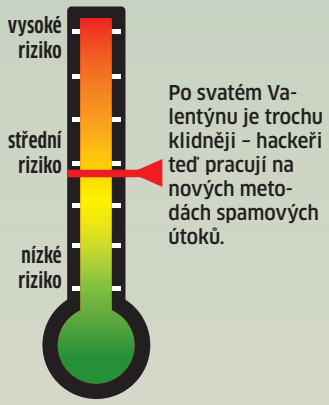
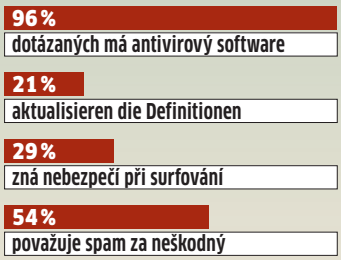
DATA A FAKTA

Barometr nebezpečí
v březnu:



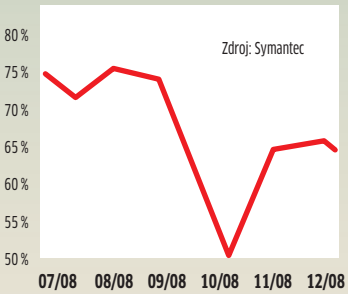
Po svatém Valentýnu je trochu klidněji – hackeři teď pracují na nových metodách spamových útoků.

Bezpečnostní anketa



Velká většina uživatelů používá bezpečnostní software, jen malá menšina si však instaluje jeho aktualizace.

Boj proti reklamě
Podíl spamu



Vypnutí nepomohlo: V listopadu 2008 úřady odpojily jeden z hlavních spamových serverů od sítě – o čtyři týdny později už pracoval náhradní.

Číslo měsíce

215

milionů eur ročně vydělají kyberzločinci obchodem s ukradenými daty na internetu.

Kovářova kobyla

Webové prezentace úřadů a výrobců antivirového softwaru lze **SNÁZE ZMANIPULOVAT** než většinu soukromých počítačů v domácnostech.

FABIAN VON KEUDELL

Kdo chce mít bezpečný počítač, musí si nainstalovat dobrý antivirový skener a hlavně důsledně nahrávat vydávané aktualizace. Co platí pro soukromé uživatele, to by si tím spíše měly vzít k srdci velké firmy. Jenomže uplynulé týdny prokázaly pravý opak. Právě podniky, které by se v této problematice měly vyznat nejlépe, si počínaly ledabyle – a brzy dostaly za vyučenou: výrobci antivirů Kaspersky, BitDefender a F-Secure se teď stali oběťmi hackerského útoku. Tyto firmy prostě zapomněly zabezpečit své webové stránky. K napadení využili hackeři bezpečnostní mezeru metodou „SQL injection". Při ní vkládají do běžné vstupní masky na webových stránkách speciální úseky kódu dotazovacího jazyka SQL. Ty pak jako odpověď vrátí přístupové informace a e-mailové adresy zákazníků. Útoky pomocí SQL nejsou nic nového – většina webových stránek už je dnes proti takovému napadení chráněna a hackerské příkazy odfiltruje. U dvou webových stránek antivirových firem však byly příslušné filtry chybně implementovány. Kaspersky dementoval, že by se důležitá zákaznická data dostala do cizích rukou – hackeři však tvrdí opak. Také BitDefender veřejnost chlácholí: napadená stránka prý patří resellerovi – který ovšem pracuje jménem firmy. Jenom firma F-Secure dokázala přiznat, že útok byl mimořádně trapnou záležitostí.

Stydět se však nemusí jen antivirové firmy, ostudu si udělali i politici na západ od našich hranic. Lépe by si měl svou webovou stránku chránit například německý ministr vnitra. Využitím mezery v databankovém systému Typo3, který se na ministrově stránce používá, dokázali hackeři převzít kompletní kontrolu nad stránkou. Hackerští aktivisté tak na hlavní stránku nainstalovali odkaz, který vedl na stránku protestující proti zaznamenávání a archivaci veškeré komunikace. Málo svědomitý správce ministerské stránky na to však nijak nereagoval a na webu ji ponechal. Teprve když tam hackeři nahráli výzvu k aktualizaci na poslední verzi, správce procitl a stránku vypnul.

Jak by asi podobný výzkum dopadl u nás, kde má většina politiků k internetu podobný vztah jako ke kurdějím a černému moru?

Aktualizace softwaru: Řešení je známé, ale nikdo je nevyužívá

Záplaty, které chrání proti SQL útokům a mezerám v Typo3, jsou k dispozici už řadu týdnů. Chcete-li tedy mít svůj domácí počítač zabezpečen lépe než webové servery bezpečnostních firem a německého ministerstva vnitra, vždy instalujte aktuální Windows Updates.

INFO: www.microsoft.cz

NOVÝ SOFTWARE

Komplexní ochrana

Společnost Symantec představila řešení počítačové bezpečnosti Norton 360 ve verzi 3.0 – kompletní bezpečnostní řešení, chránící osobní počítač i všechny typy on-line aktivit. Nyní i tento komplexní bezpečnostní balík přichází s rychlostí, která je charakteristickým rysem rodiny produktů Norton 2009. Průměrná doba instalace produktu Norton 360 se pohybuje kolem minuty, paměti je využito méně než 10 MB. Norton 360 rovněž využívá dvě technologie známé z Norton Internet Security 2009: technologii pulzních aktualizací každých 5–15 minut a technologii Norton Insight, která díky databázi důvěryhodných souborů výrazně zrychluje kontrolu počítače. A jaké další novinky produkt nabízí?

