Nebezpečí z emailu

Warezov útočí

Poslední dobou se aktivita na poli bezpečnosti stále zvyšuje. Pojďte se podívat, kdo za tím stojí…

Text: Pavel Baudiš, Alwil Software

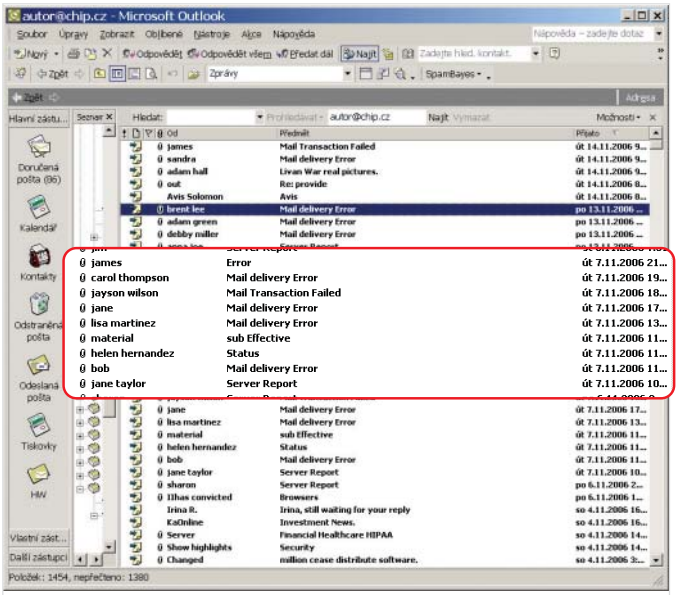
Už dlouho nebylo v našich poštovních schránkách tak plno jako v posledních několika týdnech. Teď nemám na mysli záplavy spamu, ale nejrůznější varianty červa zvaného Warezov, případně Stration. Stále se objevují nové a nové vlny výtvorů pocházejících z této dnes už rozsáhlé rodiny červů. Nové varianty jsou lehce polymorfní a odlišné od předcházejících a používají různé kódování tak, aby se vyhnuly včasné detekci antivirovými programy. Kromě toho, že se instalují do systému, jsou tyto programy schopny stahovat z internetu a přidat do počítače další škodlivý software.

Nebezpečí z emailu

Jak si mnozí z nás všimli, Warezov používá jako svůj hlavní distribuční kanál elektronickou poštu. Různé varianty používají různé předměty zpráv, nejčastěji se můžeme setkat s textem Mail server report, Error, Good dat, Mail Delivery System, Server Report, Status, test či This must be seen by everyone. Text zprávy může například obsahovat oznámení, že zpráva nemůže být zobrazena, byla převedena do binárního tvaru a je připojena jako příloha. Řada variant se tváří jako aktualizace systému proti novému viru – v takovém případě se příloha jmenuje Update-Kbaaaa-X86.exe nebo zip, kde aaaa je náhodné číslo. Je vidět, že červ pro svoje šíření využívá klasické sociální inženýrství, a ve velkém množství případů se mu bohužel podaří nezkušené uživatele přesvědčit k nevědomé a nedobrovolné spolupráci.

ICQ v ohrožení

Elektronická pošta však není jediným kanálem, který Warezov pro svoje šíření využívá. Je schopen se šířit posíláním odkazu na sebe samého přes ICQ. Počet zpráv vygenerovaných červem Warezov donutil provozovatele služby ICQ k tomu, že funkci posílání odkazů na stahování ve svém systému (dočasně?) vypnuli. Tím však způsobili spoustu nepříjemností řadě uživatelů, kteří ji normálně používají a kteří se o tom, že jejich zpráva nedošla, nikdy nedozvěděli. Po svém spuštění některé varianty vypíší okno s textem, které může obsahovat informaci o „úspěšné aktualizaci“, případně o „neznámé chybě“.



