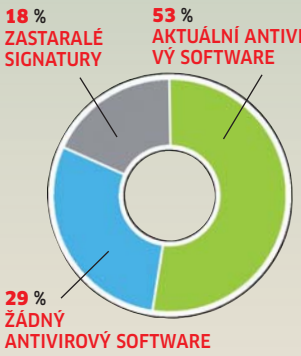
DATA A FAKTA

Barometr nebezpečí

Odborníci varují před maily s aprílovými žerty, které často roznášejí trojské koně. Zprávy od neznámých odesílatelů ihned odstraňujte.

Jste dobře chráněni?



ZDROJ: G DATA

Snadný cíl pro hackery: Téměř polovina dotázaných uživatelů surfuje na webu bez dostatečného zabezpečení.

Nejpodlejší viry

Systémy platebních karet	Trojan-Spy.Win32.Banker.ciy
Platební systémy	Trojan-PSW.Win32.VB.kq
On-line banking	Modifikation von Trojan-Spy
Trojské koně v e-mailech	Email-Worm.Win32.Netsky.q
Nejlépe ukrytý	Trojan-Downloader.Win32
Nejmenší	Trojan.DOS.DiskEraser.b
Největší	Trojan.Win32.KillFiles.mb
Nejničivější	Backdoor.Win32.Aebot.e
Nejrozšířenější	Trojan-Downloader.Win32

ZDROJ: KASPERSKY

Každý záškodník je „jedničkou“ ve své kategorii a většinou páchá ohromné finanční škody.

BEZPEČNOSTNÍ WEB CHIPU

www.chip.cz

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

Šifrování nepomůže!

NÁSTROJE PRO ZAŠIFROVÁNÍ pevného disku (jako například BITLOCKER) doposud platily za bezpečnou obranu proti hackerům. Nyní však výzkumný tým z USA dokazuje opak.

FABIAN VON KEUDELL

Neprolomí jej dokonce ani superpočítače: řeč je o 256bitovém klíči AES, jímž šifrovací nástroj Microsoftu, Bitlocker, zakódovává systémy Vista. Kdo se však domnívá, že Bitlocker je zcela bezpečný, bohužel se mýlí. Výzkumný tým univerzity v Princetonu vyvinul postup, kterým lze přečíst disky zašifrované nejen Bitlockerem, ale i podobným programem FileVault od Applu a opensourcovým nástrojem TrueCrypt. Podle všeho bude takto postižena také většina komerčních šifrovacích prostředků, které jsou dnes na trhu. K prorážení ochrany přitom výzkumníci ani nepotřebují zvlášť vysoký výpočetní výkon.

Jejich metoda se nepokouší o klasické dešifrování, ale namísto toho si přečte heslo přímo z operační paměti, kde je uloženo jako čistý text. Je-li počítač zablokován nebo je v úsporném režimu, pomůže trik: útočník připojí k PC přes USB port externí pevný disk a pak počítač restartuje. Přitom se počítač nabootuje z tohoto disku a spustí se program, který prohledá RAM. Je v tom však háček:

Hibernace: Aby paměťový blok udržel informaci i bez napájení, ochladí jej výzkumníci až na minus 50 °C.

obvykle se obsah operační paměti a s ním i heslo po vypnutí počítače vymaže. Ale nikoli ihned: obsah RAM zůstane zachován ještě po dobu tří až deseti sekund po přerušení napájení – to většinou stačí k restartu počítače bez ztráty obsahu RAM.

Pokud je počítač zabezpečen heslem pro BIOS, a tudíž nelze bootovat z externích médií, výzkumníci z něj prostě vyjmou paměťový blok. Pak už je ovšem deset sekund dosti krátká lhůta. V takovém případě pomůže ochlazení paměťového bloku pomocí běžně prodávaného spreje se stlačeným vzduchem, neboť při –50 °C se dají data načítat ještě asi deset minut. Při pokusném extrémním podchlazení tekutým dusíkem (–196 °C) zůstal obsah RAM zachován dokonce celých 60 minut.

Protiopatření: Vždy vypínat přívod proudu!

Jako uživatel se můžete bránit jen jedním způsobem: po skončení práce počítač vždy kompletně vypínejte. Pak se dočasná paměť automaticky vymaže. Nebezpečný je naproti tomu režim standby, tolik oblíbený u notebooků. Dobrou ochranu ovšem představuje režim spánku ve Windows, neboť při něm operační systém zapíše obsah RAM na pevný disk – a počítač vypne.

Pro výrobce šifrovacích prostředků pro pevné disky to znamená nový požadavek: hesla musí být v operační paměti zapsána v zašifrovaném tvaru, neboť teprve pak mají útočníci patřičně ztíženou úlohu – na dešifrování hesla by spotřebovali extrémně velký výpočetní výkon a neúnosně mnoho času.