Norton Safe Web

Služba Norton Safe Web je navržena pro zvýšení bezpečnosti práce v prostředí internetu, ať jde o prohlížení stránek, vyhledávání, nákupy, nebo komunikaci. Vzhledem k nebezpečnosti dnešních on-line hrozeb dokáže Norton Safe Web informovat návštěvníka stránek o hrozbách ještě předtím, než na danou stránku přejde. Obsah téměř 60 % stránek, které jsou službou Norton Safe Web označeny jako nebezpečné, dokáže domácí počítač infikovat bez nutnosti stáhnout si z nich či instalovat jakékoli soubory. Norton Safe Web nabízí aktuální a přesné hodnocení stránek. Servery Symantec nepřetržitě analyzují bezpečnost webových stránek unikátním algoritmem Intelligent Aging Algorithm a zároveň využívají poznatky získané dvacetimilionovou komunitou Norton Community Watch.

Ochrana identity a zálohování

K technologiím, jako je Norton Insight, a k zabezpečenému jádru přistupuje technologie Norton Identity Safe, sloužící k zabezpečení, ukládání a správě osobních dat – přihlašovacích jmen a hesel. Tím se zvyšuje komfort i bezpečí při on-line nakupování, využívání internetového bankovnictví a celkově při procházení internetem a zabraňuje se v činnosti škodlivých kódů, jako jsou keyloggery, sloužících ke shromažďování osobních informací. Další novinkou je Norton Backup Drive. Tento nástroj nabízí v intuitivním rozhraní podobném Průzkumníku Windows snadnou správu zálohování. Navíc je možné zálohovat soubory na různá cílová zařízení, jako jsou USB klíčenky, iPod, CD/DVD, Blu-ray média nebo zabezpečené on-line úložiště. Uživatelé Nortonu 360 mohou využívat volně dostupnou podporu na webu, po telefonu i elektronickou poštou, a to i v češtině. V angličtině je dostupné rovněž Norton Users Discussion Forum, které slouží pro výměnu informací a zkušeností mezi uživateli, zaměstnanci Symantecu a dalšími diskutujícími. Norton 360 je v České republice dostupný od 1. dubna 2009, doporučená cena pro koncového uživatele s roční podporou činí 1 859 Kč. Standardní edice Norton 360 obsahuje 2 GB dat na zabezpečeném on-line úložišti s možností dokoupit další prostor. Podrobněji se na novinku podíváme v příštím Chipu.

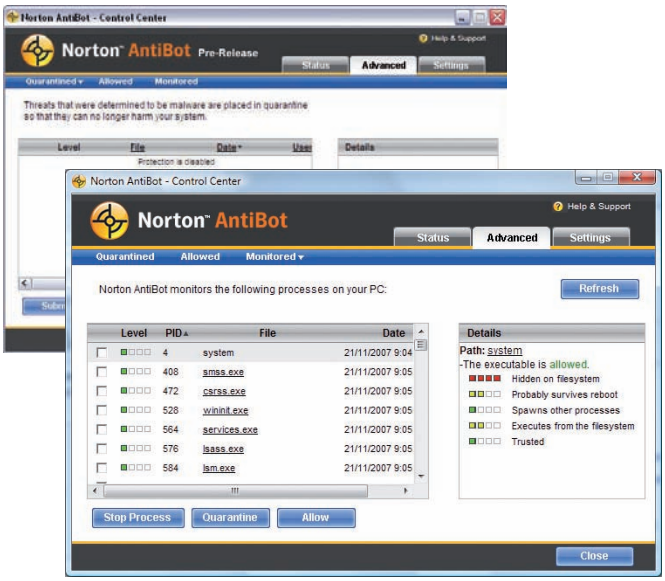
VIZE SYMANTECU

Technologie budoucnosti

V našem článku o antivirových technologiích (najdete ho na straně 64) jsme vám představili většinu taktik, které AV firmy používají v boji proti hrozbám. Firma Symantec nedávno představila další dvě nové technologie, které pomohou zvrátit skóre v souboji na stranu uživatelů: DeepClean a VIBES (Virtualization-Based Endpoint Security).

Zabezpečení na základě pověsti

Technologie DeepClean, kterou vyvinula skupina SRL Advanced Concepts, je technologie vytváření seznamů povolených položek na základě pověsti. Zákazníkům má pomoci vyhodnotit rizika a ohrožení ze strany rychle se objevujících nových hrozeb v době, kdy se nový škodlivý kód objevuje tak často jako nikdy předtím. Technologie DeepClean využívá a rozšiřuje síť Symantec Global Intelligence Network pro potřeby vytváření a udržování přesné a komplexní infrastruktury seznamu povolených položek a pověsti souborů a poskytovatelů. Technologie DeepClean využívá seznamy povolených položek a analýzu pověsti a doplňuje k nim stávající metody, jako jsou signatury, heuristika a seznamy zakázaných položek. To jí umožňuje zjišťovat současné nové hrozby z internetu a různé typy cílených útoků.



