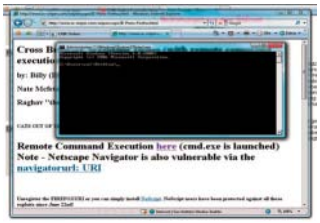
BROWSERY

Nebezpečná mezera ve Firefoxu a IE

Firefox je mnoha experty doporučován jako bezpečná alternativa k Internet Exploreru. Nyní se však ukázalo, že kdo si na svém počítači nainstaluje oba webové prohlížeče současně, prorazí tak do svého operačního systému obrovskou bezpečnostní díru.

Příčinou maléru je dosud téměř nepovšimnutá vlastnost Firefoxu: pokud URL začíná řetězcem „firefox://" namísto „http://"



ÚSPĚŠNÝ ÚTOK: Prostřednictvím zmanipulovaného odkazu aktivuje Internet Explorer za součinnosti Firefoxu režim příkazového řádku.

a takovýto odkaz je vyvolán z Internet Exploreru, potom Firefox otevře jakoukoli libovolnou adresu. Případný útočník tak může své oběti, která takový odkaz aktivuje, podstrčit jakýkoliv systémový příkaz.

Mozilla & Microsoft: Nikdo za to nemůže...

Odpovědnost za chybu necítí ani jedna z obou firem, a ani experti se nemohou v názoru sjednotit. Tomu, že zavinění je na straně Firefoxu, nasvědčuje inkriminovaná URL. Každopádně odpovídající položka v systémovém registru byla založena právě opensourcovým browserem. Svůj díl viny na celé mizérii má však také Internet Explorer: prohlížeč od Microsoftu aktivuje předloženou URL, aniž by ji předem překontroloval z hlediska výskytu zvláštních znaků. Za „firefoxovou" URL se totiž skrývá příkaz *firefox.exe -url „%1"*, přičemž proměnná *„%1"* je ta část, kterou lze ovlivnit.

Pokud tato část obsahuje uvozovku, dá se kromě parametru *-url* vložit do volání také parametr *-chrome*. A právě prostřednictvím rutiny Chrome ve Firefoxu získá útočník plný přístup do systému.

Ale ať už je na vině kdokoli, důsledky nakonec pocítí jen uživatel, který si nainstaloval oba prohlížeče. Rychlé východisko nenabízí ani Microsoft, ani Mozilla. Kdo tedy chce mezeru zacelit, musí si pomoci sám. Postačí k tomu dva jednoduché příkazové řádky:

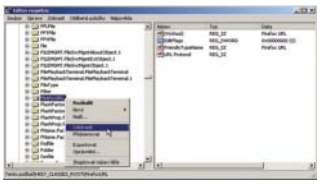
```
reg delete HKCR\FirefoxHTML /f
reg delete HKCR\FirefoxURL /f
```

Tyto příkazy vymažou ze systému (konkrétně ze sekce HKEY_CLASSES_ROOT v registrech) „firefoxovou" URL, která pak už nemůže být použita.

URL hacking: Web ohrožuje nová vlna útoků

Tomuto druhu útoků je však vystavena nejen kombinace Firefoxu a Internet Exploreru. Pouhé tři dny po zveřejnění mezery byl znám další nebezpečný pár: Internet Explorer a messenger Trillian, případně AIM. Podobně jako u Firefoxu se dá libovolný kód do počítače propašovat prostřednictvím AOL-URL.

Info: www.larholm.com



ŘEŠENÍ: Smazáním dvou položek v registrech odstraníte podstatu problému...

TRUSTPORT WORKSTATION ANTIVIRUS

Oceněný antivir

Společnost AEC, výrobce bezpečnostního softwaru řady TrustPort, oznámila získání dalšího ocenění. Její antivirový program TrustPort Workstation Antivirus se umístil na špici srpnového testu projektu AV-Comparatives a získal ocenění ADVANCED+.

Testu se zúčastnilo 17 světově známých antivirových produktů, které se utkaly v on-demand (na vyžádání) testu prověřujícím detekci škodlivých kódů, mezi kterými nechyběly makroviry, klasické Windows viry, malware, červi, trojské koně, backdoory a další. TrustPort Workstation Antivirus dokázal z předložených testovacích vzorků odhalit rekordních 99,64 % škodlivých kódů a dostal se tak v celém testu na špici. Ačkoliv je TrustPort Workstation Antivirus na antivirovém trhu relativně krátkou dobu, ukázal již své kvality, a to zejména díky inovačnímu přístupu společnosti AEC. Bezkonkurenční je použití čtyř skenovacích motorů, jejichž vzájemná kombinace zaručuje vynikající diagnostiku.

