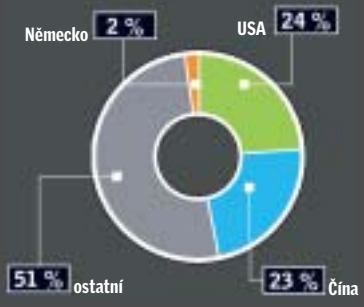
Barometr nebezpečí

Zejména ve vánočním čase sázeli mnozí spammeři na maily s blahopřáním. Ty bez otevírání rovnou odstraňujte.

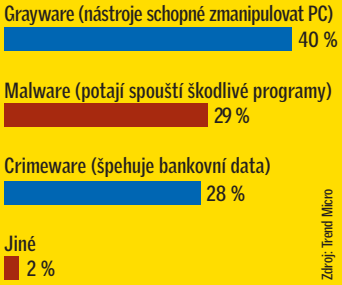
Původci phishingu



Zdroj: www.antiphishing.org

V pořadí hostitelů phishingu USA poprvé předstihly Čínu.

Ohrožení PC



Zdroj: Trend Micro

Tyto záškodnické programy už infikovaly přes polovinu všech počítačů.

BEZPEČNOSTNÍ WEB CHIPU

www.chip.cz

I na našem novém webu najdete zajímavé informace a tipy a triky z oblasti bezpečnosti.

Spam už i v podobě MP3 souboru

Zdá se, že někteří lidé si spam přímo oblíbili – přinejmenším ti, kteří si na www.spamfan.de předplatili reklamní maily. Kdo si například objedná balík Spam Pro, obdrží denně až sto spamových mailů navíc – a to ještě zdarma. Většina uživatelů však pochopitelně spam nenávidí a nasazuje proti němu filtry, které nežádoucí reklamní zprávy z normální komunikace elektronickou poštou vyřadí. Máme pro vás ale špatnou zprávu: takhle už to dlouho fungovat nebude.

Současnost: Zvukový soubor a obrazová zpráva

Doby, kdy spamové maily obsahovaly jenom prosté texty, jsou pryč. Aby šiřitelé reklamního balastu přelstili spamové filtry, používají stále zákeřnější metody.

Spam jako obraz: Aby současné spamové filtry poznaly, zda se u kontrolované zprávy jedná o reklamu, hledají v ní určité kombinace slov. Tomu se nyní autoři spamu často snaží zabránit tak, že reklamní text „nakreslí" jako obrázek. Spamový filtr pak pouze zjistí, že se jedná o JPEG soubor, jeho obsah však nedokáže analyzovat. Moderní skenery velkých bezpečnostních firem proto kromě blokování obrazových souborů sázejí také na OCR (Optical Character Recognition) – tak převedou grafický obsah na text a pak mohou spamové zprávy rozpoznat a odfiltrovat. Freewarové nástroje však tuto techniku dosud neimplementovaly.

Spam jako MP3: Výrobci antivirového softwaru nyní analyzují zcela novou variantu nežádoucích zpráv: spam v audiosouboru. K mailové zprávě – většinou bez textu a označení předmětu – je přiložen soubor ve formátu MP3. Obměňované názvy souborů jako „elvis.mp3" nebo „britney.mp3" mají zabránit identifikaci a přimět adresáta, aby si zvukový soubor poslechl. V 50 až 150 KB velkých souborech pak abstraktní ženský hlas anglicky propaguje akcie. Těmito nabídkami cenných papírů se spammeři pokoušejí vyhnat kurs akcií do výše, aby je pak mohli se ziskem prodat.

Budoucnost: Spammeři sázejí na nové formáty souborů

V roce 2008 očekávají analytici další nárůst spamu. Už nyní šiřitelé spamu využívají vedle zvukových a obrazových souborů také formáty jako PDF. V budoucnu už možná nebude existovat souborový formát, který by se nedal zneužít jako kontejner pro spam.

Info: www.cyber-ta.org

OBELSTĚN: Aby spamový filtr mailovou zprávu nezablokoval, používají útočníci namísto textu obrazové a zvukové soubory.

APPLE QUICKTIME 7.3

Záludnosti iTunes

Nainstalovali jste si všechny aktualizace Windows? Dobře jste udělali, neboť právě dírami v operačním systému se do počítače dostává většina útočníků. To se však může už brzy změnit. Vzhledem k rostoucí popularitě iPodů je dnes na mnoha PC nainstalován iTunes s QuickTime. A právě tento software si hackeři vybrali za cíl svých útoků. Přitom se v poslední době každých několik týdnů objevují aktualizace pro QuickTime, které napravují kritické mezery – v listopadu jich bylo hned šest.