Jiná ceta: **Jednu z nejlepších experimentálních technologií pro boj proti malwaru nabídl v loňském roce Symantec pod jménem AntiBot. Tuto technologii v roce 2007 koupil od firmy Sana Security..**

„Tato novátorská technologie byla navržena jako řešení požadavků na škálovatelnost a rychlost, které jsou nutné při použití v podnikových prostředích s minimálními možnostmi správy," řekl Joe Pasqua, viceprezident Symantec Research Labs společnosti Symantec. „Technologie DeepClean se nasazuje jako monitor podnikového perimetru a prostřednictvím zabezpečeného privátního webového portálu poskytuje správcům IT zprávy hodnocení rizik. Každý soubor má hodnocení pověsti, které pomáhá roztřídit legitimní a nebezpečné soubory. Výsledkem je možnost daleko komplexněji hodnotit rizika u jakýchkoli souborů i při neustálém výrazném zvyšování objemu a rozmanitosti cílených útoků," dodal.

Zabezpečení koncových bodů založené na virtualizaci (VIBES)

Technologie VIBES je inovace vyvinutá skupinou Symantec Research Labs Core Research. Technologie VIBES využívá k ochraně koncových uživatelů technologii virtualizace. Zabraňuje krádeži citlivých dat zadaných v transakcích on-line a zmírňuje rizika spojená se spuštěním nebezpečného obsahu staženého z internetu. Tato nová metoda transparentně vytváří několik izolovaných virtuálních provozních prostředí, přičemž každé má vlastní úroveň důvěryhodnosti. Tím podstatně zvyšuje zabezpečení prohlížeče, protože uživatelům umožňuje transparentně používat různá virtuální provozní prostředí k provádění různých webových transakcí. V současném prototypu technologie VIBES existují tři virtuální provozní prostředí:

Ve virtuálním počítači „Uživatel" se provádějí běžné každodenní činnosti.

V „Důvěryhodném" virtuálním počítači se provádějí důvěryhodné operace, například zadávání citlivých pověřovacích údajů.

Ve virtuálním počítači „Hřiště" se provádějí riskantnější, nedůvěryhodné činnosti, například navštěvování neznámých webových stránek nebo stahování neznámých aplikací.

„Technologie VIBES má jedinečnou schopnost automaticky zvolit nejvhodnější virtuální provozní prostředí pro daný scénář interakcí prohlížeče a úplně skrýt použití virtualizace před koncovými uživateli," řekl Pasqua.

INFO: **www.symantec.com**

Kyberzločinci zrychlují tempo

Podle výroční zprávy Trend Micro Threat Roundup & 2009 Forecast sice v minulém roce **STOUPALO VYUŽITÍ MALWARU** bezprecedentní rychlostí i objemem, rok 2009 však zřejmě přinese zvýšenou spolupráci dodavatelů bezpečnostních řešení a právních organizací s cílem omezit činnost zločineckých struktur.

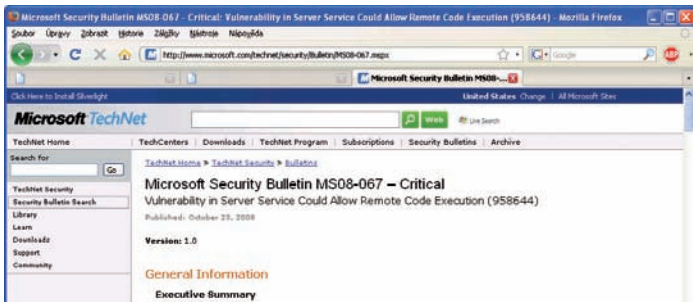
I když autoři malwaru pracovali vždy velmi rychle a uvolňovali škodlivý kód okamžitě po objevení zranitelnosti, experti Trend Micro zabývající se hrozbami zaznamenali v roce 2008 ještě rychlejší využívání malwaru než kdy před tím. Částečně k tomu přispěly modely a architektury hrozeb provozované v prostředí internetu („in-the-cloud"), které kyberzločinci znovu využívali k ziskům, a využití internetu jako hlavního prostředku k šíření malwaru. Z hlediska bezpečnostního odvětví to znamená, že tradiční metody ochrany jsou neúčinné. Společnost Trend Micro odpověděla v roce 2008 tím, že přenesla bitvu se zločinci do internetu, takže hrozby jsou zastaveny dříve, než mohou uškodit.

Většina těchto hrozeb je šířena přes internet, takže oběťmi se mohou stát všichni, kdo surfují po webu.

Přehled událostí roku 2008

V roce 2008 se prosadily takové hrozby, jako malware měnící servery DNS (Domain Name Server), který je schopen přesměrovat prakticky jakýkoli počítač na jakoukoli webovou stránku. Kyberzločinci si v roce 2008 také oblíbili možnost zneužití prohlížečů, zejména Microsoft Internet Exploreru. Další útoky byly vedeny i proti jiným prohlížečům – všechny byly provedeny rychle a utajeně ještě před tím, než byli jejich výrobci schopni vydat patřičné opravy. Během roku 2008 došlo také k výraznému nárůstu malwaru pro krádeže dat. Tento malware bývá obvykle spuštěn pomocí trojského koně a jeho hlavním cílem je odcizit citlivá data z uživatelských PC, odeslat je zpět do botnetu nebo jiných zločineckých struktur buď pro další využití, nebo na prodej na digitálním černém trhu.

