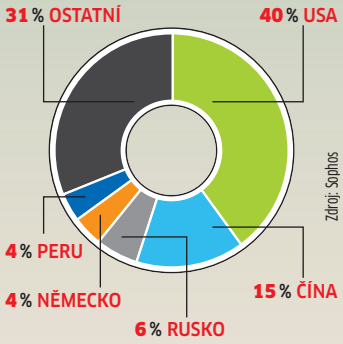
DATA A FAKTA

Barometr nebezpečí
v září

Po dovolených napadají hackeři především obrazové služby a společenské komunity.

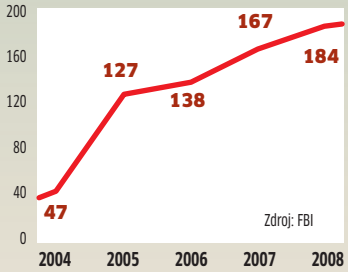
Kde sídlí hackeři



US hackeři: Většina útočníků pochází z USA, druhá největší hackerská komunita žije v Číně.

Výnosné zločiny

Škody v milionech eur



Webová kriminalita: Hackeři vydělávají stovky milionů eur ročně.

Číslo měsíce

8 eur

platí spammeři za rozeslání milionu reklamních mailů. Důvod: Sítě botů jsou stále levnější.

Každý mobil je hackerský nástroj

Pomocí jediné SMS zprávy mohou útočníci **ODPOSLOUCHÁVAT SMS A OCHROMOVAT PŘÍSTROJE** – aniž byste proti tomu jako majitelé mohli cokoli udělat.

FABIAN VON KEUDELL

Evropané ročně rozešlou kolem několika set miliard esemesek – a většina z nich by jejich mobilní telefon mohla vyřadit z provozu. Bezpečnostní experti Collin Mulliner a Charlie Miller objevili cestu, jak lze pomocí jednoduchých SMS zpráv vysílat do mobilního telefonu řídicí příkazy a převzít tak nad ním kontrolu.

Postiženy jsou téměř všechny modely. U tradičních mobilů mohou útočníci do přístrojů poslat zfalšovanou SMS provozovatele, kterou například změní WAP konfiguraci napadených přístrojů – aniž by si toho jejich majitelé mohli všimnout. Napříště poběží veškerý datový provoz přes hackerské servery. Jde totiž o to, že konfigurační SMS může normálně poslat jenom sám provozovatel sítě. Hackeři k tomu jednoduše využívají příslušnou odesílatelskou identifikaci provozovatele. Čísla odesílatelů kontrolují sítě pouze u MMS zpráv, nikoli však u SMS.

U iPhonu firmy Apple mohou útočníci zablokovat proces CommBoard, tedy komunikační centrálu přístroje. Dojde přitom k tomu, že telefon přeruší momentální hovor, ztratí přístup do sítě a na zhruba 10 sekund není dostupný. Pokud však útočníci pošlou takových SMS například několik set, je telefon zablokován na hodiny, či dokonce dny. U přístrojů se systémem Android je zranitelným místem telefonní modul com.android.phone. Je-li napaden, přeruší aktuální telefonát a uživatel musí nově zadat PIN pro SIM kartu.

Ještě hůře jsou postiženy přístroje s Windows Mobile. Zde havaruje celý mobil a nelze jej znovu zapnout. Teprve když je hackerská SMS z doručených zpráv odstraněna, podaří se mobil nastartovat. K tomu ovšem musí postižený uživatel vložit svou SIM kartu do jiného telefonu. Jestliže jsou stovky hackerských SMS vysílány na servery provozovatele podle časového plánu, například jedna zpráva za den, je pak přístroj s Windows Mobile prakticky nepoužitelný.

Společnými silami: Pomohou provozovatelé a výrobci

Záplatu pro smartphony nabízejí dosud jen Apple a Google. Právě u nejzranitelnějších přístrojů s Windows Mobile však oprava k dispozici není. U normálních mobilů momentálně pracují v Německu velcí operátoři na možnosti verifikovat identifikaci uživatele u každé SMS. Ani zde však zatím nebylo dosaženo úspěchu. V průměru trvá zhruba pět měsíců, než se tak hluboko zasahující mezeru v mobilní síti podaří odstranit. Do té doby budou provozovatelé intenzivně své sítě kontrolovat a cíleně vyhledávat neobvyklé SMS zprávy.

INFO: www.tu-berlin.de

Vstupní brána mobil: Prostřednictvím jednoduché SMS zprávy mohou hackeři přesměrovat data z mobilu nebo celý přístroj kompletně ochromit.