U bezpečnostní „netěsnosti" stačí například zmanipulovaný videosoubor k získání přístupu do počítače. Je-li na PC nainstalována Java, mohou si útočníci v kombinaci s applety pro QuickTime, které tak jako tak nejsou považovány za důvěryhodné, přivlastnit více práv.

Také v části pro zpracování obrazů v QuickTime jsou chyby, které hackerům umožňují načítat data z PC.

Chcete-li si tedy napříště stále bezstarostně pouštět videa, měli byste si vždy nainstalovat nejnovější verzi iTunes.

Info: www.iTunes.com

Nová bezpečnostní rizika

WINDOWS XP

Bezpečnostní mezera v Macrovision Security Driveru, tj. v ovladači pro kopírovací ochranu CD Macrovision, umožňuje útočníkům spustit v počítači škodlivý kód. Postiženy jsou Microsoft Windows XP a Windows Server2003. Microsoft už usilovně pracuje na nápravě.
Info: **www.microsoft.com**

XPDF

Opensourcová čtečka PDF dokumentů Xpdf vykazuje chybu v renderovací rutině. Pomocí zmanipulovaného PDF souboru proto může útočník převzít kontrolu nad počítačem. Záplata je k dispozici na webové stránce výrobce. Je doporučeno software nejprve odinstalovat.
Info: **www.fotolabs.com**

MICROSOFT

Microsoft uvolnil na svém webu pravidelnou dávku záplat. Tentokrát se jedná o tři kritické chyby týkající se vzdáleného spuštění kódu na stanici, a to v aplikaci Internet explorer, mediálním formátu Windows Media File a v DirectX rozhraní. Dále pak uvolnil čtyři důležité záplaty pro SMBv2, MSMQ, Windows Kernel a opravu výše uvedeného problému s ovladačem Macrovision. Informace najdete na webu Microsoft TechNet.
Info: **zpravy.actinet.cz**

OPERA

Chyba při začleňování externích aplikací jako čteček zpravodajství vede u Opery k bezpečnostní mezeře, skrze kterou mohou hackeři proniknout do systému. Nejnovější verze 9.24 problém odstraňuje. Instalační soubor najdete na webové stránce.
Info: **www.opera.com**

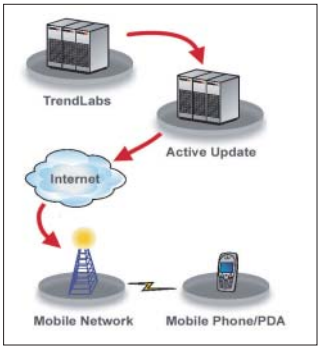
TREND MICRO SECURITY

Ochrana smartphonů Sony Ericsson

Společnost Trend Micro Incorporated oznámila, že software Trend Micro Mobile Security (TMMS) 3.0 je k dispozici i pro operační systém Symbian/UIQ 3.0, který je instalován v telefonech Sony Ericsson řady P1. Noví uživatelé těchto zařízení si mohou přímo stáhnout zkušební verzi TMMS 3.0 a vyzkoušet si ochranu před hackery, průniky a škodlivými kódy, stávajícími se stále větší hrozbou pro mobilní zařízení využívající nezabezpečené bezdrátové sítě. Toto řešení také chrání před úniky dat prostřednictvím firewallů a technologií pro zjišťování průniků.

Svým počtem mobilní zařízení rychle předstihují pécéčka. Jejich rychlost a výkonnost rostou a práce v terénu je s nimi mnohem pohodlnější. Zaměstnanci mohou díky nim přistupovat k firemním informacím prostřednictvím různých bezdrátových sítí, jako je Wi-Fi. Trend Micro Mobile Security 3.0 nabízí mobilním zařízením stejný typ ochrany, jaká je potřeba u pécéček – antivir, firewall a antispywarový program. Zároveň chrání důležitá pracovní data uložená na těchto zařízeních v případě ztráty nebo krádeže.

Trend Micro Mobile Security 3.0 je určen pro zařízení s operačním systémem Symbian OS 9.1/UIQ 3.0, použitým v modelech Sony Ericsson P1, W960 a M600. Trend Micro Mobile Security 3.0 pro Windows Mobile 5.0/6.0 je k dispozici od konce listopadu 2006, zatímco Trend Micro Mobile Security 3.0 pro Symbian/S60 3rd Edition se prodává od dubna 2007.



