DATA A FAKTA

Barometr nebezpečí v červenci

Útočníci stále častěji hledají oběti v sociálních sítích, aby tak své škůdce mezi členy co nejrychleji rozšířili.

Top 5: Útoky ze sítě

1. Čína	16,77 %
2. USA	14,33 %
3. Tchaj-wan	11,82 %
4. Venezuela	8,89 %
5. Argentina	5,65 %

Zdroj: Akamai

Téměř celá třetina všech internetových útoků přichází z Číny a USA.

Rizika stahování

Doména/země	Zkratka	Nejisté
Informace	.info	21,95 %
Rumunsko	.ro	14,18 %
Samoa	.ws	12,50 %
Byznys	.biz	11,64 %
Čína	.cn	10,75 %
Itálie	.it	10,62 %
Soukromé adresy	.<name>	10,32 %
Bulharsko	.bg	8,60 %
Belgie	.be	7,83 %
Kokosové ostrovy	.cc	7,64 %

Zdroj: McAfee

Domény nejvyšší úrovně, na nichž číhá většina infikovaného softwaru.

Patentová past z Redmondu

Microsoft chce být vynálezcem **PROAKTIVNÍ** antivirové ochrany. Bude teď uživatel muset za důležité antivirové programy platit ještě víc?

MANUEL SCHREIBER

Microsoft proniká na antivirový trh. Už v roce 2004 přihlásil patent, který popisuje nasazení proaktivní ochrany. Jeho zpracování trvalo americkému patentovému úřadu čtyři roky. Nyní už je to však oficiální zpráva: Microsoft má v rukou příslušné osvědčení. Tento ochranný mechanismus je založen na myšlence rozpoznat viry a trojské koně ještě dříve, než jsou k dispozici přesné definice škůdců. Podle představ Microsoftu má být každý program před instalací spuštěn v simulovaném prostředí, jeho chování protokolováno a vyhodnoceno. Nechová-li se standardně, tj. například se pokouší přistupovat k systémovým souborům, bezpečnostní software jej označí za rizikový a uživatele varuje.

Jistě dobrá idea, bohužel však nikoli nová, neboť zatímco Microsoft může jen poukazovat na svůj patent, všichni velcí antiviroví výrobci, jako Symantec, F-Secure, Kaspersky a Panda, už metodu založenou na chování sledovaného softwaru nabízejí ve svých programech. Vyvstává ovšem otázka, zda teď výrobci, kteří proaktivní ochranu aplikují, budou muset platit Microsoftu licenční poplatky – které nakonec stejně ponese uživatel. Jinak zbývají už jen dvě možnosti: od detekce založené na chování programů upustit, nebo najít nový způsob.

Žádný odpor ze strany výrobců antivirů se ale zatím neprojevuje. Není totiž ještě jasné, co se za patentem skrývá – a jak z něj chce Microsoft těžit. Axel Diekmann, generální ředitel Kaspersky Lab, sleduje situaci v poklidu: „Naše právní a patentové oddělení se tímto patentem samozřejmě důkladně zabývá. Bez kvalifikovaných informací o přesném znění patentu nevíme, zda se nás skutečně týká. Název ‚proaktivní ochrana' ještě nijak neprozrazuje, jaká technologie se za ním skrývá."

Analýza chování: Proaktivním postupem odhalí antivirové nástroje i neznámé viry a červy, pro které dosud neexistuje žádný popis.

Spor o vynález: Microsoft by poplatky vymáhat neměl

Na vážnou konfrontaci s Microsoftem Diekmann nevěří. „Eugene Kaspersky platí za jednoho z vynálezců heuristického postupu, který je jednou ze základních metod proaktivní ochrany." Kromě toho Kaspersky „sám patentoval celou řadu technologií".

A právě tady je další háček. Pokud by Microsoft chtěl vůči antivirovým výrobcům uplatňovat patentové nároky, musel by vědět, jak jejich ochranné mechanismy fungují – výrobci si ale určitě nenechají do svých programových kódů jen tak beze všeho nahlížet.

INFO: http://patft.uspto.gov

FLASH PLAYER A WINDOWS XP

Zpátečnický Service Pack

Microsoft maří úsilí Adobe: Flash Player ve verzi 9.0.115.0 umožňuje útočníkům propašovat do Windows škodlivý kód – stačí k tomu, aby uživatel otevřel stránku s aktivovanou flashovou animací. Podle Symantecu se to týká více než 20 000 webových stránek. Již začátkem dubna proto firma Adobe uveřejnila bezpečnostní záplatu: ve verzi 9.0.124.0 by už nemělo být možné počítače s Windows tímto způsobem napadnout. Zesílená bezpečnostní opatření však také způsobila, že některé flashové soubory přestaly fungovat.