ZDROJ: AV-Comparatives

Dalšími antiviry, které také získaly ocenění ADVANCED+, jsou mimo jiné:

- AntiVirusKit (G DATA Security);
- AVG Anti-Malware (GriSoft);
- BitDefender Prof.+ (Softwin);
- F-Secure Anti-Virus (F-Secure);
- Kaspersky AV (Kaspersky Labs);
- NOD32 Anti-Virus (ESET);
- Norton Anti-Virus (Symantec).

TrustPort Workstation Antivirus je nabízen v rámci komplexního bezpečnostního balíku TrustPort Workstation, který kromě antiviru obsahuje i personální firewall, antispam, antispyware, aplikace pro šifrování a bezpečnou skartaci elektronických dat a elektronický podpis. Uživatelé ho mohou využívat i v řešení pro ochranu internetových bran před spamem, viry a spywarem (TrustPort Internet Gateway) a v řešení pro ochranu síťového prostředí organizace na úrovni souborových serverů (TrustPort Servers).

Projekt AV-Comparatives je výsledkem práce Andrease Clementiho, který se od roku 2004 zabývá srovnávacími testy antivirových programů, zejména z pohledu spolehlivosti detekce „In-the-Wild" virů. Více informací o uvedených testech najdete na **www.av-comparatives.org**.

WINDOWS VISTA

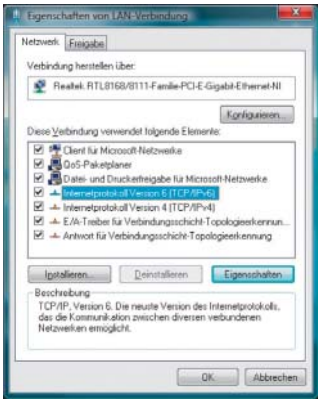
Závažná síťová chyba

Vista byla ještě v beta fázi, když už Symantec upozorňoval na možné bezpečnostní mezery v síťovém softwaru. Microsoft tehdy jeho připomínky ignoroval. Nyní však mají experti pro své domněnky i důkazy.

Problém spočívá v tom, že Vista už podporuje také nový protokol IPv6, s nímž má v budoucnu internet pracovat. Firmy, které IPv6 používají už dnes, to musí realizovat obvyklou metodou – nástavbou na IPv4. Tento postup, pokřtěný Toredo, však má své záludnosti: pokud není systém správně nakonfigurován, dá se prostřednictvím IPv6 adresy získat přístup přímo do počítače. Tomuto druhu útoku nezabrání dokonce ani firewally, poněvadž s novým protokolem většinou neumějí zacházet a prostě jej ignorují.

Bezpečnostní experti však očekávají ještě další problémy. Síťový software byl totiž pro Vistu kompletně přeprogramován. A „čerstvý kód", tím si je „Senior Director of the Symantec Security Response Team" Oliver Friedrichs jist, zpravidla obsahuje více chyb – což pro komplexní síťový systém platí především.

Info: www.symantec.com



WINDOWS VISTA: **Další bezpečnostní mezera...**

TREND MICRO

InterScan Web Security

Společnost Trend Micro Incorporated ohlásila nejnovější přírůstek do svého portfolia řešení, která chrání podnikové uživatele před webovými hrozbami. Trend Micro InterScan Web Security Appliance nabízí ochranu sítě typu all-in-one před příchozími útoky, jako jsou viry, spyware, nebezpečné webové stránky a nevhodný webový obsah.

Nástroj je nyní dostupný ve dvou verzích: InterScan Web Security Appliance Standard a InterScan Web Security Appliance Advanced. Druhá jmenovaná verze poskytuje uživatelům vedle funkcí standardní verze navíc plně integrované filtrování URL a zabezpečení appletů a prvků ActiveX založené na politikách. Obě verze obsahují zjišťování důvěryhodnosti webových stránek v reálném čase. Funkce hodnotí bezpečnost dané webové stránky podle jejího chování i obsahu. Tato vedoucí technologie pro zjišťování reputace stránek doplňuje výkonné skenování obsahu a filtrování URL, kterými produkt disponuje již několik let.