APPLE

Hackerský PC v klávesnici

Bezpečnostní mezera v mikrořadičích klávesnic od Applu umožňuje hackerům instalovat programy, které nikdo nedokáže odhalit a odstranit. Čipy v klávesnici normálně zpracovávají klávesové vstupy uživatelů, avšak tyto čipy lze jednoduchým hackerským „updatem“ nově popsat. Tomu by vlastně měl zabránit speciální kód, který je obsažen v originálních aktualizacích firmwaru – ten ale útočníci prostě zkopírovali. Tak mohou hackeři nainstalovat do klávesnice samostatné programy, například keylogger, který protokoluje klávesnicové vstupy uživatele. Aby dokázali klávesnici takto upravit, potřebují ovšem darebáci přístup k Macu, který získají například využitím bezpečnostní mezery v nějakém browseru. Je to velice praktické: data z keyloggeru si pak tito kriminálníci jednoduše vyvolají přes internet tak, že vytvoří zašifrované SSL spojení. Firewall ani jiné ochranné systémy si přenosu dat nepovšimnou. Jakmile se škůdce jednou ocitne v klávesnici, zabraňuje dalším aktualizacím. Nepomůže ani nová instalace operačního systému. Apple už však pracuje na záplatě pro postižené klávesnicové moduly. Ta má nahrávání cizích aktualizací firmwaru efektivně zabránit.

INFO: www.apple.com

NOVÁ SLUŽBA

Netgear Live Parental Control

Netgear představil ve spolupráci se společností OpenDNS novou službu Live Parental Control. Společnost OpenDNS, která je předním poskytovatelem profesionálních služeb zajišťujících bezpečnější, rychlejší a spolehlivější připojení k internetu, bude integrovat své špičkové technologie do vybraných směrovačů společnosti Netgear.

Služba Live Parental Control umožní rodinám a malým firmám omezit přístup k nebezpečným či nevhodným webovým stránkám na všech internetových zařízeních připojených přes směrovače Netgear. Dokáže filtrovat více než 50 kategorií obsahu včetně sociálních sítí či stránek s obsahem pornografie a násilí. Live Parental Control obsahuje zcela komplexní sadu funkcí pro kontrolu internetového obsahu, včetně např. vzdálené správy z mobilního zařízení či vysoce flexibilního nastavení, které nejsou dostupné v žádném jiném řešení pro rodičovskou kontrolu.

Netgear Live Parental Control umožňuje rodičům v domácnostech i administrátorům ve firmách omezit přístup k nebezpečným internetovým stránkám a filtrovat nepatřičný webový obsah. Uživatelé nemusejí instalovat ani spravovat samostatné aplikace pro rodičovskou kontrolu na každém počítači nebo dalších zařízeních s přístupem k internetu. Jednoduše nastaví pravidla přímo na směrovači, který je možné spravovat také pomocí vzdáleného přístupu. Tato síťová kontrola neochraňuje pouze počítače, ale navíc i mobilní telefony a bezdrátová zařízení typu Sony PSP či Nintendo Wii, připojená k bezdrátové síti směrovače. Live Parental Control zajišťuje rovněž pokročilou ochranu proti phishingu.

Snadnou instalaci zajišťuje CD, které je součástí prodejního balení. Uživatelé mohou rovněž navštívit webové stránky www.netgear.com/lpc, kde najdou více informací.

INFO: www.netgear.com

INFO

Nová bezpečnostní rizika

ADOBE READER A ACROBAT

Využitím mezery ve Flash modulu programů Adobe Reader a Acrobat mohou útočníci propašovat do PC zmanipulované Flash soubory a instalovat tak v počítači škodlivý software. Řešení je snadné: nainstalujte si nejnovější verzi softwaru s číslem 9.1.3.

INFO: www.adobe.com

MICROSOFT INTERNET EXPLORER

Slabinu v Active Template Library (ATL) pro ActiveX Controls mohou hackeři využít ke spouštění vlastních programů. Prostřednictvím služby Windows Update si nainstalujte nejnovější záplaty pro Internet Explorer.

INFO: www.microsoft.com

GOOGLE CHROME

V internetovém prohlížeči od Googlu využívají hackeři „heap overflow“ v interpreteru javaskriptů a paměťovou chybu v renderovacím procesu, aby do počítače propašovali vlastní záškodnický kód. Od verze 2.0.172.37 jsou problémy v googlovském browseru odstraněny.

INFO: www.google.com/chrome

BEZPEČNOSTNÍ PRODUKTY

AVG ve verzi 9.0

Společnost AVG Technologies uvolní během října 2009 na trh verzi 9.0 všech svých bezpečnostních produktů. Vývojáři program výrazně vylepšili, což se v AVG 9.0 projevuje na rychlosti, úrovni ochrany i snadném používání. Na základě zpětné vazby od zákazníků se o 50 procent zkrátila doba instalace, snížilo se zatížení paměti a také se výrazně zjednodušil proces ochrany.