Nejvíce spamu (22,5 %) se stále vyskytuje ve Spojených státech; nejvíce „prospamovaným" kontinentem je Evropa. V Číně došlo v roce 2008 ke zvýšení na 7,7 %, ve srovnání s 5,23 % či méně v Rusku, Brazílii a Jižní Koreji. Od ledna do listopadu 2008 bylo 34,3 milionu PC infikováno boty, softwarovými programy, které umožňují ovládání PC na dálku jiným subjektem. K největšímu tříměsíčnímu nárůstu došlo během června až srpna, kdy počet infekcí stoupl o 476 procent. V listopadu 2008 skupina bezpečnostních expertů odhalila jeden z největších zdrojů spamu – firmu McColo Corporation ze San José. Odborníci Trend Micro očekávají, že dojde k dalším podobným společným akcím bezpečnostní komunity s cílem odhalit a zneškodnit kybergangy.



Příčina a následek: Na mnoha počítačích chybí i staré záplaty, což znamená zelenou pro šíření červů. Tahle byla vstupenkou pro Conficker...

2009: Výhled do budoucnosti

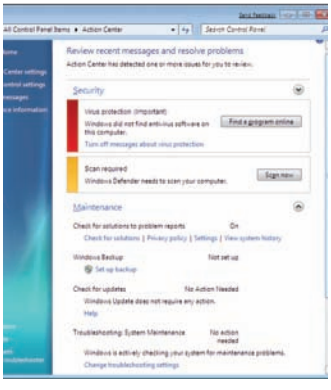
Naděje na peněžní zisky bude i nadále hlavní motivací tvůrců nového malwaru. Novým fenoménem jsou propracované kombinované hrozby. Aby se webové hrozby snáze vyhnuly odhalení, budou zahrnovat více různých prostředků a forem. Kvůli tomu, že tvůrci malwaru budou v tomto roce i nadále využívat nejlepší dostupné nástroje, budou jimi vyvinuté hrozby využívat nejnovější triky a techniky, jako je například trojský kůň měnící DNS. Ve druhé polovině se dá očekávat rozmach

MICROSOFT

Napadená Windows

Finální verze Windows 7 bude na trhu až začátkem příštího roku, ale bezpečnostní mezery vykazuje už nyní. V aktuální beta verzi se hackerům podařilo pomocí jednoduchého skriptu vyřadit nástroj Řízení uživatelských účtů (UAC). Počínaje verzí Vista pracují uživatelé Windows jen s omezenými právy; kdo chce instalovat programy nebo měnit systémová nastavení, musí nejprve potvrdit ověřovací zprávu UAC. K tomu však docházelo tak často, že to zdržovalo provoz, a Microsoft se proto rozhodl rigidní nástroj „zkrotit". Bohužel však až příliš, jak se nyní ukázalo: jednoduchý skript dokáže Řízení uživatelských účtů bez varovného hlášení kompletně vypnout. Po následném restartu pak každý uživatel pracuje na počítači s oprávněním správce. Do vydání finální verze Windows 7 chce ale Microsoft Řízení uživatelských účtů ještě podstatně vylepšit.

INFO: www.microsoft.cz



Windows 7: Na bezpečnosti se stále pracuje, ale hackeři na finální verzi nepočkají...

ZPRÁVA ESETU

Conficker trucuje a mlčí

Bublina splaskla. I tak by se dal označit poslední vývoj u největší mediální hvězdy na poli virů. Podle zprávy společnosti Eset přestal Conficker komunikovat s doménami, komunikuje jen ve své peer-to-peer síti. Tato nová verze červa je označována jako Win32/Conficker.AQ. A jak to začalo? ESET zachytil novou verzi červa Conficker, která se od předešlých variant liší v jedné podstatné, ale o to překvapivější vlastnosti. Nekontaktuje žádnou z řídicích domén, i když původně jich bylo až 50 000 denně (mediální zájem vyvolal Conficker i díky velikost jeho botnetu – síti infikovaných počítačů). Nová varianta Confickeru, která vznikla teprve 7. dubna 2009, komunikuje už pouze v rámci své sítě. Skládá se ze dvou hlavních komponent. Serverová část infikuje zranitelné počítače v síti, přičemž na ně instaluje svoji klientskou část. Takto napadené počítače se stanou součástí botnetu červa Conficker. Zajímavostí, kterou autoři červa vložili do jeho kódu, je, že po 3. květnu 2009 se serverová část automaticky deaktivuje a odstraní z počítače. Botnet však bude existovat i po tomto termínu a Conficker zůstane i nadále jednou z nejrozšířenějších aktuálních hrozeb. Tak jako všechny předcházející varianty i Win32/Conficker.AQ zneužívá zranitelnost MS08-067 operačního systému Windows. Doporučujeme mít záplatovaný počítač a používat bezpečnostní software.

INFO: www.eset.cz

v nasazení ransomwaru (softwaru pro vymáhání výkupného) se zaměřením na malé a střední podniky spíše než na jednotlivé domácí uživatele. Zranitelné budou zejména společnosti s omezenými rozpočty, od kterých si kyberzločinci budou slibovat vysoké výpalné. Malé a střední podniky jsou totiž dostatečně velké na to, aby mohly platit výpalné, ale na druhou stranu nejsou dost velké, aby mohly účinně bojovat s hrozbami zničení jejich IT nebo dlouhých výpadků.