I po aktualizaci však nebezpečí trvá: XP Service Pack 3 totiž do systému automaticky zavede zastaralou verzi. Ačkoliv Adobe zacelil bezpečnostní mezeru ještě před dnem uvolnění servisního balíku, Microsoft nestačil zareagovat a ohroženou verzi v SP3 ponechal. Nyní však „šli v Redmondu do sebe" a nabízejí záplatu. Uživatelé Flash Playeru by proto bezpodmínečně měli svůj software aktualizovat a verzi svého flashového přehrávače zkontrolovat. Číslo 9.0.115.0 nabízí hackerům vstupní bránu do počítače.

Bezpečné číslo: Pouze tato verze Flash Playeru je opravena. SP3 pro Windows XP instaluje starší verzi.

INFO: www.microsoft.com

INFO

Nová bezpečnostní rizika

KASPERSKY ANTI-VIRUS:

Chyba v ovladači firmy Kaspersky umožňuje přetečení bufferu, které mohou útočníci využít ke změně systémových práv Windows a propašovat do počítače záškodnické programy. Chybou jsou mezi jinými postiženy Kaspersky Anti-Virus a Internet Security ve verzích 6.0 und 7.0. Mezeru naštěstí odstraní aktualizace.
INFO: www.kaspersky.com

VLC MEDIAPLAYER:

Kritické chyby ve vlastních knihovnách a v Mozilla a ActiveX plug-inech pro VLC Mediaplayer umožňují útočníkům zanést do počítače škodlivé programy. Vývojáři však už na problém zareagovali aktualizací s číslem 0.8.6h.
INFO: www.videolan.org

SKYPE:

Filtr integrovaný ve Skypu, který má zabránit vyvolání spustitelných souborů, je chybný. Aby však hackeři mohli tuto mezeru využít, musí se v počítači předem nacházet kompromitovaná data. Řešením je upgrade, protože Skype bezpečnostní mezeru odstranil v aktuální verzi 3.8.0.139.
INFO: www.skype.com

TREND MICRO OFFICESCAN

Trend Micro OfficeScan verze 7.3 a starší obsahuje chyby v ActiveX knihovnách. Exploit a Workaround naleznete v oznámení na adrese **http://lists.grok.org.uk/pipermail/full-disclosure/2008-July/063524.html**.
INFO: zpravy.actinet.cz

AVG ANTI-VIRUS

V antiviru AVG byla nalezena zranitelnost, která při zpracování komprimovaných UPX souborů umožňuje pád skenovací jednotky. Chyba je opravena ve verzi 8.0.156. Více informací naleznete na webu www.nruns.com.
INFO: zpravy.actinet.cz

REAL NETWORKS REAL PLAYER

Secunia objevila zranitelnost v programu RealPlayer, která může být zneužita ke kompromitaci systému **(viz http://secunia.com/secunia_research/2007-93/advisory/)**. Zranitelnost je zaviněna chybou při zpracování snímků v Shockwave Flash (SWF) souborech. Úspěšné zneužití může dovolit útočníkovi spuštění libovolného kódu. Zranitelnost je potvrzena ve verzi 10.5 a bude opravena v následující verzi.
INFO: zpravy.actinet.cz

YOUTUBE BLOG

Ve službě YouTube Blog bylo nalezeno několik zranitelností, které mohou umožňovat vedení Cross-site scripting a SQL injection útoků. Zranitelnosti jsou potvrzeny ve verzi 0,1. Další verze mohou být také zasaženy. Vzhledem k rozsáhlosti problému naleznete další informace na serveru Secunia **(http://secunia.com/advisories/31161/)**.
INFO: zpravy.actinet.cz

EVOLUTION

Díra v Linuxu

Linuxový e-mailový klient Evolution je děravý. Ve standardním programu Gnome zejí dvě bezpečnostní mezery, které vedou k přetečení bufferu vyvolanému přílohami typu iCalender. Je-li deaktivován plug-in itip-Formatter, mohou hackeři využít mezer na počítačích ke spuštění libovolného kódu. Žádná aktualizace dosud není na webové stránce výrobce k dispozici. Pro některé linuxové systémy však už příslušné komunity dávají k dispozici balíky, které chybu odstraňují.
INFO: www.secunia.com

PHISHING

Vaše „smlouva“

Nebezpečí phishingových mailů je už dnes dostatečně známo. Proto útočníci používají stále rafinovanější metody. V současnosti rozesílané virové maily se maskují například jako smlouva a v předmětu zprávy obsahují v různých jazycích klíčová slova jako „nájemní smlouva“. V příloze se pak nachází archiv »smlouva.rar«, v němž se skrývá »smlouva.exe« včetně trojského koně. Na rozdíl od většiny phishingových pokusů bývají tyto maily v dané řeči jazykově vytříbené. K nám však tato „vymoženost“ ještě nedorazila – zdá se, že ostuda s phishingovými zprávami od „ČS“ (Drahoušek zákazník) útočníky odradila…
INFO: www.avira.com