Warezov: **Téměř každý třetí mail skrývá záškodníka…**

Potom se pokouší stáhnout jeden až dva soubory z internetu – většinou nové varianty sebe samých či nejrůznější trojské koně. Červ se též může pokusit odeslat informaci o napadeném počítači včetně své verze, instalovaném operačním systému a instalovaném antivirovém programu a firewallu. Některé varianty červa pozmění systémový soubor hosts tak, že z napadeného počítače nelze přistupovat na stránky výrobce operačního systému a některých antivirových společností, takže není možno systém aktualizovat a o případném viru se vůbec dozvědět.

Globální útok

Červ se také pokouší vypnout a smazat řadu bezpečnostních programů, jako jsou antivirové programy a firewally. Pokud se mu to podaří, napadený počítač je pak zcela nechráněný před jakýmkoli útokem zvenčí. A jestliže se na něj později podaří nainstalovat třeba trojského koně typu bot, stává se pak „poslušnou součástí“ rozsáhlé sítě vzdáleně ovládaných počítačů, které mohou být zneužity k řadě účelů – k rozesílání spamu a virů, DDoS útokům a k dalším nezákonným aktivitám. Z předcházejícího popisu je vidět, že se jedná o důkladný plán, jak nakazit co nejvíce počítačů. Autoři upravují novou variantu tak dlouho, dokud není detekována nejrozšířenějšími antivirovými programy, a pak ji naráz vypustí. Tato nová varianta se velmi rychle dostane na skoro všechny počítače napadené předchozími variantami a odtud se elektronickou poštou snaží dostat na dosud nenapadené stroje. Každá vlna, způsobená úspěšnou variantou (ne všem se to podaří), je proto větší a masivnější než ta předchozí a počet ovládaných strojů stále stoupá. Úmysly autorů nejsou dnes zřejmé. Jak dlouho bude ještě trvat tato fáze budování sítě podřízených počítačů? Co bude následovat potom? Rozsáhlý útok na nějaký konkrétní cíl, nebo pouze „standardní“ využití pro distribuci spywaru, adwaru a phishingu? Dnes o tom všem můžeme pouze spekulovat, obávám se však, že výsledky činnosti červa Warezov pocítíme na vlastní kůži dříve, než bychom si všichni přáli… ■ ■ ■

INTERNETOVÉ PODVODY

Rozsudek: Vrácení peněz obětem phishingu

Mezinárodní banky konečně berou boj proti phishingu vážně a internetovým kriminálníkům začínají kohout penězovodu utahovat. Tak například německá Postbank zažalovala u vrchního zemského soudu v Hamburku takzvanou „finanční agentku“, která přes vlastní konto přeposílala do zahraničí obnosy získané phishingovými útoky. Této dámě to teď přijde draho: musí zaplatit 32 000 eur – ačkoliv peníze už jsou dlouho v rukách jejích odběratelů. Radovat se však mohou oběti phishingu, které své peníze dostanou zpět.

Z tohoto jednoduchého způsobu praní peněz se v posledních letech vyvinul kvetoucí byznys. Tomuto boomu by však nyní mohl být konec, jak alespoň po hamburském rozsudku věří bochumský phishingový expert Georg Borges. „Tisíce finančních agentů se napříště škod způsobených phishingem jen tak nezbaví,“ sdělil Chipu tento ekonomický právník. A to i v případě, že si tak počínali „nevědomky“ nebo „v dobré víře“.

V pozadí celé záležitosti je skutečnost, že phishingoví „rybáři“ sídlí téměř výhradně v zahraničí. Při vyprazdňování účtů se tak peněžní transfer stává úzkým hrdlem – bez pomocníků to nejde. Své přisluhovače přitom internetoví kriminálníci shánějí (stejně jako své oběti) elektronickou poštou a nabízejí jim zdánlivě lukrativní vedlejší úvazky: poskytnout vlastní konto pro několik transakcí a inkasovat za to tučné provize – to je běžná nabídka hromadných mailů.