Pro kombinované antivirové/antispywarové jádro AVG 9.0 byla hlavní prioritou optimalizace scanování. Soubory jsou při první kontrole označeny jako bezpečné a potenciálně nebezpečné. Při následující kontrole program bezpečné soubory vynechává, pokud se nezmění jejich struktura. Výsledkem je mnohem kratší doba testu; až o 50 % v závislosti na konfiguraci systému. Stejně tak se o 10 až 15 % snížila doba bootování.

„Produkty AVG 9.0 poskytnou domácím uživatelům účinnější ochranu v reálném čase, aniž by ovlivnily jejich práci s počítačem. Přivádí nás to zpět k našemu hlavnímu cíli, tedy co nejvyšší bezpečnosti s co nejnižšími nároky na uživatele," řekl generální ředitel AVG Technologies J. R. Smith.

Rychlost a vícevrstvá ochrana

Nová verze AVG 9.0 kombinuje veškeré moderní technologie ochrany před nejnovějšími hrozbami v reálném čase. Nad rámec signatur známých hrozeb využívá AVG 9.0 behaviorální a in-the-cloud technologie, včetně tzv. white listování. Umožňuje to ochranu před desítkami tisíc nových hrozeb denně. Program AVG 9.0 je spojením rezidentní ochrany, firewallu a ochrany identity. Jednotlivé moduly mohou tedy sdílet informace o zjištěném malwaru. To zvyšuje schopnost AVG objevovat a odstraňovat většinu škodlivých kódů, rootkitů i pokusů o krádež identity, pro něž ještě nebyly zveřejněny signatury.

Vylepšení firewallu zahrnují celkovou přestavbu, která snižuje počet otázek na uživatele o 50 %, a díky tomu jej mnohem méně ruší. Nová databáze důvěryhodných aplikací a certifikátů umožňuje nyní bez interakce s uživatelem „posoudit", zda povolit, či zakázat komunikaci. Firewall zajišťuje velmi vysoký stupeň ochrany i před novými a doposud neznámými hrozbami, jelikož pracuje na pozadí společně s behaviorálním modulem AVG Identity Protection. AVG ve verzi 9.0 má po rozšíření funkce LinkScanner vylepšenu i detekci phishingu. Při použití více než stovky různých indikátorů potenciálních hrozeb na každou stránku rozpozná funkce rychleji a přesněji, zda internetová stránka skrývá phishingový útok. V případě nejasného výsledku zkontroluje LinkScanner phishingová data ve výzkumné síti AVG a poté na jejich základě usoudí, zda jde o potenciální hrozbu.

Produkty AVG ve verzi 9.0 mají i nový vzhled a strukturu, což ještě více usnadňuje jejich používání. O mnoho jednodušší je rovněž detekce a odstranění veškerých aplikací, které by mohly s AVG 9.0 působit proti sobě a narušit tím úroveň zabezpečení.

Nástroj proti krádežím identity

Ve světě každoročně narůstá počet krádeží identity. Vyskytují se v mnoha formách od podvodů při využívání e-shopů či e-bankingu až po krádeže při placení kartou v obchodě či restauraci. Produkty AVG nyní obsahují další vrstvu ochrany AVG Identity Protection (IDP). Ta zdokonaluje celkové zabezpečení před hrozbami, které jsou nerozpoznatelné pro běžné antivirové aplikace. Je přitom lhostejné, zda jsou na počítači nainstalovány produkty AVG, nebo jiné firmy. IDP pracuje vedle všech nejčastěji používaných antivirů spolehlivě a kdykoli. Brání útokům vedeným s cílem krádeže hesel, odcizení podkladů k internetovému bankovnictví, čísel kreditních karet a dalších cenných informací. Používá tzv. behaviorální analýzu, která zjišťuje odchylky od standardního chování programů v počítači. Pokud odhalí cokoli podezřelého, co by mohlo naznačovat pokus o krádež identity, odstraní hrozbu a ukončí danou aktivitu ještě před zasažením uživatelových dat.

AVG Identity Protection je založena na technologii, kterou firma AVG Technologies získala po akvizici společnosti Sana Security počátkem tohoto roku. Analyzuje chování jednotlivých programů, proto nepotřebuje ke své aktualizaci popisy známých škodlivých kódů a předejde snaze útočníků odcizit uživateli on-line identitu. Software se navíc průběžně učí i z informací uživatelů o reálných útocích a zajišťuje jejich neustálou ochranu.

Dostupnost a cena

Veškeré placené produkty AVG 9.0 jsou k dispozici on-line, v obchodech i v dalších prodejních kanálech. Licence AVG Internet Security 9.0 na jeden rok a jeden počítač stojí 1 345 Kč včetně DPH a cena dvouleté licence je 2 011 Kč včetně DPH. Volná verze AVG Free 9.0 bude k dispozici od poloviny října.