SYMBIAN

Mobily s mezerou

Operační systém pro chytré mobilní telefony Symbian S60 není dobře zabezpečen. Podle firmy F-Secure se v něm dají pomocí zmanipulovaných nástrojů zavést do telefonu záškodnické programy. Na rozdíl od většiny útoků zde hackeři do mobilu nenahrávají programy prostřednictvím externích přístrojů, ale nabízejí je ke stažení. Útočníci k tomu využívají software ve formátu SISX. Jakmile jsou škodlivé kódy jednou nainstalovány, obcházejí bezpečnostní omezení, provádějí změny v systému a špehují data.
INFO: www.f-secure.com

ZPRÁVA SPOLEČNOSTI TREND MICRO

Kyberzločinci mění metody útoků

Propracované techniky sociálního inženýrství, pokročilé malwarové technologie a důmyslně propojené hrozby dále posilují už tak značně rostoucí podzemní kyberzločineckou ekonomiku.

Společnost Trend Micro vydala pravidelnou zprávu „Trend Micro Threat Roundup and Forecast 1H 2008“. Uvádí v ní, že kyberzločinci nejenže využívají k šíření kyberzločinu nové technologie, ale také vytvářejí stále nové formy sociálního inženýrství, jimiž se snaží přelstít jak spotřebitele, tak podniky. Výsledkem je, že za posledních šest měsíců vzrostl počet webových hrozeb a zároveň stále klesal objem adwaru a spywaru vytvářeného zastaralými technickými metodami, které již nemohou bojovat se špičkovými bezpečnostními řešeními.

Novinky sociálního inženýrství a phishingu

Taktiky sociálního inženýrství jako „nigerijské dopisy“ nebo „španělští vězni“ se zneužívají už desítky let. V současnosti kyberzločinci tyto standardní formy obnovují a modernizují podle aktuálních trendů ve společnosti. Úrodnou půdou pro kyberzločin se také stávají nástroje a technologie používané při vytváření interaktivního prostředí oblíbených webů sociálních sítí. V březnu společnost Trend Micro odhalila, že na špičkové stránky fungující na principech Web 2.0 (tj. sociální sítě, sdílení videa a stránky pro VoIP), poskytovatele freemailů, banky a oblíbené weby pro e-komerci zaútočilo přes 400 phishingových softwarových kitů určených k automatickému vytváření phishingových stránek.

Vývoj malwaru pro kombinované hrozby

Malwarové varianty jsou obvykle považovány za samostatné hrozby. Dnes webové hrozby vytvářené s cílem osobního profitu kombinují různé škodlivé softwarové komponenty do jedinečného „business modelu“ webových hrozeb. Kyberzločinci například zašlou přes instant messengery spam nebo

Překvapivé: Mobilní hrozby prozatím hrají jen malou roli a jejich počet stále klesá…

zprávu obsahující odkaz na záludnou URL adresu. Uživatel klikne na odkaz a je přesměrován na webovou stránku, z níž se do jeho počítače automaticky nahraje soubor s trojským koněm. Trojský kůň poté stáhne další soubor (spyware), který sbírá citlivé informace, jako jsou čísla bankovních účtů (spy-phi-shing). I když jde zdánlivě o jeden incident, s kombinovanými hrozbami se mnohem hůře bojuje a pro uživatele jsou mnohem nebezpečnější.

Zneužívání nových technologií

Technika fast-flux je dalším příkladem toho, jak zločinci zneužívají technologický rozvoj. Fast-flux je mechanismus, který umožňuje zneužít DNS servery (domain-name-server) kombinací sítí peer-to-peer, distribuovaných příkazů a proxy přesměrování na skryté weby, čehož využívají především phishingové nástroje. Fast-flux pomáhá phishingovým webům zůstat delší dobu v provozu a přilákat více obětí. Bezpečnostní experti tak mají větší problém s identifikací záludných domén Storm, protože jejich vývojáři využívají techniky fast-flux a ztěžují tak odhalení těchto domén.

Snížení počtu útoků adwaru a keyloggerů

Společnost Trend Micro zjistila, že během první poloviny roku 2008 došlo k výraznému nárůstu aktivity v oblasti webových hrozeb. Jen v březnu dosáhl jejich počet 50 milionů, když v prosinci 2007 jich bylo zaznamenáno zhruba 15 milionů. Sestupný trend byl naopak zaznamenán u adwaru, trackwaru, keyloggerů a freeloaderů. V březnu 2007 bylo podle společnosti Trend Micro nakaženo adwarem zhruba 45 procent počítačů, zatímco v dubnu 2008 šlo pouze o 35 procent. V dubnu 2007 bylo trackwarem nakaženo zhruba 20 procent PC, v květnu tento počet klesl na méně než pět procent. Také keyloggery zaznamenaly sice malý, zato stálý pokles – na jaře 2008 jimi bylo nakaženo méně než pět procent počítačů, zatímco v září 2007 se tento počet vyšplhal na pět procent.