Zvýší se počet útoků na počítače Mac

S tím, jak roste tržní podíl počítačů Mac, které se obvykle neprodávají s antivirovými aplikacemi, dostanou se tyto počítače do hledáčku kyberzločinců. Nedávný malware cílený na uživatele počítačů Mac pocházel ze spamu a měl podobu videoaplikace. Pokud uživatelé klikli na odkaz, aby si prohlédli video, byl jejich počítač infikován malwarem. Poroste i počet hrozeb využívajících chyby v dalších alternativních operačních systémech, zejména s nárůstem popularity Linuxu (díky rozmachu trhu s netbooky). Microsoft zůstane věčným cílem a bude mít problémy i v roce 2009. Testovací malware prověří Microsoft Windows 7, Surface, Silverlight a Azure. Kyberzločinci budou tyto systémy napadat stále profesionálněji s cílem narušit harmonogram oprav plánovaných vždy na první úterý v měsíci.

Války mezi kybergangy se dostanou na titulní strany novin

Bezpečnostní experti očekávají války virů, červů a botnetů – kvůli rostoucí konkurenci gangů hledajících finanční zisky z phishingu a podvodů a zároveň kvůli zmenšování těchto gangů a zlepšování bezpečnostních řešení. Největší šance budou mít gangy z východní Evropy a Číny. Mnoho hrozeb, se kterými se setkáváme v reálném světě, se objevuje i ve světech virtuálních. Kyberzločinci své zločiny cílí na masy – proto obracejí svou pozornost i na obyvatele virtuálních světů a na hráče on-line her, zejména v Asii, kde se tyto hry staly nesmírně populárními.

Vzroste počet problémů s DNS systémy. Podle odborníků zločinci již dnes využívají tzv. otrávené DNS systémy k vytváření tajných komunikačních kanálů, obcházení bezpečnostních opatření a rozesílání škodlivého obsahu. Třebaže bezpečnostní komunita včetně společnosti Trend Micro (pokud je to možné) úzce spolupracuje s registrátory domén, jde o problém, který musí řešit organizace ICANN (Internet Corporation for Assigned Names and Numbers).

Podzemní ekonomika jen kvete

Nárůst malwaru určeného ke krádežím informací znamenal zvýšení počtu případů krádeží přihlašovacích údajů a informací o bankovních a kreditních kartách. Zároveň se rozvíjí podzemní trh s nebezpečnými aplikacemi i aukční webové stránky, na nichž se draží malware. Zákony, které řeší problematiku krádeží identit, přijalo jen málo zemí, takže krádeže identit budou nic netušící oběti trápit i v roce 2009. Podle centra ITRC (Identity Theft Research Center) dosáhl v roce 2008 počet případů datových úniků svého nového vrcholu.

Objem spamu dále poroste

95 % všech e-mailů obsahuje spam. Každodenně je rozesláno okolo 115 miliard zpráv se spamem, přičemž téměř všechny pocházejí ze zneužitých počítačů. V letech 2005 až 2006 přitom šlo průměrně o 75 miliard. Spam je množstevní záležitost – čím více rozeslaného spamu a čím lepší metody sociálního inženýrství, tím větší je šance, že uživatelé kliknou na odkaz ve zprávě.

Celou zprávu najdete na adrese **http://trendmicro.mediaroom.com/index.php?s=65&item=383**.

NOVÉ PRODUKTY ESETU

Smart Security 4 a NOD32 Antivirus 4

Společnost ESET představila novou generaci svých bezpečnostních řešení, zajišťujících ochranu proti novým hrozbám. Aplikace ESET Smart Security 4 a ESET NOD32 Antivirus 4 jsou postaveny na vylepšené technologii ThreatSense. Uživatelé verze 3 obou produktů si mohou novou generaci antivirových řešení ESET nainstalovat zdarma, a to okamžikem uvolnění instalačních balíčků na www.eset.cz. „Aplikace ESET Smart Security 4 je výsledkem trvalého úsilí společnosti ESET nalézt řešení bezpečnosti počítačů.
Klíčovými vlastnostmi nové generace produktů ESET jsou:
► ochrana před neznámými hrozbami – technologie ThreatSense, která zajišťuje ochranu před novými útoky;
► rychlost – řešení společnosti ESET jsou rychlá a zajišťují vysoký výkon skenování systému;
► systémová nenáročnost – antivirová řešení využívají pouze 36–40 MB systémové paměti;
Domácí uživatelé, ale i malé a střední podniky a velké firmy ocení také nové funkce a uživatelská vylepšení.

SelfDefense

Vylepšená technologie sebeobrany. Software ESET obsahuje vylepšenou obranu proti vypnutí antivirového systému malwarem nebo neautorizovanými uživateli mimo jiné díky omezení změn procesů ESETu a zaznamenávání vstupů autorizovaných uživatelů.

ESET SysRescue

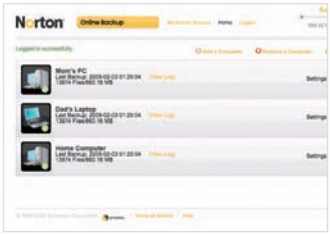
ESET SysRescue umožňuje uživatelům mnohem rychleji diagnostikovat a obnovit napadené systémy. Klient si vytvoří své vlastní záchranné CD, které může být použito pro vyčištění a obnovení systému napadeného malwarem, aniž by přitom došlo k přepsání celého systému.
V příštím Chipu se na novinku od Esetu podíváme podrobněji...

SLUŽBA SPOLEČNOSTI SYMANTEC

Norton Online Backup

Společnost Symantec, výrobce bezpečnostního softwaru Norton, oznámila dostupnost zabezpečené služby zálohování on-line Norton Online Backup.