NOVÁ BETA VERZE:

ESET Mobile Antivirus

Společnost ESET uvolnila beta verzi programu ESET Mobile Antivirus pro operační systém Symbian. Beta verze je určena pro testování základních funkcí včetně skenovacích modů (on-demand a on-access), heuristiky, updatů, logů a systémové aktivace. Optimalizovaná heuristická detekce pro mobilní zařízení umožňuje všem přístrojům s operačním systémem Symbian využívat nejlepší ochranu proti veškerým elektronickým či internetovým hrozbám.

Veřejná beta verze ESET Mobile Antiviru pro Symbian dovolí uživatelům mazat infiltrace přímo nebo je přesunout do karantény, kde už nebudou nadále představovat hrozbu pro operační systém. Soubor přesunutý do karantény může být následně nadobro vyčištěn a obnoven. Produkt také nabízí skenování a čištění integrovaných i výměnných paměťových médií. Navíc skenuje v paměti běžící procesy a všechny bezdrátově přicházející či odcházející data. Eset Mobil Antivirus pro Symbian nabízí také unikátní možnost zkontrolovat obsah komprimovaných archivů s výběrem hloubky takového skenování na stupnici od jedné do čtyř.

Automatický update zajišťuje, že mobilní zařízení bude ochráněno nejen proti aktuálním hrozbám. Řešení kontroluje, je-li databáze aktuální, a umožňuje uživateli nastavit pravidelné intervaly pro update. Jednoduché a intuitivní uživatelské rozhraní bylo navrženo tak, aby jeho použitelnost logicky korespondovala se stylem daného operačního systému. Beta verzi programu ESET Mobile Antivirus pro Symbian můžete stáhnout na **www.eset.cz/download/beta**.

MOZILLA FIREFOX

Nebezpečné surfování

Hned čtyři bezpečnostní mezery uzavře poslední aktualizace browseru Firefox. Využitím jednoho ze slabých míst mohou útočníci spouštět v počítači javaskriptové programy s oprávněním správce a instalovat tak škodlivý software. Totéž platí pro mezeru ve správě paměti browseru. Ještě kritičtější je chyba při zpracování volání SSL. Použitím speciálních funkcí v programovém kódu Firefoxu mohou hackeři uživateli předstírat, že se místo na normální stránce nachází na zašifrované SSL stránce. Čtvrtá oprava se týká problému s SSL certifikáty. Využitím mezery u certifikačních úřadů si hackeři dokážou pro webové stránky vystavit certifikáty a browseru tak například vsugerovat, že hackerská stránka je stránkou pro homebanking. Chyby odstraňuje verze 3.5.2 browseru.

Bezpečnější: Verze 3.5.3 opravuje čtyři chyby.

INFO: mozilla-europe.org

STATISTIKA ESET

Česko zamořil adware

Globálně nejrozšířenější počítačovou hrozbou byl i v září Win32/Conficker. Podle statistik systému Eset ThtreatSense.Net je tak Conficker jednoznačně nejčastěji šířeným škodlivým kódem v tomto roce. V září dosáhly nejrůznější typy červa Conficker rozšířenosti 8,76 %, což znamená, že téměř každý desátý zachycený škodlivý kód byl Conficker.

Stejně jako v srpnu i tentokrát byla na druhém místě hrozba označovaná jako INF/Autorun (7,53 %). Autorun.inf je známý soubor umožňující automatické spouštění souborů uložených na vyměnitelném médiu, ihned jak je toto médium připojeno k počítači. Dobrou zprávou je, že v průběhu uplynulého měsíce došlo ke snížení počtu trojanů zaměřených na on-line hráče či virtuální světy typu Second Life. Win32/PSW.OnLineGames byl v září na třetím místě celkem s 6,36 % ze všech detekovaných hrozeb, což sice není malé číslo, ale je druhé nejnižší od počátku letošního roku.

První pětku uzavírá rodina malwaru označovaná jako Win32/Agent, vykrádající data, a INF/Conficker, tedy různé varianty červa Conficker, zneužívající funkci autorun.inf. V průběhu září se rostoucí popularita vyměnitelných médií (hlavně díky klesajícím cenám médií) i nadále podepisovala na zvyšujícím se výskytu hrozeb využívajících ke svému šíření právě USB disky či paměťové karty.

Česko se i v září vymykalo dění v regionu. Lokální statistiky škodlivého softwaru zcela ovládl adware Win32/Adware.DoubleD, který ve variantách A až AE vévodil žebříčku u nás nejrozšířenějších hrozeb. Celkem představoval v září více než 12 % všech detekovaných hrozeb. Konkurovat mu dokázal jen trojan Win32/TrojanDownloader.Bredolab (4,25 %), který instaluje na počítače napadených uživatelů další malware. DoubleD představuje poměrně neškodný typ počítačové infiltrace – nesnaží se krást citlivé údaje nebo provádět destruktivní činnost, pouze obtěžuje uživatele, například modifikací vyhledávání na internetu, kdy se snaží směrovat na stránky s nelegálním obsahem. V Česku je adware v různých modifikacích dlouhodobě nejčastěji šířeným škodlivým kódem.