Mezi další podstatná zjištění uvedená ve zprávě patří:

Hrozby se stále více zaměřují na dobře zavedené webové stránky. Počátkem ledna bylo provedeno několik masivních útoků typu SQL injection na tisíce webových stránek patřících společnostem uváděným v žebříčku Fortune 500, vládních organizací a škol.

- Mobilní hrozby stále hrají mezi nově se rozvíjejícími hrozbami jen malou roli. V lednu objevila společnost Trend Micro malware přestrojený za multimediální soubor, který měl infikovat starší mobilní telefony Nokia.
- Se znalostmi přichází přes-

nost. Kyberzločinci se stále více zaměřují na movité uživatele, jako jsou špičkoví manažeři, kteří představují malý počet bohatých jedinců, kteří mají přístup k větším bankovním účtům, přihlašovacím údajům nebo dokonce e-mailovým adresám, které se používají v celé organizaci.

- Na počátku roku 2008 objem spamu dočasně poklesl – zřejmě šlo o přestávku po vánočních svátcích. Objem zato výrazně narostl v březnu a opět lehce poklesl v dubnu. Pokles spamové aktivity si odborníci Trend Micro vysvětlují buď jako přeskupování spammerů a přípravu na nový útok, nebo jako testování nových technik.
- Počet botů (zneužitých pécéček) narostl z více než jednoho a půl milionu v lednu na únorových více než 3,5 mil. Tento vzestup byl následován výrazným březnovým poklesem.

Předpověď na následujících šest měsíců

Podle průzkumů a pozorování útoků, které se objevily od počátku tohoto roku, odborníci Trend Micro předpovídají, že v příštích šesti měsících dojde k následujícím trendům:

- Sociální inženýrství zůstane klíčovou metodou útoků a nastoupí ještě sofistikovanější triky. Trend Micro očekává, že kyberzločinci se budou snažit zneužít takové události, jako jsou letní olympijské hry, nákupy před začátkem školního roku, prezidentská volební kampaň ve Spojených státech, utkání ve fotbalu či hokeji nebo zimní prázdniny.
- Kyberzločinci se budou i nadále zaměřovat na nově odhalené zranitelnosti v softwarových aplikacích jiných firem, jako jsou QuickTime, RealPlayer, Adobe Flash atd.
- Pomalu bude klesat počet útoků pomocí crimewaru, který se spoléhá na zastaralé technické metody, jako jsou dialery a keyloggery. Bude také klesat výskyt graywaru, jako je trackware a malware pro únosy prohlížečů (browser hijackers) – tento malware se v éře milionových botnetů příliš neuplatní.
- Objem spamu i nadále exponenciálně poroste a v průměru se zvýší na 30 až 50 milionů zpráv denně. Spam a phishing se zvýší především v srpnu s aktivitami spojenými s nadcházejícím návratem dětí do škol a olympijskými hrami. Sezonní nárůst spojený se zimními prázdninami se dá očekávat i v listopadu, kdy předpověď objemu spamu dosahuje 170 až 180 miliard zpráv denně.
- Stejně jako nyní budou v příštích měsících spam a phishing součástí kombinovaných hrozeb. Okolo 0,2 procenta, tj. jedna z každých 500 webových žádostí, je zasíláno na webové stránky hostované na infikovaných počítačích. Očekává se, že tento trend bude pokračovat.
- Boty a botnety budou hrát důležitou roli v řetězci šíření hrozeb, jako je spamming, úniky informací, cílené útoky a celoplošné útočné kampaně.

Kopii celé zprávy naleznete na **http://us.trendmicro.com/us/threats/enterprise/security-library/threat-reports/index.html**.

INFO

Nová bezpečnostní rizika

SUN SOLARIS ADOBE READER

Sun oznámil nalezení chyb v zabezpečení aplikace Adobe Reader. Úspěšné zneužití může dovolit útočníkovi spuštění libovolného kódu nebo přepis libovolného souboru pomocí symbolického linku. Jako řešení se doporučuje nenačítat PDF soubory z nedůvěryhodných zdrojů a vypnout JavaScript v prohlížeči. Zranitelnost se netýká Solaris 8–10 na platformě x86 a Open Solaris. Více podrobností naleznete na informačním serveru Sun Solaris, konkrétně na adrese **http://sunsolve.sun.com/search/document.do?assetkey=1-66-240106-1**.