INFO: www.princeton.edu

ESET SYSINSPECTOR

Rychlé zjištění stavu počítače

ESET na svých stránkách zpřístupnil zdarma ke stažení oficiální verzi nástroje ESET SysInspector, který nabízí podrobný přehled o spuštěných procesech operačního systému a slouží k odhalení nezvyklého chování aplikací, respektive celého systému, často způsobeného škodlivým kódem. Tento bezplatný diagnostický nástroj zvládne důkladně prozkoumat operační systém počítače a generuje podrobnou zprávu o jeho aktuálním technickém stavu. Pomáhá zjistit podezřelé systémové chování počítače, často způsobené počítačovou infiltrací. ESET SysInspector vytváří logy pro uživatele či technickou zákaznickou podporu, a tak napomáhá odhalovat problémy se systémem, které jsou mnohdy neviditelné (pracují na pozadí, skrytě zpomalují systém apod.).

Program obsahuje funkce pro zjištění informací o probíhajících programech a procesech komunikujících po síti, má integrovanou technologii Anti-Stealth zaměřenou na odhalování skrytých objektů – rootkitů a umožňuje porovnání dvou existujících logů, čímž zajišťuje vyhledání jakýchkoliv prvků, které nejsou společné pro oba srovnávané logy. Funkce Log compare je vhodná pro sledování změn systému, které mohou být způsobené nakažením počítače v čase mezi vytvořením obou záznamů. ESET SysInspector nevytváří v počítači žádné změny. Pokud uživatel potřebuje odstranit počítačové hrozby, může přímo z programu ESET SysInspector spustit bezplatný nástroj ESET Online Scanner (ten se stal vítězem našeho testu). ESET SysInspector je k dispozici ke stažení na stránce **www.eset.sk/eset-sysinspector-new** a je prozatím dostupný v anglické a slovenské jazykové verzi.

INFO

Nová bezpečnostní rizika

ICQ 6 BUILD 6043

Pomocí zmanipulovaných zpráv je možné komunikační program ICQ dovést ke zhroucení. Příčinou je chyba v programovém zpracování HTML. Ta umožňuje i propašování cizího kódu do počítače. Řešením je instalace aktuálního „build“ messengeru z webové stránky výrobce.
INFO: www.icq.com

SUN JAVA

V Java softwaru firmy Sun existují díry, jimiž se mohou dostat do vašeho počítače hackeři. Které komponenty přesně jsou postiženy, to Sun do redakční uzávěrky nesdělil.
Doporučujeme následující postup: nainstalujte si aktuální verzi Java Software 6 Update 5 a odinstalujte staré verze – to musíte udělat ručně.
INFO: www.sun.com

MICROSOFT ACCESS

Bezpečnostní mezera v „Jet Engine“ Accessu umožňuje v počítači zavedení a spuštění škodlivého kódu prostřednictvím souborů typu MDB. Bohužel, záplata dosud není k dispozici. Microsoft poukazuje na to, že Internet Explorer 7 a Outlook soubory MDB zásadně blokují.
INFO: www.microsoft.com

MCAFEE COMMON MANAGEMENT AGENT

Produkt McAfee Common Management Agent 3.6.0.574 a starší obsahuje zranitelnost ve FrameworkService.exe, která umožňuje případným útočníkům způsobit pád aplikace zasláním zákeřných požadavků na port 8081/TCP, na kterém CMA agent naslouchá. Na stránkách výrobce bylo zveřejněno dočasné řešení **(https://knowledge.mcafee.com/article/219/615324_f.SAL_Public.html)**, na hotfixu MacAfee pracuje.
INFO: zpravy.actinet.cz

MEDIAPLAYER

Viry z videa

Oblíbený bezplatný přehrávač médií VLC zanechává v počítači spustitelný škodlivý kód. Uvnitř reprodukce videostreamu v reálném čase nebo ve zmanipulovaném videosouboru mohou útočníci dopravit do počítače cizí kód a spustit jej. Využívají přitom chyby v protokolu RealTime Streaming Protocol (RTSP): VLC až dosud nekontroloval délku videostreamů, a mohlo proto docházet k přetečení bufferu. Tři další bezpečnostní mezery – v modulu titulků, v ovládací ploše programu a v demuxeru MP4 – rovněž otevíraly vstupní brány hackerům.

V aktuální verzi 0.8.6e už programátoři všechny mezery uzavřeli. Avšak dříve než si nový software nahrajete, měli byste ten starý kompletně ručně odinstalovat v Ovládacích panelech Windows.
INFO: www.videolan.org

SÍTĚ

Brána WLAN

Hackeři teď znají trik, jak přes rádiovou síť proniknout do cizího počítače: simulují router, k němuž se počítač připojuje, a tak získají přístup k jeho datům. Využívají přitom skutečnosti, že pokud jsou skryté WLAN sítě, které nevysílají žádné jméno sítě (SSID), uloženy v počítači jako oblíbené položky, počítač tyto sítě neustále hledá a přitom utajené jméno WLAN vysílá. Hacker pak do PC pošle zfalšovaný řídicí paket pro WLAN včetně přeneseného SSID. Tím dojde ke krátkodobému odpojení počítače od aktuální sítě a k jeho připojení k hackerovu routeru, který simuluje poznané jméno sítě.

