DATA A FAKTA

Barometr nebezpečí
v únoru:

Momentálně registrujeme vlnu phishingových útoků zaměřených na sociální komunity.

Pět hlavních spammerů

1. Canadian Pharmacy (USA)
2. Leo Kuvayev (Rusko)
3. Herbal King (Indie)
4. Vincent Chan (Hongkong)
5. Alexander Mosh (Ukrajina)

Zdroj: Spamhaus.org

Spamové maily propagují zdravotnické produkty a pornografii, nově však také transplantáty.

Phishingové maily 2008

Počet aktivních phishingových www Zdroj: Antiphishing.org

Pro rok 2009 předpokládají experti podobný vývoj phishingových mailů jako v roce 2008.

Číslo měsíce

10 000

eur měsíčně v průměru vydělávají hackeři tím, že donutí infikované počítače navštěvovat webové reklamy.

Hackerské odposlechy

Kdo chce **ODPOSLOUCHÁVAT BEZŠŇŮROVÉ TELEFONY**, ten potřebuje tři věci: notebook, hardware za necelých 30 eur a dvě minuty času.

FABIAN VON KEUDELL

Nic pro tajnosti: Telefony standardu DECT lze pomocí několika prostředků snadno a rychle odposlouchávat.

Kdo dnes při telefonování ještě stále zakopává o šňůru, ten má jednu výhodu – je dalekosáhle chráněn před útoky hackerů. Naproti tomu hovory přes bezšňůrové telefony standardu DECT (Digital Enhanced Cordless Telecommunications) mohou hackeři neuvěřitelně snadno odposlechnout. Jenomže to zdaleka není všechno – napadnutelná jsou také datová spojení podle standardu DECT, například Babyfone nebo bezdrátové terminály pro EC karty v restauracích.

Žádná velká novina to ovšem není, neboť napadnutelnost tohoto standardu je známa už řadu let. Dosud však útočníci, chtěli-li se dostat k datům rozhovoru, museli budovat velmi drahá a náročná odposlechová zařízení. Teď však na konferenci Chaos Communication Congress v Berlíně vynalézaví experti předvedli, že to jde nejen jednodušeji, ale také mnohem levněji. Všechno, co dnešní špion potřebuje, je notebook a do něj speciální VoIP karta, která přijde asi na 23 eur. Ta dokáže na rozdíl od normálního WLAN adaptéru vysílat a přijímat DECT signály. Odposlech je pak ve většině případů směšně jednoduchý, neboť mnohá DECT spojení nepoužívají vůbec žádné šifrování – tady mohou hackeři odposlouchávat data zcela bez problémů.

Jindy zase VoIP karta v hackerském PC předstírá, že je základnovou stanicí DECT, a funguje jako retranslační člen mezi mobilní částí a skutečnou základnovou stanicí. Finta spočívá v tom, že hackerský počítač oběma komponentám jednoduše vydá příkaz, aby deaktivovaly šifrování. Pak už se téměř všechna spojení dají obratem ruky „kreknout".

Lepší je to postaru: Odposlechům vzdorují jen šňůrové telefony

Zde může pomoci jen permanentní šifrování, které během spojení nepřipouští nové klienty. To by ovšem vyžadovalo změnu standardu jako takového. Dosud v něm totiž žádné povinné šifrování není předepsáno. A co horšího – jestliže nějaké domněle legitimní zařízení šifrování nepodporuje, všechny připojené komponenty solidárně přestanou šifrovat. Ale i pro případ, že hovory chrání nějaký algoritmus, už hackeři znají první slabiny, v nichž by se dal šifrovací systém prorazit.

Malý záblesk naděje představuje nový šifrovací standard DECT Standard Cipher (DSC). Ten jako přídavnou proměnnou u šifrovacích klíčů využívá náhodná čísla. Nasazen je ovšem pouze v nových modelech telefonů a EC terminálů. Staré přístroje jsou tedy i nadále napadnutelné. Kdo chce mít absolutní jistotu, ten se proto musí vrátit k dřívějším řešením s kabelovým propojením – i za cenu nebezpečí klopýtnutí…

INFO: www.ccc.de

NOKIA

SMS poškodí mobil

Jenom na Silvestra rozeslali Češi přes 30 milionů krátkých textových zpráv. Mnohé z nich byly doručeny se zpožděním, nebo dokonce nedorazily vůbec. Příčinou byla přetížená mobilní síť – nebo také nová bezpečnostní mezera v mobilech firmy Nokia. Prostřednictvím zmanipulované textové zprávy v nich hackeři dokážou budoucí příjem SMS znemožnit. Postiženy jsou všechny modely řady S60, například současný multimediální model N95 nebo pro obchodníky určený Nokia E90 Communicator. Mezera se dá využít děsivě snadno – útočníkům stačí odeslat SMS, která obsahuje e-mailovou adresu delší než 32 znaků. Tato jediná textová zpráva pak přetíží mezipaměť přístroje, který kvůli nedostatku paměti napříště žádnou SMS nepřijme. Varovné hlášení však přitom adresát nedostane – zatímco odesílatel obdrží zprávu o úspěšném doručení. Pomoci může zatím jenom kompletní hardwarový reset, ten však také vymaže všechna data. Nokia i provozovatelé mobilních sítí už pracují na příslušné záplatě.