INFO: zprávy.actinet.cz

PODSTRČENÍ FALEŠNÝCH AKTUALIZACÍ

Na stránkách společnosti Infobyte byla zveřejněna ukázková aplikace **(www.infobyte.com.ar/down/isr-evilgrade-Readme.txt)**, která dokáže zneužít nedávno zmiňovanou zranitelnost v DNS a útokem způsobu man-in-the-middle podstrčit nejrůznějším programům (Sun Java, Winzip, Winamp, Mac OS X, OpenOffice, ...) falešné aktualizace přes internet.

INFO: zprávy.actinet.cz

RED HAT – REALPLAYER

Red Hat potvrdil výskyt zranitelnosti v aplikaci RealPlayer, která umožní potenciálním útočníkům zkompromitovat uživatelský systém. Daná chyba postihuje RealPlayer 10.0.9, konkrétně doplňky v Red Hat Enterprise Linux 3 Extras, 4 Extras a 5 Supplementary. Podrobnější informace o zranitelnosti najdete na adrese **https://rhn.redhat.com/errata/RHSA-2008-0812.html**. Jediným řešením, které prozatím výrobce navrhuje, je omezit používání balíku, který obsahuje chyby.

INFO: zprávy.actinet.cz

BEZPEČNOSTNÍ SOFTWARE

Symantec uvolnil beta verze produktů s číslovkou 2009

Společnost Symantec uvolnila k bezplatnému stažení beta verze svých produktů Norton Internet Security 2009 a Norton AntiVirus 2009, které nabízejí novinky v oblasti ochrany počítačů i vylepšení z hlediska rychlosti a výkonu.

Společnost Symantec uvolnila k bezplatnému stažení beta verze svých produktů Norton Internet Security 2009 a Norton AntiVirus 2009, které nabízejí novinky v oblasti ochrany počítačů i vylepšení z hlediska rychlosti a výkonu. Produkty lze získat na adrese **www.symantec.com/norton-beta/.**

Nové produkty, jež byly vyvinuty s cílem minimálního dopadu na rychlost počítače, obsahují přes 300 vylepšení, od skenovacího modulu až po uživatelské rozhraní. Příkladem zlepšení je doba instalace beta verze, která zabírá přibližně jednu minutu, častější distribuce aktualizací a jen poloviční nároky na operační paměť než u předchozí verze.

„Na základě informací od našich klientů jsme se v této verzi zaměřili na výkon. Produkty Norton 2009 tak přinášejí svým uživatelům prvotřídní bezpečnost a zároveň umožňují rychlou činnost počítače," uvedl Vladimír Špička, Consumer Sales Manager EE společnosti Symantec ČR.

Norton 2009 obsahuje vlastnosti, které byly navrženy s ohledem na profesionální uživatele, včetně těch, kteří hrají počítačové hry on-line:

- tichý mod – automaticky zastavuje výstrahy a aktualizace, aby nedošlo k přerušení nebo zpomalení aktivit, jako jsou hry, filmy nebo prezentace;
- zjednodušuje uživatelské rozhraní – poskytuje rychlejší přístup k nastavení detailní konfigurace
- Norton Protection System – zastaví hrozby ještě před tím, než mají reálný dopad. Tento vícevrstvý ochranný systém zahrnuje ochranu prohlížeče před útoky, které pochází z napadených webových stránek, ochranu v reálném čase SONAR, preventivní ochranu proti vniknutí (IPS), antirootkit, antivirus a antispyware technologie;
- Norton Identify Safe – zdokonaluje ochranu identity uživatele zejména při obchodních a bankovních transakcích, surfování a on-line hrách (pouze NIS 2009);
- Home Networking (domácí síť) – umožňuje uživatelům zobrazit a spravovat zařízení, která jsou připojena do domácí sítě (pouze NIS 2009);
- AntiBot – zabraňuje botům (druh malwaru), aby převzali kontrolu nad počítačem.

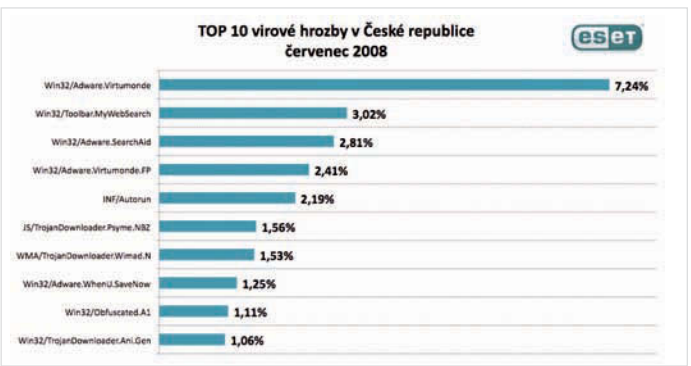
Komentář redakce:
Už NIS s číslem 2008 byla oproti předchozí verzi příjemně svižnější a čelní umístění v našem srovnávacím testu potvrdilo i její další kvality. Jednou z mála slabin komplexních bezpečnostních nástrojů bývá jejich rychlost a systémové nároky, které dokáží slabší počítač srazit na kolena. Jsme proto zvědavi na slibovanou rychlost nové verze. V jednom z příštích čísel vám nabídneme podrobnější pohled na obě bezpečnostní novinky...