InterScan Web Security Appliance nabízí podnikům možnost jednoduché ochrany jejich webové brány typu „plug-and-protect". Příchozí a odchozí provoz je analyzován a nástroj tak funguje jako chybějící článek podnikového bezpečnostního řetězu. Webová konzola umožňuje administrátorům centrální management a maximální flexibilitu při definování přístupových práv pro delegovanou správu. Stejně jako u všech ostatních podnikových řešení Trend Micro může být více nástrojů InterScan Web Security Appliance centrálně řízeno pomocí Trend Micro Control Manageru. Tato centrální správa umožňuje administrátorům efektivně monitorovat a spravovat celé vícevrstvé bezpečnostní portfolio od firmy Trend Micro.

INVEX 2007

Antivirová konference

S blížícím se termínem dalšího ročníku podzimního veletrhu ITC Invex 2007 jsme zde opět s pozvánkou na tradiční Antivirovou konferenci, kterou naše vydavatelství pořádá ve spolupráci s předními společnostmi v oboru počítačové bezpečnosti a se společností BVV.

Na rozdíl od loňského roku, kdy jsme konferenci pořádali ve výškové budově BVV, místnosti 102, bude letos místem konání Antivirové konference prezentační sál pavilonu G2. Vzhledem k jeho umístění přímo v areálu výstaviště doufáme, že bude všem zájemcům o antivirovou problematiku z řad návštěvníků veletrhu mnohem dostupnější.

V rámci dopoledního programu, který začíná v 9.30 hodin, budou přednášet přední odborníci na antivirovou problematiku ze společností AEC, Eset, Grisoft a McAfee, v jednání jsme také se společností Alwil. Ve svých přednáškách se budou věnovat všem současným aspektům boje proti virům, proaktivní ochraně, heuristice, přehledu současných typů virů a úrovní jejich nebezpečnosti, budování nejlepší antivirové ochrany, novým metodám virových útoků a dalším tématům, která jsou v dnešním světě počítačové bezpečnosti aktuální.

Konference je plánována jako dopolední, její ukončení předpokládáme ve 13.30 hodin, ale záleží samozřejmě na intenzitě diskusí a množstvích vašich dotazů. Každopádně do svých diářů si nezapomeňte zapsat termín pátek 26. 10., 9.30 hodin, prezentační sál pavilonu G2 brněnského výstaviště. Jste srdečně zváni, konference je pro vás zdarma a pro každého účastníka bude opět připraven malý dárek. Těšíme se na vás!

Jiří Palyza

INVEX: **Jako obvykle IT událost roku...**

ZRANITELNÉ PROGRAMY

Nová bezpečnostní rizika

ADOBE

Postižený Flash

Využitím slabin ve Flash přehrávači mohou hackeři propašovat do počítače libovolný kód. Postiženy jsou všechny verze včetně 9.0.45. Stále aktuální jsou i mezery ve Photoshopu CS2/CS3. Řešením je aktualizace přehrávače pomocí updatů ze stránek Adobe.

Info: www.adobe.com

MICROSOFT

Hrozba s .NET-Framework

V červenci zveřejnil Microsoft záplaty pro jedenáct bezpečnostních mezer. Tři z nich se týkají rozhraní .NET-Framework a mohou být využity i prostřednictvím webové stránky. Další tři mezery postihly všechny varianty Excelu od verze 2000. Opravy jsou už k dispozici a jsou šířeny prostřednictvím správy aktualizací Windows.

Info: www.microsoft.com

QUICKTIME

Osm mezer

Cekem osm mezer v programu QuickTime 7.1 umožňuje útočníkům propašovat do cizího počítače škodlivý kód. V případě Windows už byly takové útoky mnohokrát pozorovány. Postižen je však i Mac OS X od verze 10.3.9. Naštěstí již Apple chybu odstranil a update je k dispozici ke stažení.

Info: www.apple.com

WEBOVÉ PROHLÍŽEČE

Spoofing hrozí všem

Firefox, Internet Explorer i Opera mají potíže s mezerami umožňujícími spoofing. Typickým scénářem útoku je například phishingová stránka, u níž prohlížeč zobrazuje legitimní URL bankovní webové stránky. Řešením je použití antiphishingového filtru, který nabízejí všechny zmiňované prohlížeče.