INFO: www.nokia.com

INFO

Nová bezpečnostní rizika

MICROSOFT INTERNET EXPLORER

Využitím mezery v ošetření mezidatové vazby (data binding) v internetovém prohlížeči Microsoftu dokážou hackeři propašovat do počítače škodlivý kód a spustit jej. Postiženy jsou všechny verze od 5.01 až po aktuální verzi 8 Beta 2. Odpovídající záplatu obdrží uživatelé cestou automatických aktualizací.
INFO: www.microsoft.com

IBM STORAGE MANAGER

V produktu IBM Storage Manager byla nalezena zranitelnost dovolující kompromitovat systém. Zranitelnost je zavíněna nedostatečnou kontrolou vstupu poskytnutého souboru adsmdll.dll při zpracování dat sezení. To může způsobit přetečení zásobníku a tím i spuštění libovolného kódu. Chyba je zneužitelná jen lokálně. Více informací najdete ve zprávě IBM (**www-01.ibm.com/support/docview.wss?uid=swg21377388**).
INFO: zpravy.actinet.cz

MOZILLA FIREFOX

Hned osm bezpečnostních mezer ve Firefoxu mohou hackeři využít ke spouštění škodlivých kódů. Je mezi nimi i kritická chyba, kvůli níž rovnou havaruje celý browser. Řešením je upgrade – od verze 3.0.5 jsou chyby odstraněny.
INFO: www.mozilla-europe.org

MICROSOFT

Mimořádnou pozornost byste měli věnovat bezpečnostním záplatám pro březen 2009. Microsoft vydal záplaty pro opravu chyb v Microsoft Windows Kernelu (dovolujících vzdálené spuštění kódu), pro opravu chyb v bezpečnostním balíčku Secure Channel (umožňujících spoofing) a pro opravu chyb v DNS a WINS serverech (dovolujících útočníkům přesměrovat provoz ze serverů na jiné místo na webu). Více informací o celém balíčku záplat naleznete na webu Microsoft Technet (**www.microsoft.com/technet/security/bulletin/ms09-mar.mspx**).
INFO: zpravy.actinet.cz

TWITTER

Obama terčem hackerů

Na mikroblogové službě Twitter zapisují lidé z celého světa ve 140 znacích, co mají právě na srdci. Jako „hlásnou troubu" používají službu Twitter dokonce i prominenti, mezi nimi nový americký prezident Barack Obama nebo třeba Britney Spears. Využitím bezpečnostní mezery v podpůrných nástrojích Twitteru se nyní hackerům podařilo získat přístup k libovolným účtům.

Tyto nástroje jsou normálně určeny pro pracovníky Twitteru, aby mohli změnit mailové adresy v případě, že uživatel opustil svůj účet a už se nemůže dostat k přístupovým datům. Momentálně jsou nástroje zablokovány. Podle provozovatele služby je známo jen 33 účtů, které útočníci zmanipulovali; postihlo to i Baracka Obamu. Nedá se ovšem vyloučit, že byly napadeny i další přístupy. Uživatelé Twitteru by proto měli změnit své heslo.
INFO: www.twitter.com

SYMANTEC

Antivir ochromuje PC

Ztráty dat a zhroucení počítačů obvykle způsobují viry a ostatní škůdci. Teď však za havárie systémů mohou také virové skenery. Hackeři k ochromení počítačů využívají vadný ovladač SPBBCDRV.SYS v bezpečnostních nástrojích od Symantecu. Postiženy jsou verze napříč firemní paletou, například Norton 360, Norton AntiSpam, Norton AntiVirus a Norton Internet Security.

Mezera je výrobci známa už od dubna 2007. Tehdy na chybu v nástrojích Norton Personal Firewall a Norton Internet Security poukázal bezpečnostní expert David Matoušek. Nyní už výrobce dává k dispozici aktualizaci pro postižené produkty prostřednictvím LiveUpdate. Zdůvodnění tak značného zpoždění však Symantec svým zákazníkům zůstal dlužen.
INFO: www.symantec.com

SOFTWAROVÉ NOVINKY

TrustPort aktualizace

Společnost TrustPort vydává aktualizaci produktů TrustPort Antivirus a TrustPort PC Security, která na základě dosavadních zkušeností optimalizuje kombinaci použitých skenovacích motorů. Domácnosti a menší firmy si mohou kupovat oba antivirové produkty ve verzi pro jeden, tři nebo pět počítačů. Tento software nově zahrnuje tři skenovací motory – AVG, Norman a Dr.Web. Skenovací motor Ewido Antispyware, licencovaný společností AVG Technologies, se už dále nevyvíjí a jeho schopnosti jsou nyní součástí motoru AVG.