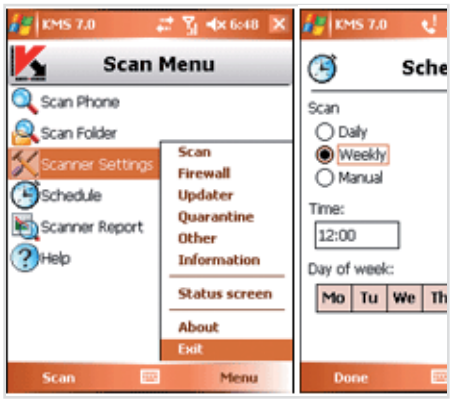
Chcete-li se před tímto druhem útoků chránit, nepoužívejte bezdrátové sítě, které pracují se skrytým SSID.
INFO: www.syss.de

KASPERSKY MOBILE SECURITY 7.0

Mobilní bezpečnost posedmé

Společnost PCS, dodavatel bezpečnostních technologií a oficiální distributor Kaspersky Lab pro ČR a SR, oznámil uvedení nové verze integrovaného řešení pro mobilní zařízení Kaspersky Mobile Security 7.0, poskytujícího ochranu před všemi typy mobilních hrozeb.

Kaspersky Mobile Security 7.0 chrání uživatele mobilních zařízení před síťovými útoky, malwarem či SMS spamem. Klíčovou novinkou nové verze je funkce úplného zablokování při ztrátě přístroje a možnost smazat data na dálku. Navíc v případě krádeže funkce SIM-Watch zabraňuje zloději v přístupu k datům v telefonu bez originální SIM karty. Jakmile je originální SIM karta nahrazena, přijde vlastníkovi telefonu upozornění na nové telefonní číslo.



Kaspersky Mobile Security: Mobilní bezpečnost začíná být stále palčivějším problémem...

Kaspersky Mobile Security 7.0 také skenuje příchozí soubory a síťová spojení v reálném čase a provádí antivirové skeny celého zařízení buď na vyžádání, nebo podle předem zadaného plánu. Chrání souborový systém před všemi objekty přicházejícími přes bezdrátová spojení (infraport, Bluetooth), před nebezpečnými MMS zprávami, během synchronizace s PC a stahování souborů přes prohlížeč. Dále zachycuje a skenuje soubory otevřené na mobilním zařízení a programy instalované z rozhraní zařízení. Kaspersky Mobile Security 7.0 také blokuje zprávy z nevyžádaných nebo neúplných čísel a rovněž SMS zprávy obsahující slova nebo spojení, jež jsou uživatelem zařazena na black list. Pravidelné aktualizace antivirové databáze zaručují, že Kaspersky Mobile Security 7.0 chrání před nejnovějšími škodlivými programy. Aktualizace jsou prováděny automaticky v intervalech nastavených uživatelem a jsou dostupné přes WAP/HTTP (GPRS, EDGE, Wi-Fi apod.) nebo během synchronizace s PC. Kaspersky Mobile Security 7.0 může být instalován na telefony s operačními systémy Windows Mobile 5.0, 6.0 a Symbian verze 9.x Series 60 3rd.

INFO

Nová bezpečnostní rizika

NERO MEDIAHOME

Streamovací server Nero MediaHome 3.3.3.0 obsažený v Neru 8.3.2.1 obsahuje chybu, která dovoluje vzdáleným útočníkům shodit aplikaci „NMMediaServer.exe“ zasláním upraveného požadavku na TCP port 54444. Další informace najdete na adrese **http://aluigi.altervista.org/adv/neromedia-adv.txt**. Oprava ještě nebyla vydána, řešením je prozatím používání aplikace v důvěryhodné síti.
INFO: zpravy.actinet.cz

OPRAVA CHYB V SAFARI

Společnost Apple oznámila chyby v prohlížeči Safari, které mohou vést k Cross Site Scripting, DoS a k případné kompromitaci postiženého systému. Více informací naleznete přímo v prohlášení společnosti Apple na **http://support.apple.com/kb/HT1467**. Současně s tímto oznámením vydala společnost Apple novou verzi svého prohlížeče, která tyto chyby opravuje. Chyby byly potvrzeny ve verzích Safari 3.x a Safari for Windows 3.x. Nová, opravená verze má označení 3.1.1.
INFO: zpravy.actinet.cz

ZRANITELNOSTI V OPENOFFICE

V kancelářském balíku OpenOffice byly objeveny zranitelnosti, jejichž zneužití může vést k potenciálnímu zkompromitování systému. Vícenásobné, blíže nespecifikované chyby byly objeveny v procesu zpracování souborů EMF, Quattro Pro, OLE a jejich zneužití může vyvolat přetečení zásobníku (heap-based buffer overflow). Další dvě chyby jsou ve zpracování textových dokumentů ODF obsahujících „speciálně upravený“ XForms. Při zneužití mohou poškodit paměťový zásobník. Úspěšné zneužití těchto chyb také může útočníkovi umožnit spuštění libovolně upraveného kódu. Chyby se vyskytují ve všech verzích, včetně 2.3. Řešením je update na verzi 2.4. Více informací najdete také na webu OpenOffice.org.
INFO: zpravy.actinet.cz