Prostřednictvím jediného centrálního vzdáleně přístupného účtu lze bezpečně zálohovat, spravovat a obnovit až pět počítačů v domácnosti. Uživatelé služby Norton Online Backup mají také snadný přístup k souborům podle potřeby doma, v práci nebo ve vzdálené internetové kavárně během cesty. Řídicí panel chráněný heslem zjednodušuje správu zálohování. Zákazníkům kdykoli a kdekoli umožňuje správu



Rychlé a snadné: Kromě firem může díky příznivé ceně služba zaujmout i domácí uživatele.

a přístup ke všem jejich záložním souborům a jejich obnovení z libovolného podporovaného prohlížeče internetu.

Podle nedávného průzkumu provedeného společností Harris Interactive se respondenti obávají ztráty všech dat, která mají v počítači, jako jsou fotografie, hudba a dokumenty, více než kontroly finančního úřadu. Přesto si byla pouze polovina respondentů jistá, že důležité soubory zálohují správně. Ti, kdo zálohují na externí média nebo pevné disky, jsou navíc nadále vystaveni riziku selhání disku, krádeže, ztráty nebo přírodní katastrofy. Služba Norton Online Backup zaručuje, že nikdy nedojde ke ztrátě cenných souborů, protože automaticky ukládá kopie každého zálohovaného a zašifrovaného souboru na samostatné, zabezpečené a profesionálně spravované replikované servery.

Hlavní rysy služby Norton Online Backup:

- Zabezpečení souborů proti ztrátě dat, poškození a jiným nehodám.
- Zajištění rychlého přístupu k souborům z libovolného počítače s přístupem na web, včetně obnovení ztracených nebo odstraněných souborů.
- Slouží jako centrální a zabezpečené úložiště všech fotografií a souborů z různých počítačů.
- Provádí automatické zálohování v době nečinnosti nebo podle uživatelem definovaného plánu.
- Poskytuje úložiště on-line o velikosti 25 gigabajtů (GB), což je přibližně prostor, který umožňuje uložení více než 6 000 skladeb, 7 000 digitálních fotografií, 100 hodin videa nebo 200 000 tabulek či dokumentů…
- Zrychluje přenosy pomocí pokročilé komprese dat a přírůstkových záloh na úrovni bloku.
- Nabízí vzdálenou správu nastavení zálohování z libovolného počítače s přístupem na web.
- Přenosy všech souborů jsou zabezpečené šifrováním na vysoké úrovni.

Cena a dostupnost na trhu

Službu Norton Online Backup je možno zakoupit prostřednictvím obchodu společnosti Symantec on-line na adrese **www.symantecstore.com** a prostřednictvím různých maloobchodů a on-line. Doporučená maloobchodní cena služby Norton Online Backup je 49,99 USD ročně. Zahrnuje úložiště on-line o velikosti 25 GB. Další úložný prostor je možno zakoupit v přírůstcích po 10, 25, 50 nebo 100 GB.

Komentář redakce: *Ukládání dat na webu je hitem letošního roku – na rozdíl od pevných disků a DVD médií může skutečně nabídnout bezpečí a přístupnost. Nabídka Symantecu má ale šanci zaujmout především firmy – na počátku března se na našem trhu totiž objevila poměrně silná konkurence. Známá firma Humyo u nás už pár týdnů nabízí obyčejným uživatelům zdarma prostor o velikosti 20 GB, což je pro většinu uživatelů více než dostatečné. Ve světě firem se ale karta částečně obrací. Humyo sice nabízí prostor o velikosti minimálně 100 GB, za rok za něj však zaplatíte minimálně 80 USD.*

INFO

Nová bezpečnostní rizika

MICROSOFT POWERPOINT

Nebezpečná zranitelnost byla zjištěna v aplikaci Microsoft PowerPoint. Ta kvůli blíže nespecifikované chybě umožňuje přístup k paměti při otevření upraveného souboru pro PowerPoint. Chyba může být zneužita ke spuštění libovolného kódu. Zranitelnost je hlášena jako 0-day, je tedy zneužívána a v současné době na ni neexistuje patch. Jediným doporučením tak zůstává „klasické“: Neotvírejte soubory z neznámých zdrojů. Zasaženy jsou Microsoft Office a PowerPoint verze 2000, 2003, 2004 for Mac, XP a Microsoft PowerPoint 2000, 2002 a 2003. Více informací naleznete na webu Microsoftu **(http://www.microsoft.com/technet/security/advisory/969136.mspx)**. Doplnění: Pro firemní prostředí navrhuje Microsoft prozatím použít script do registrů, který nastaví tzv. File block policy a zablokuje příslušné soubory. Nechybí ale také poznámka, že úpravu registrů provádíte jen „na své riziko“…

INFO: zprávy.actinet.cz

AVG TECHNOLOGIES

Nové výzkumné centrum

Společnost AVG Technologies otevřela v Brně mezinárodní výzkumné centrum AVG Malware TRAP Centrum, zkráceně M-TRAP, kde TRAP znamená Trending, Reporting, Analysis, and Prevalence. Jeho úkolem bude shromažďovat a poté analyzovat informace o škodlivých programech (malwaru) a jejich šíření na internetové síti. Náklady na unikátní pracoviště se pohybují zhruba ve výši 10 milionů korun. První výsledky by měly být k dispozici během měsíce května až června. Potřebná data získá nové centrum prostřednictvím více než 80 milionů uživatelů antivirového programu AVG.