Jednou z novinek je podstatné snížení velikosti softwaru. „Velikost instalačního souboru pro domácnosti a menší firmy se snížila u TrustPort Antiviru i u TrustPort PC Security asi o 30 %," konkretizuje změnu Petr Vaněk, vedoucí vývojového oddělení společnosti TrustPort.

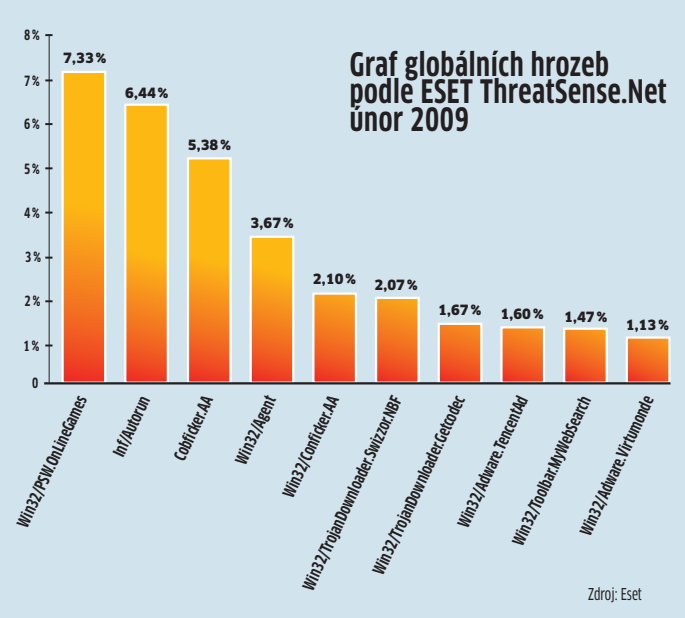
Střední a větší firmy si mohou objednat TrustPort Antivirus a TrustPort PC Security v multilicenci pro více než deset počítačů, ke které obdrží zdarma centrální správu TrustPort Management. Software v tomto případě obsahuje čtyři skenovací motory. V základní ceně jsou k dispozici motory AVG a Norman, s možností dokoupit si licenci na motory Dr.Web a VirusBlokAda. Ke zlepšením u obou bezpečnostních produktů patří například i kontrola zamčených souborů. „Nově dokážeme skenovat zamčené soubory, tedy soubory běžným způsobem nepřístupné pro čtení, a odhalit spuštěný škodlivý kód," objasňuje Petr Vaněk. „Soubor používaný běžícím procesem nelze okamžitě smazat. Náš software proto vyzve uživatele k restartu počítače a následně škodlivý kód odstraní." Schopnost detekce virů v zamčených souborech podstatně přispívá

k ochraně proti současným hrozbám. Došlo také k vylepšení detekce při skenování systémového registru. Zatímco v předchozích verzích se provádělo motorem Ewido Antispyware, v nové verzi ho zajišťují všechny použité skenovací motory. Software zaznamenal rovněž zlepšení v oblasti využití paměti.
INFO: www.trustport.cz

STATISTIKA MALWARU

Infekce přes USB klíče

Vysoká popularita vyměnitelných médií s velkou kapacitou na přenášení dat mezi počítači způsobuje nárůst výskytu počítačových hrozeb. Potvrzují to i únorové výsledky statistického systému ESET ThreatSense.Net. Ve druhém měsíci tohoto roku se stala „top hrozbou" rodina trojských koní Win32/PSW.OnLineGames (7,33 %). Tyto trojské koně se schopnostmi keyloggeru i rootkitu nejvíce ohrožují hráče počítačových her. Nejde přitom o žádnou zábavu, ale o tvrdý byznys s odcizenými virtuálními identitami. Autoři těchto hrozeb využívají různorodé techniky sociálního inženýrství a phishingové útoky. Některé z trojských koní vykrádajících údaje z on-line her používají ke svému šíření i vyměnitelná média a jsou poté detekovány jako INF/Autorun (6,44 %). Tato hrozba skončila v únoru 2009 na druhém místě. Třetí místo patří novince Win32/Conficker.AA, která začala ohrožovat počítače koncem minulého roku a která například vyřadila z provozu stovky počítačů v anglických nemocnicích. Červ Win32/Conficker.AA (5,38 %) se šíří prostřednictvím sdílených souborů a přenosných médií, jako jsou USB klíče. Na průnik do počítače využívá nezáplatovaný operační systém a automatické otevírání přenosných médií po připojení či vložení do počítače (autorun.inf).



Červ se připojuje ke vzdáleným počítačům a pokouší se zneužít chybu ve službě Server Service. Záplata operačního systému je k dispozici od října 2008, miliony uživatelů ji však stále ještě neaplikovaly. Doporučení: ESET má na svých stránkách k dispozici nástroj Conficker removal tool, který červa odstraní.