MOZILLA FIREFOX, THUNDERBIRD A SEAMONKEY

Byly oznámeny chyby v produktech Mozilla, které mohou být zneužity ke kompromitaci uživatelova systému spuštěním libovolného kódu (více informací na **www.mozilla.org/security/announce/2008/mfsa2008-20.html**). Zranitelnost je zavíněna chybou v Javascript Garbage Collectoru a může vést k poškození paměti přes určitý javascriptový kód. Chyba je opravena ve verzích Firefox 2.0.0.14, Thunderbird 2.0.0.14 a SeaMonkey 1.1.10
INFO: zpravy.actinet.cz

ANTIVIRUS JAKO SAMOSTATNÝ PRODUKT

TrustPort PC Security

Společnost TrustPort oznámila uvolnění svého antivirového programu jako samostatného produktu pod obchodním názvem TrustPort Antivirus a změnu názvu staničního řešení TrustPort Workstation na TrustPort PC Security. Doposud byl Antivirus nabízen pouze jako součást komplexního bezpečnostního balíku pro koncové stanice – TrustPort PC Security (dříve TrustPort Workstation). TrustPort Antivirus bude na českém a slovenském trhu nabízen podle stejného obchodního modelu jako TrustPort PC Security. To znamená, že koncoví uživatelé si jej budou moci zakoupit ve formě balíčků obsahujících 1, 3 nebo 5 licencí.

SERVICE PACK 3 PRO XP

Pro lepší Windows XP

Na počátku května uvolnil Microsoft pro systém Windows XP aktualizaci Service Pack 3 (SP3). Uživatelé si jej mohou stáhnout buďto prostřednictvím služby Windows Update, nebo z centra stažení softwaru společnosti Microsoft. Počátkem léta 2008 bude SP3 k dispozici také prostřednictvím služby automatických aktualizací systému Windows. Windows XP SP3 je kumulativní aktualizací systému Windows XP, která obsahuje všechny předchozí bezpečnostní aktualizace systému, opravy a vylepšení. Kromě toho přináší i některá nová vylepšení, jako je například technologie Network Access Protection, která je součástí systému Windows Server 2008 a je plně podporována systémem Windows Vista a nově také systémem Windows XP SP3.

Podrobnější informace a praktické testy SP3 vám nabídneme v příštím Chipu.

STATISTIKY MALWARU FIRMY ESET

V Česku řádí adware a spam

Stejně jako v předchozích měsících i v dubnu byla celosvětově nejrozšířenější hrozbou skupina infiltrací INF/Autorun. Vyplývá to z dubnových výsledků statistického systému ESET ThreatSense.Net, podle kterého tvořila uvedená infiltrace 7,75 % ze všech zachycených hrozeb. Počet nakažených počítačů touto infiltrací však klesá. V České republice se v dubnu INF/Autorun výrazněji neprosadil, a tak u nás i nadále vládne adware (škodlivý kód sloužící k zobrazování nevyžádané reklamy) a spam.

V dubnu byl poprvé zaznamenán průnik trojského koně Win32/PSW.OnLineGames (6,20 %) mezi elitu globálně nejrozšířenějších hrozeb. Tento trojský kůň sbírá nejrůznější informace (například přihlašovací údaje) související s počítačovými hrami. Kromě jiných informací totiž zaznamenává posloupnosti stisknutých kláves a ty pak odesílá na vzdálený server. Stejně tak používá techniky běžné pro rootkity, když zasahuje do činnosti některých bezpečnostních programů.

Adware z rodiny Virtumonde patří mezi nejrozšířenější hrozby již dlouhou dobu. Třetí místo v dubnu obsadil adware označovaný jako Win32/Adware.Virtumonde (3,58 %), následovaný svým příbuzným Win32/Adware.Virtumonde.FP (2,93 %) na místě čtvrtém. Adware Virtumonde je již delší dobu využíván jako prostředek k infiltraci počítačů a následnému řetězovitému zobrazování oken s nevyžádanou reklamou. Jednotlivé varianty tohoto adwaru jsou často modifikovány a upravovány tak, aby je prakticky nebylo možno odstranit z počítače bez poškození kriticky důležitých částí operačního systému. Otevírání „pop-up reklamních oken“ má za úkol i škodlivý kód na pátém místě dubnového žebříčku a další adware, konkrétně Win32/Adware.SearchAid (2,64 %).