Takový personální „nábor“ je v době slábnoucího trhu práce evidentně velmi úspěšný. Experti předpokládají jen v Německu několik desítek tisíc phishingových pomahačů, kteří ročně způsobí škody za více než 100 milionů eur. Prof. Dr. Georg Borges se sice tato čísla zdráhá potvrdit, domnívá se však, že „rhybáři“ stále ještě vlastní úžasné množství platných čísel TAN. Tváří v tvář tomuto problému nyní Postbank svou antiphishingovou strategii rozšiřuje: varuje už nejen před phishingovými maily a podvrženými webovými stránkami, ale také před přijímáním pochybných e-mailových pracovních nabídek.

Info: *www.a-i3.org, www.postbank.de*

TROJSKÉ KONĚ

Virus v účtu za telefon

Měsíční vyúčtování telefonních poplatků bývá zřídkakdy důvodem k radosti, ale v Německu se nyní stalo dokonce i bezpečnostním rizikem pro počítač. To v případě, že účet od Telekomu dostává účastník elektronickou poštou. Stále častěji se totiž vyskytují podvržené telefonní faktury, v nichž na svou příležitost číhají trojské koně. Princip těchto rafinovaných spamových mailů je vždy podobný: v textu jsou uvedeny nehorázné částky, které má adresát zaplatit, podrobnější vysvětlení slibuje přiložené PDF. Dokument je samozřejmě zamaskovaný škůdce. Telekom na své stránce shromáždil detailní pokyny, jak lze takové zfalšované účty poznat. Pokud uživatel vzdor všem varováním na podvodnickou přílohu klikne, může ho před napadením počítače uchránit už jen antivirový program s aktuálním seznamem signatur.

Info: *www.t-com.de/rechnung*

ZRANITELNÉ PROGRAMY

Nové bezpečnostní mezery

Microsoft Word 2000

Ohrožený Word

Mimořádně kritická mezera ve Wordu 2000 dovoluje hackerům spustit na cizím počítači škodlivý kód. Stačí jim k tomu jen propašovat do počítače zmanipulovaný wordovský dokument. Řešení: Záplata ještě není v dohledu.

Info: *www.microsoft.cz*

ICQ

Děravé ICQ

Core Security varuje před mezerami v instantním messengeru ICQ. V jeho verzi klienta Pro2003b mohou zmanipulované zprávy vyvolat buffer overflow. Jiná chyba postihla nástrojovou lištu ICQ pro Internet Explorer: RSS Feeds zde mohou spouštět programový kód. Řešením je upgrade na ICQ 5.1 a Toolbar 1.2.

Info: *www.icq.com*

Mozilla

Bezpečnostní problémy

Některé produkty stáje Mozilla Foundation obsahují bezpečnostní slabiny. Konkrétně se jedná o produkty Mozilla Firefox 1.5.0.7 a dřívější, Mozilla Thunderbird 1.5.0.7 a dřívější a Mozilla SeaMonkey 1.0.5 a dřívější. Celkem se jedná o tři zranitelnosti: chybné zpracování JavaScriptu, způsob zpracování RSA signatur s malým koeficientem (více informací o této zranitelnosti naleznete na *www.matasano.com*) a chyby při správě paměti. Více informací o jednotlivých zranitelnostech a odkazy na ně najdete na *www.kb.cert.org/vuls/id/714496*. Jednoznačným řešením je upgrade na novější verze.

Info: *zpravy.actinet.cz*

Microsoft Visual Studio

Spuštění kódu

Byla nalezena zranitelnost v MS Visual Studio 2005, která může vést ke kompletní kompromitaci cílového systému. Zranitelnost nalezená v WMI Object Broker ActiveX control (WmiScriptUtils.dll) umožní útočníkovi vytvořit na cílovém systému vlastní ActiveX, který obchází bezpečnostní model pro ActiveX na hostitelském stroji. Jedná se o zranitelnost, která je v současné době aktivně zneužívána a pro kterou existuje pouze workaround, který najdete v oznámení Microsoftu *(www.microsoft.com/technet/security/advisory/927709.mspx)*. Další informace se dozvíte například v oznámení organizace CERT *(www.kb.cert.org/vuls/id/854856)*.