Win32/Agent (3,67 %) se mezi top hrozbami udržel i v únoru. Jde o generickou detekci rodiny infiltrací se schopností vykrádat údaje z počítače. Páté místo v žebříčku globálních top počítačových hrozeb patří modifikované verzi červa Win32/Conficker.A. Tato hrozba se však nešíří prostřednictvím vyměnitelných médií, jako je tomu v případě rozšířenějšího červa Win32/Conficker.AA.

Česko ohrožuje Win32/Agent a adware

Počítače českých uživatelů v únoru masově napadl známý vykradač údajů Win32/Agent (5,68 %). Popularita USB a jiných přenosných médií i v Česku podporuje šíření hrozeb využívajících nástroj autorun.inf v operačním systému MS Windows. INF/Autorun tak u nás obsadil čtvrté místo v žebříčku nejčastěji detekovaných infiltrací (2,89 %), Win32/Conficker.AA je desátý (1,38 %). Dlouhodobě se v ČR nejvíce šíří adware, tedy nevyžádaná reklama.

Hrozba zneužití identit v on-line hrách zasáhla velké evropské země

Jaká je situace v jiných evropských zemích? Nejenom v Česku, ale i v Německu, Finsku, Litvě a Lotyšsku nejčastěji ohrožoval počítače červ Win32/Agent nebo Win32/Agent.NFL. WMA/TrojanDownloader.GetCodec.Gen dominoval ve většině evropských zemí, jako například v Rakousku, Švédsku, Dánsku, Švýcarsku, Řecku, Holandsku, Itálii či Maďarsku.

Vysoká míra detekce (přibližně 10 % a více) červa Win32/Conficker.AA byla zaznamenána v Rusku, na Ukrajině nebo v Rumunsku. Mezi top hrozbami se však objevuje téměř ve všech evropských zemích. Zajímavá je situace na Slovensku, kde se Conficker nedostal ani do Top 20. Globálně nejrozšířenější hrozba Win32/PSW.OnLineGames (populární především v Asii) zasáhla nejvíce počítačů ve velkých evropských zemích, jako jsou Polsko (8,93 %), Francie (8,06 %) a Španělsko (6,95 %).

INFO: www.eset.cz

Komentář redakce: *Hrozby z přenosných zařízení jsou stále rozšířenější a my předpokládáme, že jejich pravý boom ještě přijde. Vzhledem k tomu, že 2GB USB flash disk lze dnes koupit za 150 Kč a jeho 16GB bratříčka pořídíte za necelých 400 Kč, očekáváme v brzké době jejich masové rozšíření. Dalším prvkem očekávané „epidemie" je fakt, že jejich kontrolu provádí většina uživatelů jen zřídka (případně vůbec). A jak se bránit? Kromě kvalitního antivirového nástroje lze doporučit u neznámých disků alespoň nouzovou obranu: disk připojte k počítači se stisknutou klávesou Shift, která zabrání automatickému spuštění...*

NOVÉ TECHNOLOGIE

Kaspersky proti hrozbám

Společnost Kaspersky oznámila patent na novou technologii umožňující snadnější detekci a odstranění škodlivého softwaru. Nová technologie je založena na sledování systému a logování událostí, které mohou souviset s virovou infekcí (například změna u spustitelného souboru nebo úprava záznamu v systémovém registru).

Unikátní je, že po odhalení škůdce nástroj analyzuje všechny další události související s nalezenou hrozbou, což umožní odhalení všech nebezpečných programů podílejících se na zjištěné události. Kromě odhalení a odstranění malwaru dokáže nástroj obnovit systém souborů z důvěryhodné zálohy. Informace o zjištěné hrozbě jsou navíc ihned odeslány do centrály, kde pomohou zlepšit čas reakce na další hrozby. Například zjištění zdroje hrozby může napomoci při blokování infikovaných stránek...

INFO: www.kaspersky.com

MICROSOFT

Browserový virus

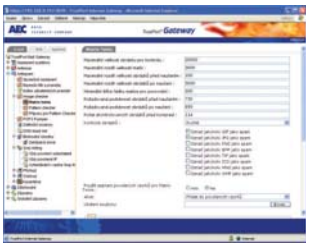
Webové stránky s fotografiemi, například Flickr, se stále častěji stávají šiřiteli virů. Prostřednictvím zmanipulovaných obrazových souborů obsahujících hackerské skripty spouštějí záškodníci v počítači kódy, pomocí nichž si zjednají přístup do počítače. Na vině je vlastnost Internet Exploreru, která měla původně zajistit jeho větší zabezpečení – u multimediálních obsahů browser nedbá na příponu souboru, ale rozhoduje sám, jak jej má interpretovat. Pokud pak soubor vedle obrazových informací obsahuje také HTML kód nebo javaskript, IE tento kód bez vyzvání uživatele spustí. Touto metodou, označovanou jako „MIME sniffing", mohou útočníci například vyšpehovat přístupová data k webovým stránkám. Nápravu má přinést až nový Internet Explorer 8. Uživatelů Firefoxu se tento problém netýká.