CO NÁS OHROŽUJE

Agresivní nevyžádaná reklama

Podle statistického systému ESET ThreatSense.Net se v ČR v posledních měsících nejvíce šíří agresivní adware Win32/Adware.Virtumonde, který zahlcuje počítače nevyžádanou reklamou. Z analýzy situace ve světě pak vyplývá, že globálně nejohroženější skupinou jsou počítače hráčů internetových her a uživatelů virtuálních světů typu SecondLife, které napadá hrozba Win32/PSW.OnLineGames.

Žebříček globálních virových hrozeb se v červenci 2008 oproti předchozímu měsíci téměř nezměnil. Celosvětově se opět nejvíce šířil Win32/PSW.OnLineGames s celkovým podílem 12,72 %. Hráči her typu Lineage či World of Warcraft, ale i uživatelé nejrůznějších virtuálních světů by si měli dávat velký pozor na řadu on-line hrozeb. Kromě neškodných virtuálních útoků a obtěžování se útočníci zaměřují na důmyslné podvodné metody, zvláště pak na phishing. Úspěšné útoky mají za následek reálnou finanční škodu, protože dochází k vykrádání informací z uživatelských účtů nebo k odcizení postav z her či virtuálních světů. Díky vysoké poptávce po tomto virtuálním zboží dochází k následnému prodeji na černém trhu.



Popularity vyměnitelných médií (hlavně levných USB disků a paměťových karet) důmyslně využívají tvůrci virových hrozeb, kteří jejich pomocí a prostřednictvím souboru autorun.inf šíří stále velké množství trojských koní. ESET tyto hrozby souhrnně označuje jako INF/Autorun a v červenci se umístily na druhém místě s podílem 4,68 %. Třetí místo patří s podílem 4,41 % rodině zákeřného adwaru Win32/Adware.Virtumonde, který se projevuje otevíráním velkého množství oken s nevyžádaným reklamním obsahem.

Nejrozšířenější hrozby v ČR

Hrozby zachycené v červenci 2008 v České republice se na celosvětových hrozbách podílely 1,12 %. Systém včasného varování ESET ThreatSense.Net označil za nejčastější hrozby rodiny nejrůznějších adwarových infiltrací, tedy aplikací snažících se zahltit počítač nevyžádanou reklamou. První místo patřilo agresivnímu adwaru Win32/Adware.Virtumonde (7,24 %), druhou nejrozšířenější hrozbou byl Win32/Toolbar.MyWebSearch (3,02 %) a třetí a čtvrté místo patřilo adwaru Win32/Adware.SearchAid (2,81 %) a Win32/Adware.Virtumonde.FP (2,41 %). Top 5 v Česku uzavírá INF/Autorun s podílem 2,19 %.

Komentář redakce:
Útoky na virtuální světy jsou prozatím největší hrozbou především v Asii, kde je zájem o on-line hry mnohem větší než v Evropě. Je však pouze otázkou času, kdy podobné útoky dorazí i na starý kontinent. Situaci „napomáhají" také internetové aukce, kde uživatelé neváhají utrácet stovky dolarů za kvalitní herní postavy nebo virtuální předměty.

CREATIVE ZEN MOZAIC

Inspirace uměním mozaiky

Creative nabízí nový přenosný přehrávač médií Creative ZEN Mozaic. Ten zvládne reprodukci hudby, fotografií a videa. Tvůrci Creative ZEN Mozaic se inspirovali uměním mozaiky a vytvořili odvážný design – na výběr je stříbrná, růžová a černá verze. ZEN Mozaic je vybaven vestavěným reproduktorem a 1,8palcovým barevným LCD displejem, FM rádiem a funkcí nahrávání hlasu. Kompaktní přehrávač s rozměry 79,5 × 40 × 12,8 mm je dostupný ve variantách s dvěma, čtyřmi nebo osmi GB paměti s cenou od 1 500 do 2 200 Kč. Na podzim bude k dispozici i model se 16 GB za 3 500 Kč.