OCHRANA: Mobile Security ochrání váš telefon se symbianem...

Nová bezpečnostní rizika

APPLE QUICKTIME

V Apple QuickTime 7.x byly oznámeny zranitelnosti **(viz http://docs.info.apple.com/article.html?artnum=307176)**, které mohou být zneužity k poškození cizího systému. V první řadě se jedná o chybu ve zpracování zákeřně upravených QTL souborů, což může mít za následek Buffer overflow. Úspěšný útok umožňuje spuštění libovolného kódu. Další blíže nespecifikované chyby se vyskytly v QuickTime modulu pro Flash. Útočník přes něj může taktéž spustit libovolný kód. Poslední chyba se vyskytla ve zpracování hlaviček Real Time Streaming Protokolu, přičemž prohlížení zákeřně upraveného RTSP souboru může způsobit ukončení aplikace nebo spuštění kódu. Potřebné patche jsou obsaženy v updatu na verzi 7.3.1, který v závislosti na operačním systému naleznete na webu Apple Downloads (www.apple.com/support/downloads/).
Info: **zpravy.actinet.cz**

MP CLASSIC A MWMP

Media Player Classic je náchylný k přetečení paměti zásobníku, protože nedokáže zkontrolovat uživatelem zadaná data **(viz www.securityfocus.com/bid/26774/info)**. K úspěšnému provedení útoku je zapotřebí, aby uživatel spustil zákeřný MP4 soubor. Využití tohoto problému dovoluje útočníkovi spuštění libovolného kódu. Nevydařený exploit pravděpodobně vyústí v Denial-of-Service. Zasažena je verze MPC 6.4.9, u ostatních to není vyloučeno. Stejným problémem je zasažen i Microsoft Windows Media Player ve verzi 6.4 **(www.securityfocus.com/bid/26773/info)**. Prozatím nebylo ohlášeno žádné řešení.
Info: **zpravy.actinet.cz**

MAC OS X LEOPARD

V novém operačním systému Applu je firewall standardně deaktivován. Kdo jej zapne vlastnoručně, riskuje, že programy přestanou korektně fungovat. Apple ale o problému ví a pracuje na záplatě.
Info: **www.apple.com**

MICROSOFT WEB PROXY

Microsoft prošetřuje oznámení o zranitelnosti ve způsobu, jakým Windows nakládají s názvy stanic neobsahujícími plně kvalifikované doménové jméno FQDN **(viz www.microsoft.com/technet/security/advisory/945713.mspx)**. Technologie, kterou tato zranitelnost postihuje, je Web Proxy Auto-Discovery (WPAD). Technologie WPAD řeší jména stanic až po domény druhého řádu. Toho může být využito k provedení tzv. man-in-the-middle útoku, který umožní získat a pozměňovat zasílaná data vůči doménám třetího a nižšího řádu. Ve článku Microsoftu je uvedeno i několik způsobů, jak tento problém obejít, ačkoli se nejedná o plnohodnotná řešení.
Info: **zpravy.actinet.cz**

APPLE SAFARI A FIREFOX

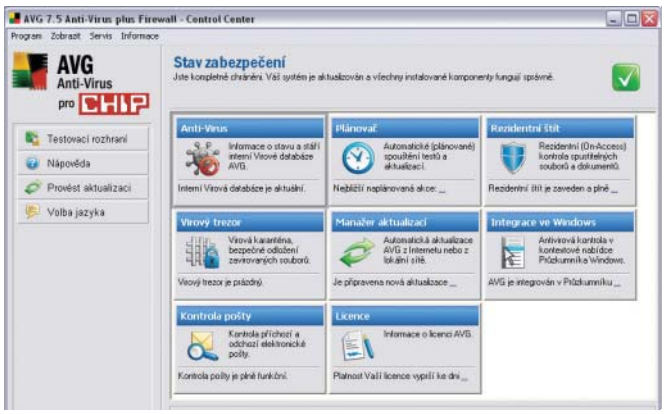
Apple Safari a Mozilla Firefox jsou náchylné k JavaScript key-filteringu, protože si nedokáží bezpečně poradit s psaným vstupem od uživatele – to tvrdí zpráva zveřejněná na serveru Security Focus **(www.securityfocus.com/bid/26669/info)**. Úspěšný útok vyžaduje, aby uživatel na klávesnici napsal potřebný řetězec a umožnil tak útočníkovi odeslat na vzdálený počítač různá data. Vzhledem k množství potřebného textu útočníci pravděpodobně použijí hry hojně využívající klávesnici, blogy nebo podobné weby lákající uživatele k napsání požadovaného vstupu. Aktualizace zatím nebyly vydány.
Info: **zpravy.actinet.cz**