INFO: http://hackernews.jaanix.com/

TRUSTPORT NET GATEWAY 5.3

Pro sítě bezpečnější

Společnost TrustPort uvádí novou verzi bezpečnostního řešení pro počítačové sítě TrustPort Net Gateway. Toto ucelené řešení kontroluje veškerý poštovní a webový provoz mezi vnitřní sítí a internetem a umožňuje systematickou likvidaci rizik, jako jsou viry, spyware a spam. Stará se také o autorizaci uživatelů, což je podmínkou bezpečnosti při vzdáleném přístupu do počítačové sítě. Nová verze, TrustPort Net Gateway 5. 3, znamená další posun směrem k větší přehlednosti rozhraní, současně zahrnuje významné technologické novinky. Z hlediska ovládání řešení stojí za pozornost sjednocení záznamů vztahujících se k webovému provozu. S tím souvisí pokročilejší generování grafických statistik. Jakmile jsou statistiky webového provozu připraveny, lze je prohlížet ve vztahu k aktuálnímu měsíci nebo roku, případně je možné zobrazit si celkovou statistiku za dobu používání řešení. Na základě statistik může správce sítě analyzovat chování uživatelů a identifikovat problémy. Další novinkou jsou globální záznamy webového provozu. Tento nástroj je vhodný tam, kde objem provozu nedovoluje použití jediné internetové brány, takže je zapotřebí sloučit statistiky z více serverů. Pro poštovní provoz byly globální záznamy zavedeny již v předchozí verzi.



TrustPort Net Gateway 5.3 nabízí další sofistikovanou metodu eliminace spamu, a sice blokování podezřelých uzlů. *„Při této metodě nedochází k přijetí vlastní poštovní zprávy, ale k jejímu zhodnocení na základě povahy připojení a informací o odchozí doméně,“* popisuje Petr Vaněk, vedoucí vývojového oddělení společnosti TrustPort. *„Tímto způsobem lze rozpoznat podezřelé odesílatele a zabránit příjmu až dvou třetin spamu.“* Dochází tak k dalšímu snížení zbytečného přenosu dat.

Všichni zákazníci používající řešení TrustPort Net Gateway mohou zdarma přejít na novou verzi tohoto produktu. Instalační balíček rozpozná předchozí instalovanou verzi a hladce převezme stávající nastavení.

INFO: www.trustport.cz

EMSI SOFTWARE

Rafinovaná podlost

Výrobce antivirového softwaru Emsi odhalil novou metodu, pomocí níž hackeři propašovávají do cizího počítače škodlivé kódy. Útočníci zhotovili k nerozeznání věrné padělky policejních formulářů pro pokutování dopravních přestupků, na nichž je přidán odkaz na údajnou webovou stránku policie – tam se má pachatel přestupku o svém činu blíže informovat. Ve skutečnosti si z domnělé úřední stránky stáhne do svého počítače virus. Webová stránka sice obsahuje fotografie nesprávně zaparkovaných aut, daný případ však mezi nimi chybí. Ten má být možno najít až po nainstalování „Picture Search Toolbar“. Tím se však do počítače dostane malwarový DLL soubor, který se včlení do systému jako Browser Helper Object (BHO) a pak zobrazí hackerem generovanou varovnou zprávu propagující antispywarový skener. Kdo na ni klikne, vpustí si do PC hackery. Ochranu nabízejí všechny běžné antivirové systémy. Kromě toho platí, že úřady na pokutových blocích nikdy neodkazují na webovou stránku, která by podrobněji informovala o inkriminovaném činu.

INFO: www.emsisoft.com

INFO

Nová bezpečnostní rizika

ADOBE FLASH

V Adobe Flash byla potvrzena zranitelnost u verze 10.0.12.36 a všech předchozích pro Windows, ale je pravděpodobné, že zranitelné jsou i verze pro Linux a OS X. Zranitelnost se projevuje při zpracování Shockwave souborů a může být zneužita k DoS, případně i spuštění libovolného kódu. Více informací najdete na webu Adobe (**www.adobe.com/support/security/bulletins/apsb09-01.html**).

INFO: zpravy.actinet.cz

LINKSYS WLAN KAMERA WVC54GC

Pokud útočník vyšle zmanipulovaný datový paket na UDP port 916, získá tak přístup k údajům o systémové konfiguraci, mezi nimi k heslu pro WLAN a jménu uživatele. A oprava? Do přístroje nainstalujte aktuální verzi firmwaru 1.25.