„M-TRAP bude hledat vzájemné souvislosti a způsoby, jak vyvinout ještě lepší metody detekce a prevence šíření škodlivých kódů. Výsledky výzkumu využijeme při vývoji nových technologií pro efektivní boj s počítačovými viry,“ řekl technický ředitel AVG Technologies a hlavní iniciátor projektu Karel Obluk. Jednoduše řečeno, odborníci spustí škodlivý kód v karanténním prostředí, sledují, jak se chová, a pak na něj vytvoří „lék“ a „protilátky“. Velmi důležitým aspektem je také sledování rychlosti a způsobu šíření různých typů virů po celém světě. Tým projektu AVG Malware TRAP Centrum nyní zaměstnává pět počítačových odborníků, později přibudou další. Příležitost zde najdou také studenti.

„V době, kdy se celý svět v menší či větší míře potýká s krizí a firmy spíše propouštějí, je toto jeden z pozitivních signálů, který ukazuje, že AVG Technologies je stabilní firma se silným zázemím,“ uvedl ředitel oddělení lidských zdrojů společnosti Jiří Omelka.

Brněnské centrum je jedním ze tří pracovišť firmy AVG Technologies, která se nyní odhalováním škodlivých kódů zabývají. Další dvě jsou na východním a západním pobřeží USA, přičemž M-TRAP by se v budoucnu měl stát páteří těchto datových center. Jeho tým pod vedením renomovaného specialisty na antivirové programy, Američana Ryana Hickse, bude zpracovávat obrovské množství dat od uživatelů z celého světa a sledovat chování počítačových virů. AVG Technologies na celém projektu úzce spolupracuje s Fakultou informačních technologií (FIT) Vysokého učení technického v Brně. Pracoviště M-TRAP funguje v prostorách fakulty, v nedávno rekonstruovaném kartuziánském klášteře v Božetěchově ulici v Brně-Králově Poli. „Spolupráce naší firmy s FIT se úspěšně rozvíjí již několik let. V minulosti jsme podpořili několik výzkumných projektů, sponzorujeme akce fakulty, studentům zadáváme témata bakalářských a diplomových prací. V souvislosti s otevřením našeho výzkumného centra nabídneme studentům a doktorandům fakulty možnost podílet se na výzkumné činnosti centra,“ doplnil Karel Obluk.

KOMUNITA

Kritika Facebooku

V rámci změny obchodních podmínek chtěli provozovatelé sociální sítě Facebook získat možnost navždy ukládat uživatelská data. Všechna práva týkající se fotografií a videí umístěných uživateli měla náležet sociální síti – a to i v případě, kdy uživatel svůj profil již vymazal. Ochránci dat a členové platformy proti novým nařízením ostře protestovali. Nyní Facebook ustupuje – provozovatelé chtějí obchodní podmínky kompletně přepracovat a uživatelé Facebooku údajně mají mít na jejich podobu velký vliv.
INFO: www.facebook.com

NOVÝ APPLE IPOD SHUFFLE

Nejmenší iPod mluví

Firma Apple představila novou verzi hudebního přehrávače iPod shuffle. Jde prý o nejmenší MP3 přehrávač na světě – menší než tužková baterie AA. Jde také o první přehrávač, který na vás díky integraci funkce VoiceOver mluví (a to dokonce i česky). Uživateli čte do sluchátek názvy skladeb, autorů a playlistů. Je o polovinu menší než jeho předchůdce, podporuje playlisty a jeho ovládání je snazší. Opět je založen na funkci „shuffle“, a náhodně tedy přehrává skladby jednotlivých nadefinovaných playlistů. Ovládá se pomocí miniaturního ovladače, který je integrován do sluchátkového kabelu. Nová generace iPod shuffle je nyní vybavena 4GB pamětí. Koncová cena v ČR bude patrně 2 650 Kč včetně DPH.
INFO: www.apple.cz

CASIO

Vysokorychlostní kompakty

Nové modely 9,1Mpx digitálních fotoaparátů EXILIM EX-FS10 a EX-FC100 obsahují funkci vysokorychlostního sériového snímání. Fotoaparáty nabízejí na kompakty vysokou rychlost snímání – 30 snímků za sekundu (při použití nižšího rozlišení – 6 Mpx). Video lze zachycovat rychlostí až 1 000 snímků za sekundu. Model EX-FS10 je přitom fotoaparát o velikosti karty, je tenký pouze 16,3 mm. Model EX-FC100 je pak kompaktní fotoaparát s větším, tedy 5násobným optickým zoomem a s rozměry 99,8 × 58,5 × 22,6 mm. Konstruktéři fotoaparátů využili rychlosti i k dalším funkcím – je možné zachytit statický obraz, zatímco uživatel sleduje pohyb předmětu zpomaleně. Můžete si vybrat a uložit jeden snímek z probíhajících záběrů. Fotoaparáty také zaznamenávají snímky ještě před stisknutím spouště (tzv. Prerecord CS), takže nepromeškáte správný okamžik pořízení fotografie. Uložit si můžete až 25 snímků před stiskem spouště. Vyšší rychlost napomáhá i ostrosti snímků.
INFO: www.casio.cz