APACHE HTTP SERVER

Apache má při vyřizování žádostí ústících v HTTP 413 chyby sklony podlehnout Cross-Site-scriptingu **(podrobnější informace najdete na www.securityfocus.com/archive/1/484410)**. Útočník může této skutečnosti využít ke krádeži přihlašovacích údajů uložených v cookies a spustit další útoky. Zranitelné jsou verze 2.0.46 – 2.2.4, zranitelnost dalších verzí není zatím potvrzena.
Info: **zpravy.actinet.cz**

STATISTIKA PODLE AVG

Žebříček hrozeb za rok 2007



S CHIPEM V BEZPEČÍ: Proti zmiňovaným hrozbám vás ochrání i námi nabízený bezpečnostní balík od AVG.

Bezpečnostní experti Grisoftu zveřejnili žebříček hlavních virových hrozeb a exploitů v roce 2007. Zároveň předpovídají rizika, kterým budou počítačoví uživatelé čelit v roce 2008. Podle výzkumného týmu představovaly viry pouze 15 % všech útoků vyskytujících se v roce 2007. V souladu s předpovědí z roku 2006 patřila většina hrozeb spíše do kategorie červů, trojských koní, keyloggerů nebo spywaru...

Top 10 Malware roku 2007

Larry Bridwell, globální bezpečnostní stratég Grisoftu, sestavil následující „hitparádu" malwaru za rok 2007:

1.	Win32/Virut
2.	I-Worm/Stration
3.	I-Worm/Nuwar
4.	Downloader.Tibs
5.	Downloader.Zlob
6.	BackDoor.Hupigon
7.	PSW.OnlineGames
8.	I-Worm/Netsky
9.	I-Worm/Mytob
10.	Worm/Feebs

„Antivirový průmysl v posledních dvou až třech letech prošel značným vývojem, stejně jako bezpečnostní hrozby, kterým musí čelit. Z obyčejného viru se vyvinul celý komplex rizik, zahrnující infikovanou webovou stránku kombinovanou s exploitem a sociálním webem, který důvěryhodného uživatele připraví o jeho data," řekl Bridwell. „Tváří v tvář novým typům nebezpečí budou uživatelé nuceni posílit svou antimalwarovou ochranu o nové nástroje, umožňující bezpečné surfování. Na rozdíl od klasického malwaru, jakým je trojský kůň nebo virus, které slouží spíše k vyvolání chaosu, jsou exploity rychle se rozvíjející hrozby z kategorie crimewaru. Využívají je skupiny zločinců, které se chtějí obohatit – například prodejem zcizených dat. Exploity se k uživatelům dostávají ve formě downloadů zneužívajících konkrétních zranitelností webových serverů, prohlížečů a často používaných aplikací."

„V roce 2007 začali počítačoví zločinci hojně využívat exploity a postupy sociálního inženýrství k výrazným ziskům prostřednictvím webu," dodává Karel Obluk, technický ředitel AVG. „Očekáváme, že se tito lidé budou snažit zužitkovat získané poznatky k mnohem větším útokům. K tomu jim bude sloužit širší škála malwarových nástrojů. Skutečnou hrozbu pak představuje fakt, že tyto útoky by mohly mít vliv na využívání vyhledávačů a elek-

tronického obchodu, ale i na oblibu sociálních sítí."

Top 10 Web Exploity roku 2007

Na základě výzkumu, získaného po akvizici Exploit Prevention Labs, identifikoval Grisoft následujících 10 největších a nejnebezpečnějších exploitů v roce 2007.