INFO: www.linksys.com

MICROSOFT EXCEL

V aplikaci Microsoft Excel byla nalezena závažná chyba, která způsobuje možnost volání špatného objektu a tím pádem spuštění libovolného kódu pomocí upraveného souboru zneužívajícího tuto zranitelnost. Bližší informace o zranitelnosti naleznete na stránkách Microsoft TechNet (**www.microsoft.com/technet/security/advisory/968272.mspx**), kde také naleznete způsoby, jak problém dočasně řešit.

INFO: zpravy.actinet.cz

ADOBE READER/ACROBAT

V aplikacích Adobe Reader 9, Acrobat 9 (i předchozích verzích) byla zjištěna zranitelnost, která může způsobit pád aplikace a potenciálně i umožnit útočníkovi převzít kontrolu nad zasaženým systémem. Adobe plánoval vydat update k 11. březnu. Do té doby byla známa jediná ochrana, a to zakázání JavaScriptu v aplikacích Adobe. Ani to však neřeší všechny možné komplikace. Více informací naleznete v oznámení výrobce (**www.adobe.com/support/security/advisories/apsa09-01.html**).

INFO: zpravy.actinet.cz

TWITTER

Ve světě Twitteru se nyní šíří červ, který pokouší uživatele zprávou „Don't Click“. Kdo na ni klikne, předá stejnou zprávu dál ze svého vlastního účtu.
Twitter už pracuje na příslušné záplatě.

INFO: www.twitter.com

IBM AIX

V IBM AIX verze 5.2, 5.3 a 6.1. byla nalezena chyba, která může vést ke zvýšení privilegií. Příkaz „at“ nesníží oprávnění při čtení souboru, což může být zneužito místním útočníkem k přečtení jakéhokoliv souboru na systému. Řešením je aplikace fixů nebo APARs. Více naleznete na ibm.com (konkrétně na adrese **aix.software.ibm.com**).

INFO: www.zpravy.actinet.cz

GOOGLE CHROME

Využitím bezpečnostní mezery v prohlížeči Google Chrome mohou hackeři propašovat do počítače záškodnický kód a spustit jej. Řešení je snadné. Nainstalujte si novou verzi Chrome tak, že v menu kliknete na »Přizpůsobení a ovládání Google Chrome | O aplikaci Google Chrome«.

INFO: www.google.com/chrome

MODIFIKACE HROZBY

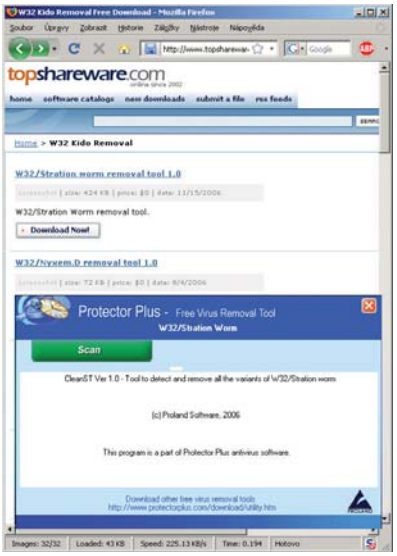
Kido chytřejší

Společnost Kaspersky Lab odhalila novou modifikaci trojského koně Kido. Poslední verze trojského koně se od starších variant tohoto škodlivého programu liší rozšířenou funkčností. Představitelé nové verze malwaru Kido jsou například varianty Net-orm. Win32.Kido.ip a Net-Worm. Win32.Kido.iq. Na infikovaných počítačích jsou tyto programy schopny narušit funkčnost antivirového softwaru. Nová varianta trojského koně také výrazně zvyšuje počet doménových jmen, které se škodlivý program pokouší každý den kontaktovat, aby si odtud stáhl aktualizace. Zatímco předcházející verze se takto pokoušela připojit k 250 serverům, v nové verzi činí tento počet už 50 000.

„Nová verze trojského koně Kido až dosud nepředstavovala hrozbu s povahou epidemie," uvádí Vitaly Kamluk, senior antivirus expert společnosti Kaspersky Lab. „Pokud ale stávající verze Kido budou nahrazeny jeho poslední variantou, výrazně to zkomplikuje situaci všem, kdo se proti autorům tohoto škodlivého programu snaží bojovat."

Trojský kůň Kido funguje i jako downloader, což znamená, že do nakaženého počítače stahuje a instaluje další škodlivé programy. První infekce Kido byly zaznamenány v listopadu loňského roku. Záznam o nových variantách trojského koně Kido byl do antivirových databází společnosti Kaspersky Lab přidán v sobotu 7. března 2009.

Společnost Kaspersky Lab všem uživatelům znovu doporučuje nainstalovat si příslušné aktualizace zabezpečení operačního systému (**www.microsoft.com/technet/security/Bulletin/MS08-067.mspx**). Prevencí proti infekci je také antivirové řešení s aktualizovanými databázemi definic a správně nakonfigurovaným firewallem. Uživatelé, kteří si nainstalovali aktualizaci zabezpečení vydanou Microsoftem, jsou proti trojskému koni Kido plně chráněni.