Info: www.mozilla.org

SUN JAVA RUNTIME ENVIRONMENT

Vzdálené spuštění příkazů

Společnost Sun oznámila zranitelnost ve svých produktech Sun JDK, JRE a SDK, která umožní vzdálenému útočníkovi převzít kompletní kontrolu nad cílovým systémem. Chyba se objevuje při tzv. parsování fontů, čehož může útočník zneužít a pomocí zákeřného appletu si může přidělit vyšší systémová práva nebo spustit lokální aplikaci přístupnou napadenému uživateli. Vzhledem k závažnosti chyby se doporučuje urychlený upgrade na verze minimálně JDK a JRE 5.0 Update 10 a SDK a JRE 1.4.2_15.

Info: zpravy.actine.cz

SYMANTEC

Spuštění zákeřného kódu

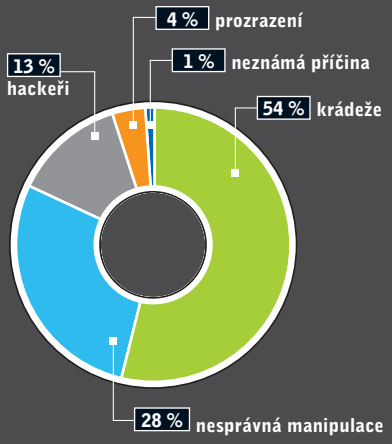
Několik zranitelností bylo identifikováno v produktech společnosti Symantec. Jedná se o produkty Norton Antivirus 2006, Norton Internet Security 2006, Norton Internet Security 2005, Anti Spyware 2005 a Norton System Works 2006. Jde o zranitelnost typu přetečení bufferu při zpracování ActiveX ovladačů. Tato chyba může v případě úspěšného zneužití vést k totální kompromitaci cílového stroje nebo k útoku typu Denial of Service. Více informací najdete na adrese http://securityresponse.symantec.com/avcenter/security/Content/2007.08.09.html. Doporučuje se urychlený upgrade přes LiveUpdate.

Info: zpravy.actine.cz

Barometr nebezpečí

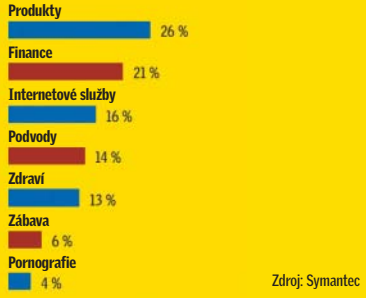
Web je ohrožován mnoha novými bezpečnostními mezerami – a mnohé jsou už využívány. Téměř každý výrobce musí své softwarové produkty opravovat.

Ztráty dat



Přes 50 % případů ztráty dat připadá na obyčejné krádeže.

Kategorie spamu



Méně porna: Pornografický spam momentálně představuje jen 4 % celkového objemu nežádoucí pošty.

ČÍSLO MĚSÍCE

100 000 USD

se na webu platí za „MPack", nástroj, který skrze bezpečnostní mezery propašuje do počítače škodlivé programy.

IBM X-FORCE

Stará hrozba neumírá!

Jak byste odpověděli, kdyby se vás někdo zeptal: „Za jak dlouho se červ Slammer přemění v opravdovou hrozbu?"

Slammer se poprvé objevil 24. ledna 2003 ráno, a již během prvních 10 minut svého šíření stihl napadnout 75 000 serverů běžících na systémech Microsoft SQL. Většina bezpečnostních specialistů si dodnes myslí, že je to červ, který „mohl a dělal". Kdy se z něj stala opravdová hrozba? O týden později? Nebo za měsíc?

Skutečně překvapující pro vás bude možná zpráva, že Slammer je stále nejběžnější hrozbou, se kterou se i dnes systémy řízené správou zabezpečení společnosti IBM ISS setkávají. Podle některých statistik je v současné době červem Slammer napadeno pravděpodobně o mnoho víc serverů, než tomu bylo v roce 2003, tedy v době, kdy si mnozí mysleli, že internet už má své dny „sečteny". Právě o tomto opakujícím se životním cyklu zranitelností píše ve svém blogu na adrese **http://blogs.iss.net/archive/OldThreatsNeverDie.html** Gunter Ollmann, ředitel bezpečnostních strategií IBM ISS.

Hlubší pohled do problematiky životního cyklu zranitelností a modelů dopadu opožděného odstraňování hrozeb získáte z nově publikovaného white-paperu, který popisuje, co to pro dnešní bezpečnostní technologie znamená a jak by měly společnosti rozvíjet své zabezpečení. White-paper najdete na adrese **www.iss.net/documents/whitepapers/old_threats_never_die_wp.pdf**.