1. Super Bowl/Dolphins website download hack (únor)
2. Google AdWords přes škodlivé stránky (duben)
3. Google Bait & Switch keyword stránky exploit servery (červenec)
4. Bank of India website drive-by download hack (srpen)
5. Storm Trojan Fakes YouTube Links přes phishing a falešné kódy (srpen)
6. Gov Hacks vládní hackeři přes porno stránky, malware, a falešný anti-spyware (září)
7. Facebook Banner Ads sloužící na šíření adware-driven exploity (září)
8. Alicia Keys/MySpace Hack (listopad)
9. MLB & NH malware (listopad)
10. Monster.com (listopad)

„Od útoků na Facebook, oficiální stránku americké baseballové ligy, až po stránky zpěvačky Alicie Keys je jasné, že nebezpečí on-line hrozeb za poslední rok rapidně vzrůstá," uvedl Roger Thompson, šéf výzkumného týmu AVG. „V roce 2008 by se měli internetoví uživatelé připravit na sofistikovanější hrozby. Organizovaný zločin se bude zaměřovat na napadání sociálních sítí kvůli krádeži a zpeněžení dat. Sociální sítě jsou zranitelné především kvůli rozsáhlému sdílení informací a důvěřivosti uživatelů."

Hlavní bezpečnostní hrozby očekávané v roce 2008

Tým Rogera Thompsona identifikoval pět nejrizikovějších oblastí pro bezpečnost uživatelů internetu v následujícím roce.

- Webové exploity a útoky za pomoci sociálního inženýrství. „Viry budou i nadále představovat hrozbu, ale zejména nás čeká nárůst výskytu exploitů využívajících sociálního inženýrství a rozvoj Webu 2.0 v roce 2008," řekl Thompson.
- Storm Worm na vzestupu. „Storm tady zůstane," uvádí Thompson. „Registrujeme kousky Stormu rozprodaného mezi útočníky a očekáváme jeho šíření napříč mnohými platformami."
- E-mailové viry. Mnoho nových uživatelů zůstává neinformovaných o e-mailových hrozbách. Nadále otevírají přílohy od neznámých odesílatelů nebo klikají na nebezpečné odkazy.
- Webové exploity napadají důvěryhodné stránky. „Dnešní kyberzločinci se snaží sklízet lehce dosažitelné ovoce," uvedl Thompson. „Pokud infiltrují populární, do té doby důvěryhodnou stránku, ovoce sklízí ve velkém a velice brzy."
- Vzestup útoků na Windows Vista. Se stoupajícím počtem uživatelů se Windows Vista budou stávat lákavějším cílem pro útočníky.

Grisoft očekává, že tvůrci mezinárodního práva budou v roce 2008 věnovat kyberzločinu větší pozornost. Je však nepravděpodobné, že přísnější zákony útočníky zastraší. „Mezinárodní zákony o obchodování s drogami či zbraněmi příjmům nelegálních obchodníků nezabránily," upozornil Obluk. „Nemáme tedy důvod si myslet, že zákony namířené proti kybernetickým zločincům nějak zásadně ovlivní jejich výskyt. Zkrátka se tak dá jednoduše vydělat příliš mnoho peněz."

Nová bezpečnostní rizika

SYMANTEC BACKUP EXEC

Symantec Backup Exec for Windows Servers 11d obsahuje několik chyb, které dovolují vzdáleným útočníkům provést DoS útok **(viz http://securityresponse.symantec.com/avcenter/security/Content/2007.11.27.html)** . Chybu mohou útočníci vyvolat zaslání zákeřně upravených paketů. Podrobnosti a odkazy na aktualizace naleznete v původním oznámení výrobce.
Info: **zpravy.actinet.cz**

SUN SOLARIS

Sun Solaris verze 8, 9 a 10 obsahuje chybu v příkazu unzip verze 5.52 a starším, který může nastavit chybná práva u extrahovaných souborů. V době uzávěrky byl bohužel k dispozici zatím jen preliminary patch pro Solaris 9. Podrobnosti s řešením zranitelnosti naleznete v původním oznámení výrobce **http://sunsolve.sun.com/search/document.do?assetkey=1-26-103150-1.**
Info: **zpravy.actinet.cz**

MAC OS X LEOPARD

Objevila se zranitelnost v Apple Mac OS X 10.5.0 (Leopard), která může způsobit Denial of Service (DoS) VPN „démonu": VPN démon zamrzne, pokud na něj útočník pošle zákeřně upravený paket. Podrobnější informace o chybě najdete na serveru Secunia **(http://secunia.com/advisories/27938/)**. K dispozici už je i exploit spouštějící chybu **(http://milw0rm.com/exploits/4690)**. Ostatní verze Mac OS X mohou být touto chybou také zasaženy. Patch se zatím neobjevil, tudíž jediné nabízející se řešení je omezení síťového přístupu VPNd jen důvěryhodným klientům.
Info: **zpravy.actinet.cz**