Info: *zpravy.actinet.cz*

Bezpečnost pro Windows

AVG pro Windows Vista

Grisoft oznámil zpřístupnění aplikací AVG řady 7.5 v „Centru zabezpečení“ připravovaného operačního systému Windows Vista. Podpora se týká i bezplatného antivirového systému AVG Anti-Virus Free Edition. Uživatelé mohou s AVG pracovat již v testovacích verzích Windows Vista – viz např. *(www.microsoft.com/athome/security/update/windowsvista-RC1AV.mspx)*. Získají tak jistotu, že jejich počítač bude připraven čelit internetovým hrozbám okamžitě po zahájení prodeje nového operačního systému.

AVG 7.5: Ve Windows Vista je už jako doma...

„Spolupráce s partnery představuje klíčový prvek pro úspěch naší platformy a zajištění uživatelské bezpečnosti,“ uvedl Ben Fathi, viceprezident společnosti Microsoft pro oblast bezpečnosti. „Grisoft s námi při vývoji AVG 7.5 úzce spolupracoval na podpoře uživatelů Windows Vista. Tato spolupráce nám pomáhá naplnit cíl, kterým je ochrana uživatelů, rozšíření jejich možností volby a rozvoj nových řešení prostřednictvím nezávislých vývojářů.“

Produkty společnosti Grisoft připravené pro nasazení s Windows Vista zahrnují AVG Anti-Malware 7.5, AVG Anti-Virus Professional Edition 7.5 a AVG Anti-Virus Free Edition 7.5. Grisoft jejich prostřednictvím nabízí ochranu proti široké škále internetových hrozeb, mezi něž patří viry, trojské koně, nevyžádané reklamy, dialery, červi a nástroje pro odposlech citlivých údajů.

NORTON INTERNET SECURITY

Upgrade z 2006 na 2007

Symantec nabízí svým zákazníkům rozšíření funkcí bezpečnostního systému Norton Internet Security 2006 na úroveň aktuální verze 2007. Ochranu před novými typy hrozeb získají uživatelé s aktivním předplatným služeb Norton Internet Security 2006 v rámci bezplatné automatické aktualizace prostřednictvím služby Norton Update Center.

„Od vydání Norton Internet Security 2006 se objevila řada nových hrozeb, které mimo jiné zvyšují riziko finančních ztrát,“ uvedl Patrick Müller, Consumer Channel Sales společnosti Symantec. „Cítíme jako svou povinnost ochránit své zákazníky i před novými typy škodlivého softwaru. Proto jsme se rozhodli k tomuto netradičnímu kroku a v rámci předplatného nabízíme nejen aktualizace virové databáze, ale také nové bezpečnostní funkce.

Sada bezpečnostních aplikací Norton Internet Security 2007 obsahuje nástroje pro odhalení podvodných webových stránek a pokusů o krádež identity, ochranu proti přímému napadení sítě hackery, schopnost odhalovat nové verze virů a červů bez aktualizace virové databáze a rovněž kontrolu komunikace pomocí instant messagingu. Reakci na nejnovější vývoj představuje také nástroj pro odhalení tzv. rootkitů – škodlivého softwaru, který se důmyslně maskuje, takže je pro většinu antivirových systémů neviditelný. Tato technologie, která umožňuje odhalit skryté hrozby na uživatelské a aplikační úrovni i úrovni jádra operačního systému, čeká na udělení patentu.