BOOTKIT

TrueCrypt dešifrován

Bezpečnostní specialista Peter Kleissner vyvinul bootkit, jímž může vyřadit z činnosti šifrovací nástroj pevného disku TrueCrypt. Jeho program se přitom zapíše do MBR (Master Boot Record) pevného disku, který je vždy nezašifrovaný, neboť systém musí zavést dešifrovací rutinu. Hackerský software se nyní do systému včlení jako komunikační rozhraní mezi Windows a TrueCrypt. Tak může nástroj kdykoliv nainstalovat do počítače software, aniž by to virové skenery zaznamenaly. Imunní jsou jenom šifrovací systémy, které sledují MBR a využívají modul TPM (Trusted Platform Module), například BitLocker od Microsoftu. Ale také programátoři TrueCryptu už na aktualizaci pro dosud nezabezpečený šifrovací software pracují.

INFO: www.truecrypt.org

NOVINKY OD SYMANTECU

Norton pro rok 2010

Společnost Symantec uvádí produkty Norton 2010 s novými technologiemi zjišťování pro boj s počítačovou kriminalitou. Klíčovou novinkou je tentokrát technologie Quorum – zabezpečení založené na „pověsti". Norton Internet Security 2010 a Norton AntiVirus 2010 využívají nový model zabezpečení s kódovým označením Quorum, který zajišťuje zjišťování nového škodlivého kódu a převyšuje tradiční zjišťování založené na signaturách a analýze chování. Quorum využívá největší zbraň počítačových zlodějů, kterou mají ve svém arzenálu, a to jejich schopnost děsivou rychlostí generovat jedinečné fragmenty škodlivého kódu, a tuto jejich zbraň obrací proti nim.

Nejen nejrychlejší

Symantec se snaží navázat na úspěch produktů Norton ve verzi 2009 a pokračuje v poskytování bezpečnostních produktů, které jsou rychlé a efektivní. V Nortonu 2010 byla opět velká pozornost věnována výkonu, přestože byla v této verzi přidána také nová důležitá technologie ochrany. Skupina technologií Norton Insight v nových produktech 2010 využívá rozsáhlé informační systémy on-line k proaktivní ochraně počítače a informování uživatelů o tom, jaký vliv na výkon a zabezpečení mají soubory a aplikace, se kterými se setkávají při každodenním použití počítače on-line.

► Norton Download Insight: Využívá rozsáhlé on-line informační systémy, které k proaktivní ochraně počítače využívají informace o pověsti. Analyzuje a oznamuje bezpečnost nových souborů a aplikací před tím, než je uživatelé nainstalují a spustí.

► Norton System Insight: Poskytuje funkce a srozumitelné informace o systému, které pomáhají udržovat špičkový výkon počítačů. Automatická a vyžádaná optimalizace aplikací oživuje výkon aplikací. Zobrazuje poslední události v počítači a poskytuje informace potřebné ke zkoumání a analyzování problémů s počítačem. Výkonové grafy pomáhají přesně určit příčiny zpomalení počítače.

► Norton Threat Insight: Poskytuje podrobnosti o hrozbách zjištěných v počítači, včetně užitečných informací o jejich původu (adresa URL) a prvním kontaktu.

► Norton Insight Network: Využívá koncept shluků. Tato funkce založená na technologii Quorum přispívá k tomu, že zabezpečení založené na shlucích překonává svými schopnostmi tradiční seznamy zakázaných a povolených položek. Určuje úroveň důvěryhodnosti souboru pomocí statistické analýzy atributů souboru, která je založena na miliardách prověření několika milionů počítačů. Software Norton je tímto způsobem schopen určit důvěryhodné a nedůvěryhodné soubory, které by spadaly do šedé oblasti neznáma, pokud by byly použity pouze tradiční metody zabezpečení.

Doporučená maloobchodní cena aplikace Norton Internet Security 2010 CZ je 1 499 Kč včetně DPH (u aplikace Norton AntiVirus 2010 CZ je to 1 099 Kč včetně DPH) a zahrnuje licenci pro jeden počítač.

Komentář redakce

Bezpečnostní produkty firmy Symantec v našich testech pravidelně zaujímají přední místa a Norton Internet Security byl první bezpečnostní produkt, o kterém jsme mohli bez uzardění říci, že nebrzdí počítač – a právě proto jsme zvědavi, jak si povede jeho nástupce. V příštím čísle tak najdete jeho podrobný test, včetně srovnání s konkurencí.