Stejně jako v případě celosvětového žebříčku i hrozby v ČR mají svou stálici. Není jí však INF/Autorun, ale Win32/Adware.SearchAid (4,77 %). Uživatel si takovou potenciálně nechtěnou aplikaci nainstaluje většinou nevědomky jako součást licenčního ujednání jiného programu. Win32/Adware.SearchAid následně přesměruje internetový prohlížeč a nutí ho otevírat okna s nevyžádanou reklamou. Na druhém místě v dubnové statistice systému ESET ThreatSense.Net nalezneme trojského koně Win32/Ozdok (3,91 %). Ten se mediálně proslavil již na začátku tohoto roku pod jménem Mega-D botnet a má za úkol infiltrovat počítač a následně ho využít k hromadnému odesílání e-mailů, tedy ke spamování. Třetí místo pak obsadil již zmiňovaný Win32/Adware.Virtumonde (3,76 %). Infiltrace INF/Autorun (3,16 %) u nás zatím ještě pomalu roste (v březnu 2,95 %), přesto v „žebříčku malwaru“ kvůli nárůstu infiltrací výše zmiňovaného adwaru klesla ze třetího na čtvrté místo.

AVG ANTI-VIRUS FREE EDITION 8.0

Bezpečnostní novinka zdarma

Společnost AVG Technologies uvolňuje AVG Anti-Virus Free Edition 8.0. Tato bezplatná edice má omezeny některé funkce, nicméně poskytuje plnohodnotnou ochranu počítače před viry i spywarem, a to stejně jako u komerčních produktů díky zcela novému a přepracovanému jádru programu. AVG Free Edition 8.0 je určena pouze pro soukromé a nekomerční použití v jednom domácím počítači, bude k dispozici v anglickém, později i v japonském jazyce a firma pro ni nezajišťuje technickou podporu. Ke stažení je uživatelům k dispozici od 24. dubna 2008.

„Uvolněním bezplatné verze AVG 8.0, obsahující ochranu před viry i spywarem, chceme poskytnout možnost zabezpečení počítače skutečně všem uživatelům,“ uvedl Karel Obluk, technický ředitel společnosti AVG Technologies. „Kvůli stále intenzivnějším webovým útokům jsme navíc zařadili do free edice také funkci AVG Search-Shield, která bezpečně vyhodnotí v reálném čase všechny výsledky hledání na internetu a míru rizika nákazy signalizuje ikonou vedle jednotlivých odkazů,“ doplnil.

Funkce AVG Search-Shield pracuje s internetovými vyhledávači Google, Yahoo! a MSN. Je součástí unikátní technologie LinkScaner, kterou firma AVG Technologies zařadila do svého bezpečnostního systému po loňské akvizici americké firmy Exploit Prevention Labs. Ve srovnání s bezplatně poskytovanou verzí 7.5 obsahuje verze 8.0 vedle antiviru i antispyware a dále nabízí vylepšené detekční schopnosti, efektivnější heuristickou analýzu i možnost nastavit prioritu testu v jeho průběhu. Nechybí zde ani možnost eliminace potenciálně nežádoucích programů a tzv. cookies, což dříve obsahovaly pouze komerční verze systému AVG.

Software AVG patří podle renomovaného zpravodajského serveru CNet mezi dvacítku nejčastěji stahovaných programů všech dob. Jeho bezplatná verze AVG Anti-Virus Free Edition pokořila již několikrát hranici 1 000 000 stažení za jeden týden na prestižním serveru Download.com. Volnou edici AVG Anti-Virus 8.0 lze snadno stáhnout, instalovat i používat. Zjednodušenému ovládání napomáhá i nově zařazená komponenta AVG Security Toolbar. AVG 8.0 je kompatibilní s operačními systémy Windows Vista, Windows XP i Windows 2000. Vylepšenou verzi AVG 8 s firewallem a webovým štítem najdete zdarma na každém Chip DVD.

INFO: www.avg.cz

INFORMACE OD SPOLEČNOSTI TREND MICRO

Komplexní webová hrozba

Společnost Trend Micro zjistila, že už přes půl milionu webových stránek bylo napadeno novým webovým útokem. K útoku na stránky došlo pomocí úpravy SQL kódu a vložení javaskriptu, který přesměruje uživatele na dvě URL adresy se závadným obsahem. Přesměrování proběhne okamžitě a bez vědomí uživatele.

Některé z těchto přesměrování vedou na URL adresy, na jejichž webové stránce se zobrazí náhodně vygenerovaný obrázek. Jde o obvyklou akci používanou při zobrazování reklam. Stránka také využívá cookies ke zjištění doby, po kterou je obrázek zobrazen, a po určité době jej vymění za jiný. Kromě zobrazení obrázku však může být uživatel dále přesměrován na mnohem nebezpečnější cestu, během níž dojde ke stažení malwaru JS_DLOADER.AEHM a TROJ_REALPLAY.BR. Oba tyto kódy poté stáhnou do počítače trojského koně TROJ_AGENT.AKVP, který po zavedení do systému stáhne seznam dalších škodlivých stránek.

Mimo to může být do systému staženo mnoho dalších škodlivých souborů včetně JS_SENGLOT.C, HTML_DLOADR.CJ, JS_REPL.CB, JS_AGENT.ALIG, TROJ_AGENT.ALGQ a EXPL_EXECOD.A. Je zajímavé, že posledně jmenovaný malware je relativně starý a obsahuje kódy pokoušející se využívat různé zranitelnosti aplikací Yahoo! Jukebox a Lianzong Online Gaming Platform, užívaných převážně v Číně.