BITDEFENDER 2008

Nové verze produktů

Společnost BitDefender, jejíž produkty na trzích České republiky a Slovenské republiky distribuuje Tech Data Distribution, oznámila uvedení produktu BitDefender 2008. Jde o novou řadu bezpečnostních řešení, poskytujících proaktivní zabezpečení před počítačovými viry, spywarem, hackery, spamem, phishingovými útoky a jinými běžnými bezpečnostními hrozbami z internetu. Produktová řada BitDefender 2008 zahrnuje systémy BitDefender Antivirus 2008, Internet Security 2008 a Total Security 2008.

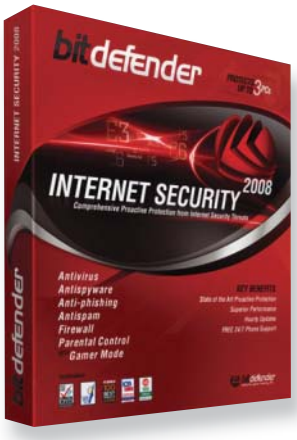
BitDefender Antivirus 2008 poskytuje uživatelům ochranu před viry, spywarem a ostatními typy malwaru a zahrnuje:

- *real-time ochranu před viry* – s automatickými hodinovými aktualizacemi;
- *proaktivní ochranu* – využíváním patentované vyhledávací technologie B-HAVE společnosti BitDefender;
- *antirootkitovou ochranu* – nalezením a odstraněním skrytých hrozeb;
- *ochranu soukromí* – snižováním rizika krádeže identity prostřednictvím úniku informací přes e-mail anebo web;
- *antispywarovou ochranu* – v reálném čase, monitorováním a prevencí spywaru.

Novinkou je zabudovaný „Gamer Mode" – kolekce ochranných nástrojů, které mají ochránit hráče při hraní on-line her.

BitDefender Internet Security 2008 je určen pro uživatele, kteří požadují komplexní ochranu před malwarem a jinými běžnými internetovými hrozbami. Internet Security zahrnuje všechny funkce produktu Antivirus 2008 a přidává:

- *firewall* – kontrolující „vstup na internet" a „skrývající" počítač před hackery;
- *e-mail antiphishing a antispam* – poskytující ochranu před různými druhy spamu a scamu;



- *rodičovskou ochranu* – pro blokování přístupu k nevhodným webovým stránkám a e-mailům;
- *časovač* – umožňující povolovat a zakazovat přístup k internetu ve specifických hodinách;
- *kontrolu aplikací* – umožňující uživatelům omezovat přístup k určeným aplikacím.

K dalším výhodám patří ochrana Wi-Fi, která upozorní uživatele na nedovolený vstup do Wi-Fi sítě.

BitDefender Total Security 2008 je zaměřen na uživatele, kteří vyžadují maximální ochranu před hrozbami z internetu a ochranu před ztrátou citlivých dat. Toto řešení současně obsahuje nástroje na udržování výkonnosti počítače uživatele. Total Security obsahuje všechny funkce již zmiňovaných produktů (Antivirus 2008 a Internet Security 2008), přičemž navíc nabízí:

- *data backup* – ochranu dat tvorbou zálohových kopií na lokálních discích anebo CD-R/RW a DVD-R/RW;
- *PC Tune-up* – zvyšování výkonu PC pomocí odstraňování nepotřebných souborů a zápisů do registrů;
- *mazání stop* – kompletně odstraní soubory a „stopy" na discích tak, aby se soubory už nedaly obnovit.