SYMANTEC MESSAGELABS INTELLIGENCE REPORT

Roboti útočí

Společnost Symantec Corp. oznámila výsledky zprávy 2009 MessageLabs Intelligence Report za 3. kvartál. Rozbor upozorňuje na to, že robotické sítě jsou nyní odpovědné za zasílání 87,9 % veškeré nevyžádané pošty. Novější robotická síť Maazben zaznamenala po nesmělém počátku koncem května rychlý růst a rozesílá hlavně nevyžádanou poštu, která se týká kasin. Jedna z nejstarších a největších robotických sítí Rustock od června zdvojnásobila svoji velikost a má nyní předvídatelné časové rozložení rozesílání nevyžádané pošty.

Pracovní doba spambotů

Podle týmu MessageLabs Intelligence vzrostl podíl robotické sítě Maazben během uplynulého měsíce ze srpnových 0,5 % veškeré nevyžádané pošty na zářijových 1,4 % veškeré nevyžádané pošty. Robotická síť Rustock je největší co do počtu botů, ale její výstup v přepočtu na jednotlivé boty zůstal relativně nízký. Největší robotická síť Rustock s 1,3 mil. až 1,9 mil. botů má nyní ustálené časové rozložení rozesílání nevyžádané pošty, které začíná každý den v 9 hod. ráno SEČ, dosahuje vrcholu ve 13 hod. SEČ a ustává v 1 hod. SEČ. Následuje osmihodinová přestávka, po které znovu začíná rozesílání. Rustock je jediná robotická síť s pravidelným cyklem rozesílání nevyžádané pošty. Rustock je jedna z nejvýznamnějších robotických sítí a je odpovědná za 10 % veškeré nevyžádané pošty. Její časové rozložení rozesílání nevyžádané pošty se proto projevuje v celkovém denním časovém rozložení nevyžádané pošty.

„V uplynulém roce bylo několik poskytovatelů služeb internetu odpojeno kvůli hostování aktivit robotické sítě, což se ukázalo jako dvojsečné opatření a vedlo k posunu ve schopnostech robotických sítí," řekl Paul Wood, MessageLabs Intelligence Senior Analyst společnosti Symantec.

„Byly tím těžce zasaženy významnější robotické sítě jako Cutwail a vytvořen prostor pro vznik nových robotických sítí jako Maazben. To ale nebude platit vždy, protože i technologie robotických sítí se od konce roku 2008 vyvíjela a nejnovější případy ukončení činnosti poskytovatelů služeb internetu mají menší vliv na výslednou činnost. Prostoj nyní trvá pouze několik hodin, a nikoli týdnů nebo měsíců jako dříve."

Po ukončení činnosti těchto poskytovatelů služeb internetu v průběhu uplynulých tří měsíců měly dvě další robotické sítě možnost vybojovat si pozici nejaktivnější robotické sítě, která zůstala po síti Cutwail. Pozici nejaktivnějších robotických sítí pro distribuci nevyžádané pošty převzaly robotická síť Grum, co do velikosti polovina sítě Rustock, ale odpovědná za 23,2 % nevyžádané pošty, a robotická síť Bobax, odpovědná za 15,7 % nevyžádané pošty. Robotická síť Cutwail byla předtím odpovědná za 45,8 % nevyžádané pošty.

Další fakta

Nevyžádaná pošta: V září 2009 byl globální podíl nevyžádané pošty v e-mailovém provozu z nových a dříve neznámých závadných zdrojů 86,4 % (1 z 1,2 e-mailu), což je od srpna pokles o 2,1 %. Podíl nevyžádané pošty byl ve 3. kvartálu 2009 v průměru 88,1 %, oproti 81,0 % ve 3. kvartálu 2008.

Viry: Globální podíl e-mailů napadených virem v e-mailovém provozu z nových a dříve neznámých závadných zdrojů byl v září jeden z 399,2 e-mailu (0,25 %), což je od srpna pokles o 0,09 %. 39,8 % škodlivého kódu šířeného e-mailem obsahovalo v září odkazy na nebezpečné webové servery, což je od srpna zvýšení o 22 %. Ve 3. kvartálu 2009 se aktivita škodlivého kódu šířeného e-mailem pohybovala v průměru na úrovni 1 výskytu z 330,3 e-mailu, oproti 1 z 122,5 ve 3. kvartálu 2008.

Zářijová zpráva 2009 MessageLabs Intelligence Report obsahuje podrobnější údaje o všech výše uvedených trendech a hodnotách a podrobnější rozbor trendů v zeměpisných oblastech a ve vertikálních oborech. Úplná zpráva je k dispozici na adrese **www.messagelabs.com/intelligence.aspx**.