Pravý nebo falešný: Kromě pravých nástrojů (na obrázku) na odstranění hrozby se vyrojilo i mnoho falešných pomocníků.

Komentář redakce: *Zajímavým důsledkem rostoucí nebezpečnosti hrozby skrývající se pod označením Kido je i nárůst počtu falešných nástrojů na její odstranění.*

Samotný malware funguje takto. Poté, co se červ do počítače dostane, spustí se proces „SERVICES.EXE", který vytvoří HTTP server, resetuje bod obnovy a pokusí se vypnout antivirové nástroje. Nakonec stáhne z vybraných serverů nové škůdce…

STATISTIKA NAVRCHOLU.CZ

Rozlišení monitorů se zvyšuje

Ještě v květnu roku 2008 byl podíl dvou nejpoužívanějších rozlišení obrazovek počítačů, 1 024 × 768 pixelů a 1 280 × 1 024 pixelů, prakticky vyrovnaný. Činil přibližně 40 %, což v porovnání s daty z ledna 2006 znamenalo výrazný posun směrem k vyššímu rozlišení obrazovek. Do té doby totiž na českých počítačích převládalo s téměř 60% podílem rozlišení 1 024×768 pixelů. Z aktuálních statistik služby pro sledování návštěvnosti Navrcholu.cz z ledna 2009 je jasně patrný další posun směrem k vyšší kvalitě rozlišení obrazovek.

Trend postupného zvětšování obrazovek je zřejmý i z dalších čísel, například rozlišení 1 400 × 1 050 pixelů již využívá téměř 7 % sledovaných návštěv a rozlišení 1 600 × 1 200 a vyšší pak více než 9 %.

PRÁCE NA WEBU

Nový personální server

Společnost Monster, která je světovou jedničkou na on-line trhu práce, spustila v lednu nově vytvořený pracovní portál, a to ve 24 zemích po celém světě včetně České republiky. Na internetových stránkách **www.monster.cz** mohou zájemci využít nové zajímavé služby, které jsou okamžitě k dispozici všem uživatelům i zaměstnavatelům. Jedná se zejména o personalizovanou stránku Můj Monster, vylepšenou službu Správa životopisů a rozšířené služby Hledání nabídek práce a Správa pracovních míst. Monster připravil nové a zdokonalené služby také pro zaměstnavatele a personální agentury. Těm propracovaný systém umožní najít více vhodných kandidátů na obsazení konkrétní pozice, a to díky důmyslnému zacílení podle oborů či regionů a sdílení mezinárodní databáze uchazečů z více než 61 zemí.

HP TOUCHSMART ALL-IN-ONE

Dotykový počítač HP na českém trhu

Jako „společníka pro domácí zábavu“ prezentuje firma HP svůj zajímavý dotykový počítač TouchSmart All-in-One. Nabízí přirozené uživatelské rozhraní – fotografie, video, filmy, hry, televize nebo internet se spouští a ovládají dotykem prstu. Prostřednictvím 22palcového dotykového displeje v širokoúhlém provedení vše přehledně zobrazíte, například jako dlaždice nebo vějíř. „Sáhnout“ si můžete i na ostatní funkce, kterými touchsmart disponuje: videa, poznámky, kalendář, hodiny, RSS a mnoho dalších. Počítač je založen na technologii Intel (Core 2 Duo), je vybaven 500GB diskem a obsahuje také webkameru s mikrofonem, čtečku media karet, dva USB porty, zdířku pro sluchátka, bezdrátovou klávesnici, dálkový ovladač TV, výkonné reproduktory a také bezdrátovou síťovou kartu. Model HP TouchSmart IQ522 PC se v České republice prodává za doporučenou cenu 36 990 Kč vč. DPH. Dodává se však bohužel jen s anglickým rozhraním.

INFO: **www.hp.cz**

NETGEAR WNDR3700

Špičkový domácí router

Model WNDR3700 je gigabitový dvoupásmový směrovač řady RangeMax Wireless-N, využívající současně dvě různá frekvenční pásma – 2,4 GHz a 5 GHz. Jedná se o první produkt značky Netgear v designovém provedení páté generace. Obsahuje USB rozhraní pro připojení externího USB úložného zařízení a porty gigabitové LAN pro vysokorychlostní datový přístup hned několika počítačů v domácí síti.

Vnitřní výbava směrovače, zahrnující 680MHz MIPS procesor, vysoce výkonný zesilovač a osm ultracitlivých metamateriálových antén, zaručuje maximální bezdrátový výkon i pokrytí. K dalším vlastnostem patří energeticky úsporný „green“ přepínač se čtyřmi ethernetovými porty, QoS pro bezdrátové streamování videa, samostatná tlačítka pro vypnutí bezdrátové části i celého zařízení či možnost regulace výkonu pro dokonalou optimalizaci spotřeby energetické energie. Díky funkci Push 'N' Connect, využívající standardu Wi-Fi Protected Setup (WPS), lze navíc snadno připojit další bezdrátová zařízení.