Mezi napadené stránky patří několik zdravotnických, výukových, vládních a zábavních sajtů po celém světě. Fakt, že webové stránky jsou umístěny v mnoha různých lokalitách včetně Indie, Velké Británie, Kanady, Francie a Číny, vyvolává dojem, byl použit automatizovaný nástroj vyhledávající zranitelnosti webových stránek.

Podle Jamze Yanezy, manažera programu Trend Micro pro průzkum hrozeb, „mohou být vícenásobné útoky, jako je tento, snáze neutralizovány následujícím prověřeným bezpečnostním návodem, kterého by se měli uživatelé držet při vytváření online prezentací. Primární příčinou takových útoků je často nedostatek skutečného bezpečnostního plánování. Při nasazování a provozu nejnovějších webových technologií je nezbytné, aby se postupovalo se znalostí bezpečnostních konsekvencí. Jen tehdy je možné zajistit ochranu značky a předejít ztrátě její reputace“. Autory tohoto útoku jsou stejní zločinci jako ti, kteří potvrdili autorství útoku nihaorr1.com, uskutečněného 29. dubna 2008.

Na ochranu postižených uživatelů vytvořila společnost Trend Micro nový nástroj Web Protection Add On. Nástroj si můžete stáhnout z adresy **http://us.trendmicro.com/us/products/enterprise/web-protection-add-on/.**

Uživatelé si také mohou prověřit svůj počítač pomocí bezplatné skenovací služby HouseCall, kterou Trend Micro nabízí on-line zdarma na adrese **http://housecall.trendmicro.com.**

Kontrola: Uživatelé si také mohou prověřit svůj počítač pomocí bezplatné skenovací služby HouseCall.

INFO

Nová bezpečnostní rizika

ZVÝŠENÍ OPRÁVNĚNÍ V MICROSOFT WINDOWS

Byla nalezena zranitelnost, která umožňuje spuštění libovolného kódu s oprávněními LocalSystem. Chyba se týká systémů Microsoft Windows XP s SP2, Vista a všech podporovaných serverových systémů. Zranitelnost je zaviněna chybou umožňující spuštění kódu v kontextu účtů NetworkService a LocalService a přístup k ostatním procesům běžícím pod stejným oprávněním, ale s možností navýšit svá oprávnění na LocalSystem. Bližší informace najdete na serveru Microsoft Technet **(www.microsoft.com/technet/security/advisory/951306.mspx)**.

INFO: zpravy.actinet.cz

ICQ A PERSONAL STATUS BUFFER OVERFLOW

V ICQ byla nalezena zranitelnost umožňující kompromitovat vzdálený systém **(viz www.infigo.hr/en/in_focus/advisories/INFIGO-2008-04-08)**. Zranitelnost je umožněna chybou ve zpracování tzv. osobního stavu. To může mít při zneužití za následek heap-based Buffer Overflow a následné spuštění libovolného kódu vytvořením určitého osobního stavu a například zasláním zprávy. Chyba byla oznámena v ICQ verzi 6 build 6043.

INFO: zpravy.actinet.cz

BUFFER OVERFLOW V PRODUKTECH ADOBE

Byla oznámena chyba v několika produktech společnosti Adobe, která může být zneužita ke kompromitování systému. Zranitelnost je zaviněna chybou ve zpracování BMP souborů, kvůli které tyto produkty nekontrolují závadnost hlaviček souborů před vykreslením souboru. To může při zneužití způsobit přetečení vyrovnávací paměti u BMP souborů s poškozenou hlavičkou a dovolit tak spuštění libovolného kódu. Více informací naleznete na **www.adobe.com/support/security/advisories/apsa08-04.html** ve vyjádření výrobce.

INFO: zpravy.actinet.cz

FOXIT READER

Prohlížeč PDF dokumentů Foxit Reader 2.2 obsahuje chybu ve zpracování XObject a ExtGState v PDF dokumentu, která může dovolit případnému útočníkovi kompromitovat uživatelův systém. Více informací naleznete v oznámení na stánkách **www.vallejo.cc/proyectos/foxitreader1.htm** a **www.vallejo.cc/proyectos/foxitreader2.htm**. Nejjednodušší ochranou je otevírat pouze dokumenty z důvěryhodných zdrojů.

INFO: zprávy.actinet.cz

YAHOO! ASSISTANT YNOTIFIER.DLL

V aplikaci Yahoo! Assistant byla nalezena zranitelnost, která může být zneužita ke zkompromitování uživatelova systému. Více informací naleznete na adrese **http://secway.org/advisory/AD20080506EN.txt**. Zranitelnost je zaviněna chybou v souboru yNotifier.dll (ActiveX ovladači) a může mít za následek spuštění libovolného kódu při návštěvě určitých webových stránek. Chyba je oznámena ve verzi 3.6, u ostatních verzí nejsou problémy potvrzeny.