INFO: www.symantec.com

OPERÁTOŘI

Dva internety za cenu jednoho

Až do konce října mají zákazníci O2 možnost získat levné mobilní připojení. Za 750 Kč získá zákazník jak pevné připojení domů pomocí ADSL, tak mobilní připojení na cesty. Při objednání služby O2 Internet (standardní cena 750 Kč) a O2 Mobilní internet (standardní cena 600 Kč) zaplatí zákazníci za obě služby 750 Kč. Opravdu tak platí reklamní slogan „dva internety za cenu jednoho". Další 100Kč slevu získají zákazníci, kteří mají jakýkoliv tarif O2 Neon. Za oba internety pak zaplatí 650 Kč. Kromě mobilního internetu je možné k ADSL dokoupit také O2 TV, potom je celková cena 900 Kč, nebo 300 volných minut na O2 Volání s cenou 720 Kč. Obě ceny je opět možné snížit o 100 Kč při kombinaci s tarifem O2 Neon. Srovnání cen pevného a mobilního připojení, včetně parametrů, najdete v toplistu na straně 98.
INFO: http://www.cz.o2.com

WELL SIP-T20P

Telefon napájený přes ethernet

VoIP telefon SIP-T20P firmy Well si vystačí s napájením přes ethernet. Tímto připojením si uživatel zajistí provoz telefonu i při výpadku elektrické sítě. Telefon je určen do kanceláří menších i větších firem, ale i do moderních domácností. Snadné ovládání zajistí česká lokalizace displeje a web managementu. Telefon disponuje adresářem až pro 300 záznamů a paměť pojme až 100 volaných čísel, 100 příchozích čísel a 100 zmeškaných volání. WELL SIP-T20P zaujme i designem i tím, že jednoduchým otočením podstavce lze telefon postavit na stůl, nebo ho lze pověsit na zeď.
INFO: www.joyce.cz

GPS NAVIGACE

Mio Moov V505 a V735

Výrobce Mio představil dvě nová navigační zařízení vybavená multimediálními funkcemi. Mio Moov V505 nabízí 4,7" dotykový displej, zatímco hlavním znakem Mio Moov V735 je displej se 7" úhlopříčkou. V navigačním softwaru Mio Spirit jsou mapy díky zobrazení TruMap přehledné a nejsou zakryty dalšími informacemi. Při odbočování či na sjezdu z dálnice řidič ocení detailní navádění pro řazení v jízdních pruzích. Snížit náklady na pohonné hmoty zase pomůže nová možnost výpočtu ekonomické trasy, která bere v úvahu průjezd světelnými křižovatkami a zatáčkami a omezí tak počet zbytečných zastavení, brzdění a rozjezdů. Obě navigační zařízení obsahují přijímač dopravních informací RDS-TMC s vestavěnou anténou.

Novou funkcí je vyhledávání destinace na jednom řádku, kdy uživateli stačí napsat do řádku požadovanou adresu nebo klíčové slovo, stejně jako při vyhledávání na internetu, a navigace zobrazí výsledky v seznamu i na mapě. Výhodu širokoúhlého displeje uživatel ocení především při využívání multimediálních funkcí. Navigační zařízení umí přehrávat audiosoubory a videosoubory a díky vestavěnému DVB-T tuneru sledovat i televizní vysílání. Multimediální funkce se dají ovládat pomocí přiloženého dálkového ovládání. Navigační zařízení Mio Moov V735 se prodává za 9 990 Kč, model V505 za 8 490 Kč.
INFO: http://eu.mio.com

NOTEBOOKY VAIO

Netbook Sony a další modely

Společnost Sony předvedla svůj první netbook: Sony Vaio série W. Jeho přednostmi oproti konkurenci jsou kromě stylového designu především vysoké rozlišení 10,1" obrazovky (1 366 × 768) a dobrá výbava zahrnující velký, 250GB pevný disk. Baterie má výdrž více než sedm hodin. Netbook se bude dodávat už s novým OS Windows 7 Starter.

V nabídce bude mít Sony na podzim i další nové modelové řady notebooků Vaio: multimediální sérii CW v pěti módních barvách a spíše profesionální řadu NW. Modely CW i NW mají nad klávesnicí tři „zlatá" tlačítka: jedno pro rychlé spuštění webového prohlížeče bez nutnosti čekání na kompletní start počítače (do 15 sekund), druhé pro okamžité vypínání displeje (šetří energii například při poslechu hudby nebo sledování filmů na připojeném TV) a třetí tlačítko „VAIO" pro přímé otevření galerie médií (prohledávání, přehrávání a prohlížení digitálních fotografií, videa a hudby).