INFO: **www.netgear.cz**

SAFARI 4 BETA

Nejrychlejší prohlížeč?

Apple zpřístupnil první beta verzi webového prohlížeče Safari 4. Ta přináší nové javascriptové jádro a podporu nejnovějších webových standardů. Podle výsledků benchmarkových testů iBench a SunSpider je nový javascriptový engine s názvem Nitro až 4,2krát rychlejší než v předcházející verzi prohlížeče. Co se týká porovnání rychlosti JavaScriptu s ostatními prohlížeči, Safari 4 beta vede nad Internet Explorerem až 30násobně.

Mezi další zajímavé vlastnosti nového Safari patří například funkce TopSites, která uživatelům poskytne vizuální náhled na často navštěvované stránky. Vývojáři nezapomněli ani na zlepšení správy záložek a podporu CSS 3.

INFO: **www.apple.com/safari**

OLYMPUS

Unikátní fotografie Země

K výročí devadesáti let od svého založení si společnost Olympus připravila dárek: Olympus Vesmírný projekt. Při této příležitosti bude Koichi Wakata, japonský astronaut z Japanese Aerospace Exploration Agency (JAXA), vybaven digitální zrcadlovkou Olympus E-3 a objektivy Zuiko Digital, aby pořídil záběry planety Země z vesmíru. Obrázky pořízené z japonského experimentálního modulu Kibo při Mezinárodní vesmírné stanici (MVS) budou umístěny na webových stránkách firmy Olympus a představeny na fotografických výstavách. Na Mezinárodní vesmírnou stanici přenese Dr. Wakatu a jeho E-3 při svém startu raketoplán Discovery.

INFO: **www.olympus.cz**

SLUNEČNICE.CZ

Co se stahuje

Nejoblíbenějším softwarem v kategorii Hry ke stažení byla na serveru Slunečnice.cz v lednu 2009 demoverze simulátoru skutečného života The Sims 2. Potvrzuje to mnohaletý úspěch hry The Sims, která se brzy po svém vydání dostala na přední příčky herních prodejních žebříčků a vytvořila si silnou základnu svých příznivců. Hráči v ní mohou ovládat vybranou postavu, tzv. „simíka“, po celou dobu jejího života, určit, jak bude žít, kde bude pracovat, co ji bude bavit, a díky mnoha doplňujícím datadiskům dále rozšiřovat herní prostředí a možnosti.

Druhým nejčastěji stahovaným programem byl Moorhuhn Wanted. Jedná se o nenáročnou střílečku na slepice, odehrávající se na Divokém západě, která zaručuje příjemné odreagování. Verze Moorhuhn 3 se umístila na slušné deváté pozici. Bronzovou příčku získal realistický simulátor automobilových závodů Life for Speed.

ROZŠÍŘENÍ

DVD standard nyní obsahuje 3D

Je starší, a přesto rychlejší: Ještě předtím, než byl standard Blu-ray přizpůsoben pro třírozměrné filmy, DVD fórum rozšířilo DVD standard o 3D. Poté, co konsorcium porovnalo systémy různých výrobců, rozhodlo se pro technologii firmy Sensio. Technologii Sensio 3D lze využít ve spojení s téměř všemi DVD přehrávači, které umožňují výstup v půlsnímcích (interlacing, prokládané video). Dodatečné informace jsou ukryty v datovém DVD streamu, dekodér Sensio při přehrávání vypočítá příslušné obrazy pro pravé a levé oko. Následuje výstup nezávislý na zařízení: Sensio 3D je možné používat se současnými monitory, televizory a projektory se 100hertzovou technologií, a to pomocí zatmívacích nebo vícebarevných brýlí. Podporována jsou navíc autostereoskopická zobrazovací zařízení. Dosud je dostupných téměř čtyřicet DVD s novou technologií.

INFO: **www.sensio.tv**

INTERNETOVÁ TELEFONIE

Skype: Lepší kvalita audia

Vývojáři nové verze Skype 4.0 slibují vyšší kvalitu. Mimo jiné pracovali na kvalitě komprese audia. Nový kodek má být lépe přizpůsoben pro současně dostupné šířky pásma. Při videochatu je také zobrazen zjevně větší obraz ve vyšší kvalitě. Výkonnější je i rozpoznávání headsetů, webových kamer a mikrofonů, což má především začátečníkům usnadnit práci s programem. Kromě toho bylo kompletně přepracováno uživatelské rozhraní. Nástroj nyní sjednocuje různá okna pro kontakty a komunikaci. Uživatelé, kteří nechtějí používat nový vzhled programu, mohou jednoduše přepnout na starou podobu předcházejících verzí.

INFO: **www.skype.com**