Symantec také uvolnil k bezplatnému stažení doplněk pro bezpečnostní systém Norton Internet Security 2007. Uživatelé po jeho instalaci získají čtyři nové funkce (AntiSpam, Parental Control, blokování citlivých informací a odstranění reklam), které zvýší jejich bezpečnost při používání internetových služeb. Balíček je k dispozici v několika jazykových verzích na adrese *http://service1.symantec.com/SUPPORT/custserv.nsf/docid/2006092616462646*. Norton AntiSpam automaticky rozpoznává nevyžádané zprávy elektronické pošty včetně podvodných e-mailů. Norton Parental Control dává uživatelům možnost kontrolovat obsah, ke kterému na internetu přistupují děti. Mezi nevhodný obsah je řazena zejména pornografie a násilí. Funkce blokování citlivých informací varuje uživatele před každým pokusem o odeslání citlivých informací, jako jsou čísla kreditních karet, a to prostřednictvím elektronické pošty, webových stránek a nástrojů pro okamžitou komunikaci (ICQ, MSN a další). Funkce odstranění reklam snižuje zátěž, kterou na internetové připojení i samotné uživatele klade na internetu všudypřítomná agresivní reklama.

Windows XP Firewall

Vzdálené odstavení

Článek „New Windows attack can kill firewall“ na serveru NetworkWorld *(www.networkworld.com/news/2006/103006-new-windows-attack-can-kill.html?page=2)* uvádí, že plně záplatovaná Windows XP s běžícím ICS (Internet Connection Service) trpí zranitelností dovolující vzdálenému útočníkovi vyřadit z činnosti Windows XP Firewall. FAQ k této záležitosti naleznete na blogu The VERT Daily Post v příspěvku z 29. 10. 2006 *(http://blog.ncircle.com/archives/2006/10/microsoft_ics_d.htm)*.

Info: *zpravy.actinet.cz*

Firefox

Bezpečnostní mezery

Ve zdrojovém textu Firefoxu se skrývá 71 potenciálních bezpečnostních mezer. Odhalila to analýza softwarového dodavatele Clockwork, který svým nástrojem K7 hledá ve zdrojových programech logické chyby.

Vývojáři Firefoxu o slabinách vědí. Sledujte proto vydávání nových aktualizací.

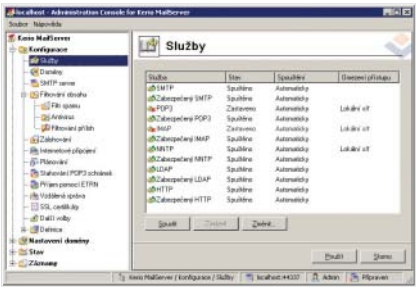
Info: *www.browser1.de*

Kerio Mail server

Ztrácíte telefony a PDA?

Kerio MailServer 6.3 bezdrátově synchronizuje e-maily, kontakty, kalendáře a úkoly se smartphony, telefony a PDA vybavenými protokolem Microsoft ActiveSync, a to bez nutnosti instalace klienta třetí strany nebo serverového softwaru. Nově také může být řešením zabraňujícím ztrátě citlivých dat.

„Neustále se setkáváme s otázkami, jak zabránit úniku informací při ztrátě mobilního telefonu nebo PDA,“ prohlašuje Jiří Birgus ze společnosti HCV Group, která je certifikovaným Business Partnerem společnosti Kerio Technologies. „Potřebujeme vyřešit problém, jak kompletně vymazat veškerá firemní data z telefonu, když někdo svůj přístroj ztratí.“



Pro tyto případy nabízí Kerio MailServer funkci Smart Remote Wipe, díky níž mohou administrátoři jednoduše vymazat veškerá data z konkrétního smartphonu napojeného na firemní mail server. Ačkoliv hardwarový Remote Wipe není ve starších telefonech Windows Mobile dostupný, Kerio MailServer 6.3 pro tyto starší přístroje nabízí vlastní alternativní řešení. Administrátoři mohou zaslat do telefonu náhradní, prázdná data, čímž vymažou všechny e-maily a groupwarové informace.

Kerio MailServer podporuje všechny smartphony a přístroje založené na technologii Windows Mobile, jako je například Palm Treo 700w, Motorola Q a další OEM telefony nabízené společnostmi T-Mobile, Vodafone a O2.