INFO: **www.creative.com**

ČLÁNKY O WEBDESIGNU

Weblogy.cz prodány

Společnost Internet Info rozšířila portfolio svých serverů nákupem služby Weblogy.cz, která sleduje blogy v oblasti internetového dění, webdesignu a technologií. Kupní cena ve výši 260 tisíc korun byla stanovena v aukci, do níž se zapojilo sedm zájemců. Mezi dalšími účastníky dražby byly například společnosti Jyxo, Ataxo a Superhosting.cz. Pro zařazení blogu na službu Weblogy.cz je nutno splnit řadu kritérií. Obsah musí být jak stylisticky, tak především odborně kvalitní. Samotný blog musí být funkční, dostupný a s kvalitními službami. Zároveň musí být dostatečně tematicky profilován. V současné době tvoří obsahový základ Weblogů přibližně 150 zdrojů. Autory blogů jsou známé osobnosti české internetové komunity – od provozovatelů webů a novinářů přes specialisty na internetový marketing či webdesign až po tvůrce webového obsahu.

NINTENDO WII

Nová technologie sledování pohybu

O úspěchu herní konzole Wii od firmy Nintendo jistě není pochyb. Za tímto úspěchem stojí partnerství firmy Nintendo se společností InvenSense, tvůrcem originálního ovladače. Nedávno jsme se dočkali jeho nové verze.

Ovladač s názvem Wii Motion Plus dokáže na rozdíl od svého předchůdce snímat i rotaci v libovolném směru. Podle slov Joe Virginia, viceprezidenta IS, je toto maximální možný stupeň sledování pohybu, má být totiž v poměru 1:1. Tohoto úspěchu se podařilo dosáhnout kombinací originálního gyroskopu s akcelerátorem. Citlivost snímače by měla být velmi vysoká, minimálně 500 stupňů za sekundu. Určitou cenou za tuto možnost je zvýšená energetická náročnost.

Nový ovladač je tedy dostupný, jeho příchod však zaskočil i mnoho vývojářů her. Na nové tituly, které možnosti Wii Motion Plus dokáží naplno využít, si budou muset majitelé herních konzolí počkat, protože „staré“ tituly využijí jenom schopnosti předchůdce.

INFO: **http://wii.ign.com**

MIVVY M310

Další netbook pod 10 000 Kč

Nabídka levných netbooků s procesorem Atom se opět rozšířila, a to o model M310 značky Mivvy (známé z oblasti mobilních telefonů). Netbook má rozměry 260 × 180 × 31,5 mm a hmotnost pouze 1 kg. K dispozici jsou 2 GB operační paměti a celých 120 GB na pevném disku. 10palcový displej má rozlišení 1 024 × 600 bodů. M310 nabízí i bezdrátové technologie Wi-Fi a Bluetooth, ale také univerzální čtečku paměťových karet, 1,3Mpx webkamerku a tři USB porty. Podle výrobce lze při běžné práci počítat až s šestihodinovou výdrží. Novinka od Mivvy se bude prodávat s předinstalovanými operačními systémy Windows XP a Vista nebo alternativním Linuxem Ubuntu 8.04. Cena začíná na 9 500 Kč s DPH.

INFO: **www.mivvy.eu**

VYHLEDÁVAČ

Google Earth jako plug-in browseru

Po Google Earth dal nyní Google k dispozici také variantu založenou na prohlížeči. Pomocí této aplikace je možné propojení 3D glóbu s webovými stránkami. Až dosud zde bylo možné sledovat jenom 2D mapy. Pro provozovatele internetových stránek je především zajímavé, že je zde pro ně k dispozici rozhraní, které mimo jiné umožňuje umísťování značek na jednotlivá místa. První uživatelské možnosti se nacházejí na google.com, například je možné díky zoomovací funkci na 3D glóbu téměř vidět kadeřnictví na rohu. Plug-in je dostupný zdarma. Jediný háček: celé to funguje jenom pod Windows pod Firefoxem 2 a ve verzi Internet Explorer 6 a výše.

INFO: **www.google.com**

VOIP

Neomezená linka od O2

Jednoduché řešení pro firemní zákazníky nabízí Telefónica O2. Ta poskytuje službu O2 Neomezená linka, která je založena na bázi VoIP technologií a umožňuje integrovat hlasové i datové spojení s okolním světem do jediné přípojky. Hlavním benefitem služeb je přístup k virtuální telefonní ústředně bez investic do jejího pořízení, správy a provozu. Virtuální znamená i to, že je možné ji využívat i na více lokalitách jako jednotného systému. Koncoví uživatelé navíc získají možnost personalizace – vlastnosti služby si mohou jednoduše nastavit přímo ze svého počítače, a také flexibilitu – počet uživatelů (tel. čísel) lze snadno měnit.

Neomezené volání na pevné linky přijde na 273,30 Kč vč. DPH měsíčně, 1 000 volných minut do všech mobilních sítí v ČR stojí 595 Kč vč. DPH.