INFO: zpravy.actinet.cz

APACHE HTTP SERVER

Oblíbený Apache HTTP server je náchylný k cross-site scriptingu, protože aplikace nedokáže dostatečně ošetřit uživatelem poskytnutý vstup. Podrobné informace najdete na webu Security Focus **(www.securityfocus.com/bid/29112/info)**. Útočník může tyto problémy zneužít ke spuštění libovolného skriptu v prohlížeči uživatele v kontextu postiženého webu. To může útočníkovi dovolit odcizit citlivé údaje založené na cookies a vést další útoky.

INFO: zpravy.actinet.cz

WI-FI

Nové produkty Netgear

Netgear vypouští na trh nové produkty založené na návrhu specifikace IEEE 802.11n Draft 2.0, certifikované Wi-Fi aliancí a využívající sadu několika vnitřních antén. Sada metamateriálových antén založená na patentované struktuře používá několik v těsné blízkosti umístěných antén, které směrují energii signálu na cílová bezdrátová zařízení, přičemž se vyhýbají každé vzájemné kolizi nebo překážkám rušícím signál. Umístění antén těsně vedle sebe umožňuje umístnit šest až osm vnitřních antén do kompaktního pouzdra a nabídnout lepší pokrytí, propustnost a stabilitu připojení.

Základním modelem je Netgear RangeMax Wireless-N WNDR3300. Ten poskytuje souběžnou podporu starším zařízením standardu 802.11g, klientům založeným na 2,4GHz nebo 5GHz technologii Wireless-N i novým počítačům s vestavěnou podporou jedno- a dvoupásmových bezdrátových zařízení standardu 802.11n verze 2.0.

Sada osmi metamateriálových antén spolu s podporou 5GHz Wireless-N technologie umožňuje dvoupásmovému směrovači WNDR3300 využít výhod až 23 nepřekrývajících se kanálů a vyhnout se tak rušení domácích spotřebičů, bezdrátových telefonů, Bluetooth zařízení i dalších Wi-Fi sítí ze sousedství.

Vrcholem nabídky je pak Netgear RangeMax Wireless-N WNR3500 (na obr.). Nabízí sadu osmi vnitřních antén pro snížení rušení rádiových frekvencí a maximalizaci bezdrátového výkonu a dosahu.

Komentář redakce: *Starší model WNR854T byl na trhu již déle než rok, přesto patřil ke špičce. Pokud WNR3500 naváže na úspěch svého předchůdce, pak bude velmi pravděpodobně nejrychlejším Wi-Fi routerem všech dob. Je však třeba počítat s odpovídající cenou: model WNR3500 stojí 4 290 Kč vč. DPH, model WNR3300 je o 1 000 Kč levnější.*

VERBATIM

Disky s černým designem

Společnost Verbatim uvádí na trh externí pevné disky. Nové disky v 3,5palcovém formátu nabízejí úložné kapacity 500 GB, 750 GB a 1 TB. Připojují se přes USB port, anebo jsou vybaveny kombinovaným USB/FireWire 400 rozhraním. Jejich celková hmotnost činí méně než jeden kilogram, konkrétně 961 gramů, což je polovina hmotnosti předchozí generace disků. Nově jsou vyvedeny v černém designu a mají nezvyklý čelní panel. Ani terabajtový model nevyžaduje speciální chlazení; disky jsou proto tiché. Stojí od 2 599 Kč do 4 589 Kč (doporučená maloobchodní cena) a jsou k dostání ve specializovaných prodejnách od dubna tohoto roku.

INFO: www.verbatim-europe.com

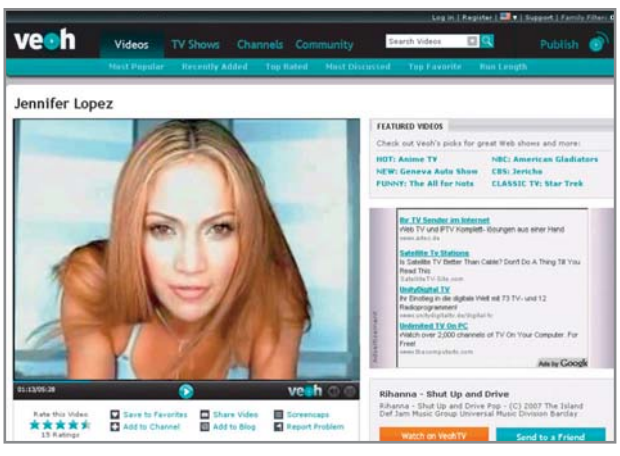
VEOH

Problém s následovníkem videoplatformy Stage6

DivX uzavřel svoji videoplatformu Stage6. Důvody pro tento krok byly strategické; pokud bychom měli věřit dohadům, náklady na provoz prudce vzrostly, protože díky své technologii přátelské k filmům Stage6 nalákal mnoho filmových pirátů: pro videa byly poskytnuty dva gigabajty datového prostoru, délka klipů zůstala neomezená, stejně jako jejich rozlišení. Stage6 byl podobný známému YouTube, s tím rozdílem, že nabízel možnost uložení a prohlížení videa ve FullHD kvalitě.