NEBEZPEČÍ Z INTERNETU

Excel a e-maily ze Zimbabwe

Společnost McAfee zveřejnila poznatky o novém trendu v oblasti nevyžádané pošty. Spammeři si v poslední době oblíbili přidávat k nevyžádané poště dokumenty ve formátu Microsoft Excel, které mohou například lákat k nákupu akcií. Tímto způsobem se odesilatelé nevyžádaných e-mailů snaží obejít antispamové filtry. Postup spammerů popisuje Nick Kelly, pracovník laboratoří McAfee Avert Labs, ve svém příspěvku zveřejněném na webu **www.avertlabs.com**. Nick Kelly zde vychází ze skutečného příkladu spamu, který propagoval německé akcie a byl rozeslán do domény .de a německým firmám používajícím doménu .com. Další odborník popisuje, co se stalo, když se pokusil odpovědět na podvodný e-mail. Zpráva měla být odeslána ze Zimbabwe a její odesilatel se vydával za syna místního farmáře, který byl zavražděn a zanechal po sobě 7,7 milionu dolarů. Dotyčný se je však v Zimbabwe bojí investovat a nabízí podíl z této částky, pokud někdo investuje tyto peníze ve své zemi (v tomto konkrétním případě ve Velké Británii) za něj. Celý vývoj korespondence včetně e-mailů podvodníků je k dispozici také na webu **www.avertlabs.com.**

JMÉNA CELEBRIT

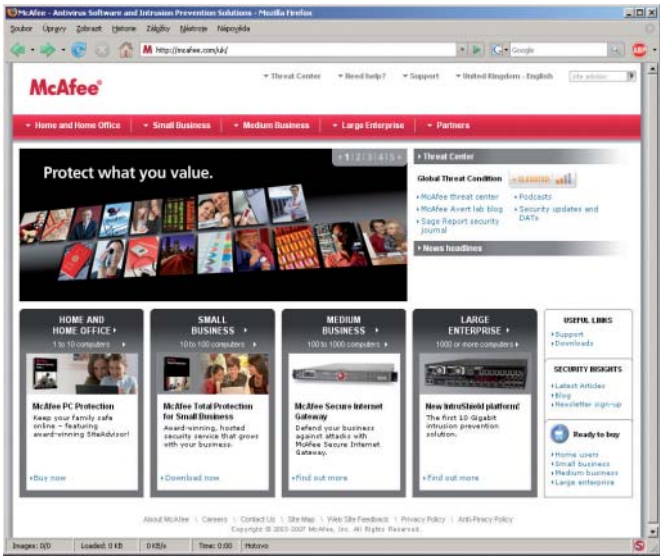
Nejnebezpečnější: Paris Hilton a Karel Gott

Klepy a informace týkající se celebrit jsou vděčným předmětem zájmu nejen bulvárního tisku. Řada z nás sleduje, co dělají naše oblíbené hudební či filmové hvězdy, jak se oblékají či s kým se scházejí. Za celebritami se nejen otáčejí lidé na ulici, ale zajímají se o ně také kybernetičtí zločinci. Jména celebrit využívají podvodníci k infikování PC spywarem, adwarem či spamem, nebo se dokonce tímto způsobem pokouší o krádeže identity.

Společnost McAfee, která nabízí řešení internetového zabezpečení, podnikla podrobný průzkum světa slavných osob, respektive té jeho podoby, jež existuje na internetu. Předmětem zájmu byla míra nebezpečí, která jednotlivé hvězdy provází. Nejnebezpečnější celebritou kybernetického světa se stala Paris Hilton. Podvodníci zneužívající její jméno se snaží přiživit na zájmu, který souvisí s jejím nedávným uvězněním. Jméno Paris Hilton je tak dnes spojeno s největším množstvím webových stránek, jejichž návštěva představuje pro uživatele riziko.

Žebříček deseti slavných osobností, které pro uživatele internetu představují největší nebezpečí, zahrnuje následující jména:

1/ Paris Hilton
2/ Amy Winehouse
3/ Cristiano Ronaldo
4/ Britney Spears
5/ Heidi Klum
6/ Pete Doherty, Valentino Rossi
7/ José Mourinho
8/ Madeleine Bernadotte (švédská princezna)
9/ Charlize Theron, Elisabetta Canalis a Nicolas Sarkozy
10/ Antonio Banderas



V České republice aktivity kybernetických podvodníků nejčastěji zneužívají jména zpěváků Karla Gotta a Heleny Vondráčkové.

Jedou z možností, jak minimalizovat podobná rizika, je použití aplikace McAfee SiteAdvisor, která barevně známkuje jednotlivé webové stránky podle jejich bezpečnosti. Tato aplikace chrání uživatele nejen před podvodníky zneužívajícími zájem o klepy ze života celebrit, ale ve všech ohledech zvyšuje bezpečnost při prohlížení webových stránek. Nástroj SiteAdvisor je zdarma k dispozici na webu **www.mcafee.com**, odkud si jej už stáhlo více než 50 milionů uživatelů.