K většině notebooků Vaio se dodává předinstalovaný software Sony pro intuitivní zpracování obrázků, střih videa, sdílení dat v rámci domácí sítě a ukládání fotografií v přehledném kalendáři. Všechny nové modely Vaio budou dodávány už se systémem Windows 7.
INFO: www.sony.cz

GOOGLE STREET VIEW

První ochutnávka Street view

Google spustil panoramatické fotografie Prahy a okolí v aplikaci Street View. Uživatelé se tak mohou projít po nábřeží Vltavy, vychutnat si pohled na Pražský hrad, nebo se virtuálně zatoulat v některé z pražských uliček. Česká republika je tak osmou zemí v Evropě, kde je služba Street View spuštěna. Zajímavým doplňkem bude pro řidiče i neřidiče pohled na trasu dálnice D1 do Brna, po které se mohou virtuálně projet. Googlu se v první fázi podařilo zobrazit 3 500 km ulic, silnic a dálnic.
INFO: mapy.google.cz/street-view

WEBOVÁ FOTOGALERIE

Zoner nabízí Zoneramu

Zájem uživatelů internetu o sdílení svých fotografií strmě stoupá. Není proto divu, že na rostoucí poptávku reagovali všichni významní poskytovatelé internetových služeb v tuzemsku i zahraničí. Na webové adrese www.zonerama.cz dokončila a v ostrém provozu spustila novou fotogalerii také společnost Zoner software, producent programů pro digitální fotografii a současně jeden z největších poskytovatelů webového prostoru. Zonerama, na rozdíl od mnohých konkurenčních galerií, nabízí svým uživatelům prezentaci fotografií v nezměněné kvalitě. Při vkládání obrázků až do velikosti 1 920 × 1 200 bodů a do objemu 1,5 MB nejsou fotografie jakkoliv upravovány a uživatel tak má šanci vystavit svoje fotografie v přesně požadované podobě, tedy včetně nastaveného stupně komprese, doostření apod. Větší obrázky jsou dodatečně zmenšeny a upraveny pomocí algoritmů.
INFO: www.zonerama.cz

FERRARI ONE

Designový netbook od Aceru

Společnost Acer představila řadu svých nejexkluzivnějších netbooků: Ferrari One. Detaily, barvami a funkcemi připomínají netbooky vozy Ferrari – například víko má charakteristickou červenou barvu závodních vozidel. LCD displej s LED podsvícením má úhlopříčku 11,6", vysoké rozlišení 1 366 × 768 bodů a filmový formát 16:9. Pevný disk má kapacitu až 500 GB. Nechybí samozřejmě ani bezdrátová síťová karta (802.11a/b/g/Draft-N), Bluetooth 2.1+EDR (Enhanced Data Rate) a webová kamerka.

Na rozdíl od jiných netbooků nemá Ferrari One procesor od Intelu (ostatně jako všechny modely Ferrari), protože s touto značkou je spojeno i AMD, a tak byla použita druhá generace platformy Ultrathin Platform (AMD 'Congo'), konkrétně dvoujádrový procesor AMD Athlon X2 L310 1,2 GHz v nízkonapěťovém provedení a grafická karta ATi-Radeon HD 3200, která zvládne pohodlně i vysoké rozlišení. Podporována je i technologie ATI XPG, která umožňuje použít výkonnější externí grafiku. Výdrž na baterii výrobce zatím neuvádí. Netradičně je u tohoto stroje zvolen i operační systém – 64bitová verze nového systému Microsoft Windows 7 Home Premium. Cena by se měla pohybovat kolem 12 000 Kč.

INFO: www.acer.cz

MCKLEIN OAK PARK

Kabelky na notebook pro ženy

Společnost Sekora consulting nabízí novou řadu luxusních kožených kabelek na notebook McKlein Oak Park s delšími uchy pro nošení přes rameno. Vnitřní prostor je rozdělen na hlavní oddíly, z nichž jeden je polstrován vrstvou hmoty, která absorbuje nárazy a chrání přenosný počítač před poškozením. Druhý hlavní oddíl je vybaven množstvím kapsiček pro uložení různých drobností moderní ženy. Kabelky jsou k dispozici ve třech barevných variantách.

INFO: www.sekora.cz

TELEVIZE NA WEBU

TV Prima má nové stránky

Koncem prázdnin se po téměř dvou letech web Televize Prima (www.iprima.cz) dočkal nové podoby, která vychází ze staniční grafiky televizní stanice. Nový web je připraven tak, aby obsahoval více zajímavých informací o oblíbených pořadech. Komfortnější je též například sledování videí k jednotlivým pořadům; videoarchiv je připraven ve spolupráci se serverem Stream.cz. Nové stránky nabízejí návštěvníkům také větší možnosti zapojit se do tvorby webu prostřednictvím interaktivních a komunitních prvků. V dohledné době se mohou diváci těšit na speciální stránky některých pořadů. Chystají se také inovace zpravodajského videoarchivu.

INFO: www.iprima.cz