké míry automatizuje a je natolik snadno ovladatelná, že s ní lze „zbastlit" napadení i bez programátorských znalostí. Funguje to takto: při vyvolání webové stránky hledá MPack prostřednictvím iFrame v surfařově browseru bezpečnostní mezery. Pokud nějaké najde, infikuje počítač individuálně přizpůsobenými exploity.

NEBEZPEČNÉ: **Kromě blikajících bannerů a odkazů čeká na návštěvníky warezových stránek především malware.**

Virová infekce na potkání

Stačí jediná návštěva na warezové stránce, a hned můžete „chytit" malware – zde falešný antispyware.



Malware je investice s dobrou návratností

Hackerská stavebnice přijde na 1000 amerických dolarů – za tuto cenu však kupující získá skvělý servis. Prodávající tak například zaručuje, že jeho nástroj nebude rozpoznán žádným virovým skenerem, při změnách ve virových signaturách obdrží zákazníci MPacku updaty, po nichž jsou exploity znovu dlouhodobě funkční. Tato aktualizační služba stojí navíc 150 USD ročně – může se však rychle zhodnotit. Tak například americký hacker Jeanson James Ancheta si se 400 000 PC v síti botů rozesílajících spam přišel na 60 000 dolarů. Ancheta byl však nakonec dopaden a nyní si odpykává 25 let za mřížemi.

„Autoři malwaru hledají způsob, jak k vám propašovat záškodníka."

Rainer Link, bezpečnostní specialista Trend Micro

Takové peníze si zřejmě nevydělá německý hacker, který nedávno vyděsil několik uživatelů lačných po neplacených downloadech. Ti se přihlásili u policie, poněvadž jim po návštěvě na torrentových a warezových stránkách naskočila na monitoru podivná zpráva: „Na vašem počítači byly zjištěny různé ilegálně stažené soubory." Pak následovala pohrůžka trestním oznámením a výzva k zakoupení Paysafecard za 50 eur. „Při odeslání 16místného kódu na konkrétní e-mailovou adresu security@safe-mail.net bude od trestního oznámení upuštěno." Tyto zprávy samozřejmě nepocházely od policie – byly to podvrhy. Mnohé „klienty" warezu však evidentně tížilo špatné svědomí a požadovaný obnos zaplatili. Měli štěstí v neštěstí: už po několika dnech byla částka zvýšena na 100 eur.

Andreas Henstschel