Webová stránka Stage6 mezitím odkazuje na svého exkonkurenta veoh, který rovněž hostuje libovolně dlouhá videa. Co je ovšem k zlosti: aby bylo možné prohlížet si klipy, které běží déle než 30 minut, musí se uživatel nalogovat a nainstalovat si veoh player – v éře webu 2.0 naprosto nepochopitelné.

INFO: www.divx.com



VISUAL RANK

Vyhledávání obrázků od Googlu

Výzkumníci Googlu zkouší novou technologii, pomocí níž bude moci vyhledávač zpracovávat a hodnotit jednotlivé obrázky podle jejich obsahu, podobně jako je tomu nyní u stránek HTML. Systém hodnocení je nazván podobně jako Page Rank u stránek HTML – Visual Rank. V současných vyhledávačích jsou obrázky nejčastěji vyhledávány podle textu, který je s nimi asociovaný. Navzdory dlouhodobému úsilí však zůstává mnoho nevyřešených problémů při vyhodnocování obrázků. Velký pokrok byl vykonán při automatické detekci tváře v obrázcích, ale najít a identifikovat další objekty, jako například hory, zůstává i nadále doménou lidí.

„Chceme sloučit všechny výzkumy této problematiky do jednoho a z výsledku vytvořit web framework," sdělil Shumeet Baluje, senior staff researcher Googlu.

Výzkumníci se zaměřili na 2 000 nejpopulárnějších produktů vyhledávaných přes Froogle, jako iPod, Xbox a Zune. Potom porovnali deset prvních obrázků, které byly získány běžným vyhledáváním a za pomoci nového algoritmu. Tým zaměstnanců Googlu poté vytvořil bodový systém na určení relevantnosti obrázků.

INFO: www.nytimes.com

NOKIA

N810 s WiMAX

Internetový tablet Nokia N810 bude od léta 2008 dostupný také ve variantě s WiMAX. Jako WLAN zařízení vysílá do vzdálenosti několika kilometrů. Přenosová rychlost N810 WiMAX má dosáhnout až 10 Mb/s, přístroj však bude nejprve dostupný jen v USA. Cena zůstává zatím otevřená.

INFO: www.nokia.cz

PŘEDPLACENÝ BALÍK

Nový model od Microsoftu

Microsoft bojuje s jedním ze svých největších konkurentů, společností Google, na všech možných frontách. Softwarový gigant připravuje pod kódovým jménem Albany nový model poskytování svých produktů a služeb. Koncovým uživatelům by na určitý čas pronajímal kancelářský balík Office 2007 v edici pro domácnosti a studenty, poskytoval bezpečnostní řešení Windows Live OneCare a další služby z rodin Office Live a Windows Live. Zatím probíhá uzavřené testování, ale Microsoft již existenci takového projektu potvrdil.

Projekt Albany by měl být pro koncové uživatele cenově lákavý. Řadoví uživatelé počítačů se zatím mohli ve větší míře setkat hlavně s předplatným na přístup například k aktualizacím antivirových programů nebo s předplatným on-line služeb.

INFO: www.microsoft.com

BENQ JOYBOOK

Multimediální notebook

Joybook S32B/S32EB je označení nových notebooků značky BenQ. Oba modely používají zvukovou technologii SRS TruSurround XT, mají vestavěnou webovou kamerku QEye 1,3 megapixelu a jasný širokoúhlý LCD displej s úhlopříčkou 13,3 palce a rozlišením WXGA. Víko s displejem je z hliníku a má metalickou úpravu vyvolávající představu vrstvy hvězdného prachu z hlubin galaxie. Joybook S32B je dodáván s nejnovější generací procesorů Intel Core 2 Duo, levnější model S32EB si pak vystačí s procesorem Intel Celeron M 540.

INFO: www.benq.cz

O2 [:KŮL:]

Tarif pro mladé

Od 1. května nabízí Telefónica O2 nový tarif se zajímavým názvem [:kůl:]. Nový tarif je určen pro zákazníky od 6 do 26 let. Za 250 Kč měsíčně získá zákazník 60 volných minut do všech sítí a neomezené množství poslaných SMS do sítě O2. Do ostatních sítí stojí SMS 1,50 Kč, minuta volání nad rámec paušálu přijde na 4,50 Kč za minutu, účtována je ale každá započatá minuta.

Komentář redakce: *Operátoři bojují o mladé zákazníky a používají k tomu právě SMS. Třeba Vodafone nabízí doplněk Student SMS Grátis, kdy můžete SMS posílat do všech sítí zdarma, ale zobrazí se vám reklama. Žádný tarif nabízený operátory není nejlepší, záleží na dalších preferencích. Bav se nabízí levné volání do sítě T-Mobilu, [:kůl:] nejlevnější volnou minutu, Vodafone zase SMS zdarma, resp. za reklamu, do všech sítí.*