SONY HANDYCAM

Full HD kamerka s GPS

Nová kamera Handycam HDR-TG7VE je podle výrobce, firmy Sony, nejmenší a nejlehčí Full HD videokamerou na světě (váží 230 gramů). Titanové tělo je opatřeno povrchem odolným vůči poškrábání. 16GB interní paměť pojme až 6 hodin Full HD videa se stereozvukem (paměť lze rozšířit pomocí karet Memory Stick). Zajímavé je, že videokamera dokáže zaznamenávat i geografické informace – uvnitř je ukryt GPS přijímač. Režim Map Index vám potom na displeji ukáže, kde byly videosekvence nebo statické snímky pořízeny. Po návratu domů si svou cestu můžete znovu projít na počítači s využitím on-line map v přiloženém programu Picture Motion Browser. Ovládací prvky kamery jsou omezeny na minimum. Kamera má 2,7palcový dotykový LCD displej a objektiv s 10násobným zoomem.
INFO: www.sony.cz

KANCELÁŘSKÝ SOFTWARE

OpenOffice 3.1 bude týmový

Nová verze bezplatného kancelářského balíku OpenOffice bude brzy zveřejněna, vývojáři již uvedli seznam s vylepšeními. Bude zde například uvedena funkce antialiasingu, díky níž budou grafiky zobrazeny méně „pixelovatě“. Získat na tom mají především grafy. Díky přepracované funkci ochrany nyní již dva uživatelé nebudou moci otevřít a zpracovávat jeden dokument. Vývojáři kromě toho pracovali na funkci komentářů, aby spolu uživatelé mohli diskutovat nebo si vyměňovat data.
INFO: http://openoffice.org

FLEPIA

Čtečka s barevným displejem

I když se zprvu zdálo, že čtení knih i jiných delších textů zůstane ještě dlouho doménou tradičního papíru, nachází mezi uživateli stále větší popularitu čtečky na bázi počítačů. Doposud byly tyto čtečky jen černobílé, to se však právě nyní mění: společnost Fujitsu oznámila zahájení komerčního prodeje vůbec prvního barevného mobilního přístroje na bázi e-papíru.

Čtečka s názvem FLEPia je dostupná ve velikostech A4 a A5 a je vybavena displejem schopným zobrazit až 200 000 barevných odstínů v rozlišení 1 024 × 768. FLEPia je dále vybavena USB 2.0, Wi-Fi 802.11 b/g, ale i technologií Bluetooth 2.0. Čtečka by měla dokázat pracovat na Li-Ion baterie až 40 hodin nebo zobrazit až 2 400 stránek. Fujitsu Laboratories vyvinuly barevný e-papír v dubnu 2007, cesta ke komerčnímu výrobku tedy trvala téměř přesně dva roky.
INFO: www.frontech.fujitsu.com/

LIFESTYLOVÝ WEBZIN

Portál o životním stylu

V polovině března byl spuštěn nový projekt společnosti Internet Info s názvem Vitalia.cz (**www.vitalia.cz**). Jde o internetový magazín zaměřený na zdravý a aktivní životní styl. Portál je určen především náročnějším čtenářům a jeho obsah je kromě redakční práce zčásti založen také na moderním komunitním principu. Obsahovou páteř serveru tvoří čtyři samostatné sekce věnované velkým tematickým celkům – zdraví, rodině, relaxu a jídlu. V každé z těchto sekcí najdou čtenáři vedle řady tematicky laděných článků a aktualit také speciály věnované konkrétním tématům, jako jsou cyklistika, golf, fitness a podobně. Značnou část obsahu tvoří podrobné katalogy, díky nimž lze snadno a rychle najít nejbližší bazén, fitness zařízení, golfové hřiště nebo sjezdovku. Pro jednoduchou lokalizaci slouží podrobná mapa České republiky. Připraveny jsou i další přehledy – od receptů, vitaminů, bylin a koření až po nemoci či zdravotnická zařízení. Všechny databáze se nesou v duchu Webu 2.0, neboť počítají také s uživatelsky generovaným obsahem.

SLUNEČNICE.CZ

Co se stahuje

Program pro vypalování CD a DVD nosičů Nero byl v únoru nejčastěji stahovaným softwarem ze serveru Slunečnice.cz v kategorii Audio & MP3. Jeho nejnovější varianta s pořadovým číslem 9 podporuje například vypalování i nejmodernějších Blu-ray a HD DVD disků. Jde pouze o zkušební verzi; plná verze, která je rovněž k dispozici na serveru Slunečnice.cz, je zpoplatněna. Mezi softwarem k vypalování je však k dispozici i řada programů ke stažení zdarma, například Ashampoo Burning Studio (5. místo). DVD Shrink, nástroj určený k zálohování DVD, obsadil stříbrnou příčku. Uživatelsky zajímavou vlastností tohoto programu je možnost komprimace DVD a jeho částečná editace. Třetí skončil známý a hojně rozšířený přehrávač Windows Media Player, podporující širokou škálu formátů.

SPORTOVNÍ KANÁL

TV Nova spouští Videosport.cz

Počátkem března rozšířila TV Nova své internetové aktivity a přinesla uživatelům internetovou službu s názvem Videosport.cz (**www.videosport.cz**). Na své si na novém webu přijdou zejména fanoušci sportů a sportovních odvětví, která se na televizních obrazovkách příliš neobjevují. Díky novému „televiznímu kanálu“ tak sportovní fandové mohou sledovat přímé přenosy z florbalu, skateboardu, hanspaulské ligy malého fotbalu, golfu, lakrosu, futsalu (sálová kopaná), amerického fotbalu a mnoha dalších sportovních odvětví. Diváci se mohou těšit zhruba na čtyři až šest přenosů za měsíc, doplněných zhruba čtyřicítkou zpravodajských reportáží za měsíc.