500 000 SPAMOVÝCH ÚČTŮ

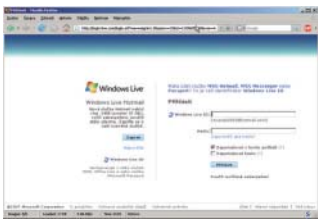
Trojský kůň pro Hotmail a G-mail

Společnost BitDefender oznámila, že díky společnému úsilí bezpečnostních týmů společností BitDefender a Yohoo byla kriminální činnost tvůrců trojského koně Trojan.Spammer.HotLan zastavena. Zmiňovaný trojský kůň využíval e-mailové účty Yahoo k rozesílání spamu, ale „nesložil zbraně". Jeho tvůrci přesunuli své aktivity na Hotmail a G-mail účty, zřejmě pomocí obejití CAPTCHA systémů obou poskytovatelů e-mailových účtů.

CAPTCHA systémy mají zajistit, že to budou pouze lidé, a ne počítače, kdo bude vytvářet e-mailové účty, aby se předešlo uvedenému zneužití e-mailových služeb. Každá aktivní kopie HotLan trojského koně se snaží vytvořit účet, přičemž vyšle CAPTCHA obraz v zašifrované podobě na spammerem kontrolovanou webovou stránku. Tam je tento obraz analyzován a výsledek je poslán zpět a následně vložen do příslušného pole. Poté tento trojský kůň stáhne zakódované spamové zprávy z další webové stránky, rozšifruje je a následně rozesílá na e-mailové adresy, které zase získal na jiné stránce.

„K pátku 3. 8. 2007 bylo evidováno 514 000 takovýchto Hotmail účtů a 49 000 podobných účtů na severech společnosti Google," komentoval současnou situaci ředitel antivirové laboratoře společnosti BitDefender Viorel Canja. *„Za zmínku však určitě stojí, že i když jsou tyto účty na serverech Googlu blokovány celkem rychle, obvykle po pár dnech od jejich vytvoření, většina spamových Hotmail účtů zůstává nadále funkčních."*

Společnost BitDefender tohoto trojského koně objevila jako první a dodala jeho signaturu, úspěšně identifikující všechny verze, které byly doposud vytvořeny. Analytici BitDefenderu zjistili, že tento trojský kůň není příliš rozšířen, což může naznačovat, že jeho tvůrci se nechtějí chovat nápadně.



HOTMAIL: Pod neustálou palbou hackerů...

SPOLUPRÁCE STAHUJ A ESET

Bojíte se virů?

V srpnu proběhl na **www.stahuj.cz** průzkum, který odpověděl na otázky, jak čeští uživatelé vnímají virové hrozby. Podle výsledků má na svém počítači antivirový program téměř 98 % uživatelů, ale přesto se více než tři čtvrtiny českých uživatelů obávají nákazy některé z počítačových infiltrací. Průzkum na vzorku čítajícím téměř čtyři tisíce respondentů se uskutečnil v rámci bezpečnostního projektu Stahuj.cz a společnosti ESET, výrobce antivirového řešení ESET NOD32.

Lidé prostřednictvím Stahuj.cz odpovídali na osm jednoduchých otázek týkajících se počítačové bezpečnosti. Přesně 97,6 % ze vzorku 3900 uživatelů odpovědělo, že na svém počítači má nainstalovaný antivirový program. Je zajímavé, že 19 % uživatelů používá pouze trial verzi, 48 % uživatelů chrání svůj počítač bezplatnou verzí, 13 % uživatelů si antivirový program koupilo, 11 % používá bezpečnostní aplikaci dodanou s počítačem a 6,6 % získalo antivir jinak.

Svůj antivirový program pravidelně aktualizuje většina lidí (95 %), 85 % z nich však tuto činnost nechává automaticky na používané aplikaci. Firewall se postupně stal důležitým prvkem ochrany počítače a podle průzkumu ho používá 83 % lidí. V drtivé většině se jedná o softwarové řešení. Obavu z napadení virem má 74 % uživatelů, a to i přesto, že svůj počítač chrání nějakým bezpečnostním řešením. Možná je to i z důvodu, že virovou infiltraci nějakého typu mělo na svém počítači 88 % účastníků průzkumu. Nejčastěji jsou počítače napadány prostřednictvím e-mailu a internetu. Zapomenout však nelze ani na fyzické šíření, a to například pomocí v poslední době oblíbených USB klíčů.