Komentář redakce: *Telefónica přichází s takovou službou opravdu velmi pozdě. Kdo chtěl na VoIP přejít, pořídil si už službu u konkurence. Na druhou stranu cena je velmi příznivá – tak levné volání do mobilních sítí jinde neseženete.*

INFO: **www.cz.o2.com**

TOSHIBA CAMILEO

Kamera o velikosti fotoaparátu

Toshiba představila nové videokamery řady Camileo. Tyto videokamery mají velmi malé rozměry (71 × 34 × 108 mm) a přitom nabízejí záznam obrazu s vysokým rozlišením (1 280 × 720 bodů). Jako médium slouží paměťové karty SDHC. Model Camileo Pro HD nabízí v rozměrech 70 × 33 × 113 mm navíc trojnásobný optický zoom. Kamera také zvládne plnit funkci fotoaparátu (rozlišení snímků je až 3 744 × 2 808 bodů), MP3 přehrávače a diktafonu. Je vybavena bleskem a režimem pro potlačení efektu červených očí. K dispozici je 8x digitální zoom a displej s úhlopříčkou 2,5", který lze natáčet až o 240 stupňů. Baterie NP60-Li-Ion zvládne 105 minut natáčení nebo 140 minut přehrávání. Součástí balení je i software a 1,2 m dlouhý HDMI kabel. Videokamera Toshiba Camileo HD bude k dostání za doporučenou koncovou cenu 2 790 Kč vč. DPH, Camileo Pro HD za 4 790 Kč.

INFO: www.toshiba.cz

HP LABORATORY MASTERCLASS 2008

Seminář se soustředil na inkoustový tisk

Na každoroční technologický seminář „HP Labs" se těší většina evropských hardwarových redaktorů. Tento seminář totiž představuje nejen jednu z mála příležitostí, při kterých výrobci uvádějí novinky určené pro nadcházející sezonu, ale zároveň možnost nahlédnout hlouběji pod pokličku technologického vývoje s výhledem na léta dopředu. Letos se tento seminář specializoval hlavně na inkoustový tisk a představena byla řada nadcházejících produktů. O některých z nich zatím ještě nemůžeme psát, některé však už máme na zkoušku i v naší testovací laboratoři. Jedná se například o zajímavé novinky HP Photosmart Pro B8850 a HP Photosmart D5460, jejichž recenzi vám přineseme v příštím čísle. Model HP Photosmart D5460 používá k tisku pět inkoustů (nové kazety HP 364 obsahují čtveřici POC Dye inkoustů a samostatnou pigmentovou černou), díky kterým dokáže kombinovat fototisk a kvalitní černý text, srovnatelný s laserovým tiskem.

Nosnou technologickou novinku bylo představení nových inkoustů a produktů kombinujících vlastnosti pigmentového a „Dye" tisku. Zvýšení kvality tisku rovněž přináší tzv. technologie „Dual Drop Volume", tedy možnost vystřelovat z jedné hlavy kapičky inkoustu o dvou velikostech. Praktickým výsledkem je, že díky různým velikostem kapiček a kombinaci pigmentového a obyčejného inkoustu je dosahováno kvality srovnatelné se šestibarevným tiskem, tedy vyššího barevného gamutu, rychlejšího zasychání barev a nižší rozpíjivosti. Při kancelářském tisku je hlavní výhodou zvýšená kvalita tištěného textu, jehož nedostatky patří k hlavním nevýhodám inkoustového tisku v porovnání s tiskem laserovým. Speciálně pro stroje vybavené pětiinkoustovým tiskovým systémem byl uveden i nový nanoporézní fotografický papír HP Advanced Photo Paper, který využívá výhod kombinace pigmentového a POC Dye inkoustu. S kompletním portfoliem nových tiskáren a multifunkčních zařízení, stejně jako s dalšími novinkami a technologiemi, které byly představeny na HP Laboratory Masterclass 2008, vás budeme průběžně seznamovat v rámci našich srovnávacích i krátkých textů.

INFO: www.hp.cz

SYNCHRONIZACE

Dálkově řízené mobily

Nokia od července nabízí novou verzi mobilního řešení Nokia Intellisync Mobile Suite 9.0. Toto serverová platforma je určena pro smartphony Nokia E Series E51, E61, E66, E71 a další i pro přístroje s OS Symbian 3. edice a Windows Mobile. Software nabízí kromě plynulé synchronizace elektronické pošty, kalendáře a osobních (PIM) údajů také novou řadu nástrojů pro vzdálenou správu a údržbu telefonů. Administrátoři nebo i sami uživatelé mohou na dálku svoje mobilní zařízení spravovat, např. je zabezpečit v případě ztráty nebo odcizení.

Komentář redakce: *Službu jsme měli možnost testovat déle než týden a po celou dobu pracovala bez zaváhání. Je velmi pohodlné, když máte s sebou v mobilu ten samý obsah jako ve svém Outlooku v počítači, případně na Exchange serveru v zaměstnání. Kontakty, e-maily, připomínky, vše se automaticky synchronizuje.*

INFO: www.nokia.cz