Sophos Anti-Virus

Spuštění kódu a Denial of Service

Řada produktů společnosti Sophos obsahuje několik zranitelností, které může útočník potenciálně zneužít a spustit tak na cílovém stroji libovolný kód nebo spustit útok typu Denial of Service. Jedná se celkem o čtyři zranitelnosti, které vznikají při zpracování archivů Petite, RAR a CHM souborů. Více informací včetně podrobného výpisu postižených verzí naleznete v původním ohlášení *(www.sophos.com/support/knowledgebase/article/7609.html)*.

Info: *zpravy.actinet.cz*

Adobe Flash Player

HTTP Header Injection

Adobe Flash Player 7.x, 8.x a 9.x má problémy při zpracování uživatelského vstupu do metody „XML.addRequestHeader()“ a vlastnosti „XML.contentType“. Díky těmto chybám může útočník pozměnit HTTP hlavičky klientských požadavků, což může vést ke spuštění příkazů v některých internetových aplikacích. Podrobný popis zranitelnosti naleznete na *www.rapid7.com/advisories/R7-0026.jsp*, vyjádření Adobe a odkaz na záplaty najdete na oficiálních stránkách *(www.adobe.com/support/security/advisories/apsa06-01.html)*.

Info: *zpravy.actinet.cz*

Wireshark

Pád aplikace

Několik nových zranitelností *(www.wireshark.org/security/wnpa-sec-2006-03.html)* bylo objeveno ve Wiresharku (bývalý Ethereal), verze 0.99.3 a dřívější. Chyby byly nalezeny v dissectorech protokolů HTTP, LDAP, XOT, WBXML, MIME a AirPcap a jejich zneužití pomocí speciálně upravených paketů může vést k vyčerpání systémových zdrojů nebo k pádu aplikace. Řešením je upgrade na verzi 0.99.4.

Clam AntiVirus

Spuštění kódu a Denial of Service

Opensourcový antivirus ClamAV *(www.clamav.net)*, verze dřívější než 0.85.5, obsahuje několik zranitelností, které může vzdálený útočník zneužít k útoku typu Denial of Service nebo ke spuštění libovolného kódu na cílovém stroji. V prvním případě se jedná o zranitelnost typu přetečení paměťové haldy ve skriptu „rebuildpe.c“ při zpracování PE souborů a ve druhém případě se jedná o chybu při rozbalování CHM archivů. Původní oznámení naleznete na *http://sourceforge.net/project/shownotes.php?release_id=455799*. Chyby byly opraveny ve verzi 0.85.5.

Info: *zpravy.actinet.cz*

Vyhledávání na webu

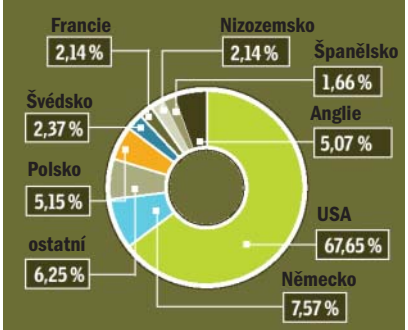
Bezplatný nástroj proti spamu od Googlu

Google je nejoblíbenější vyhledávač – i mezi rozesílateli spamu. A tak se jeho nic netušící uživatelé často ocitají na zmanipulovaných stránkách podvodně načítajících webové přístupy nebo – což je horší – na stránkách s malwarem a dalšími škodlivými programy. Bezplatný nástroj pro browsery „Googlefilter 2.1“ vás před takovým vyhledávačovým spamem ochrání. Jeho nově přepracovaná verze roztřídí nálezy Googlu na „dobré“ a „špatné“ a označí stránky, které jsou v databázi jejího dodavatele „Filtertechnics“ vedeny jako spam. Tento seznam je denně aktualizován. Googlefilter funguje s prohlížeči Firefox, SeaMonkey, Internet Explorer a Netscape od verze 7. Uživatelé Opery se však musí i nadále přehrabovat ve všech nálezech Googlu. Verze Premium za jedno euro měsíčně využívá vylepšenou databanku.

Info: *www.filtertechnics.de*

Googlefilter: Braňte se spamu na nalezených stránkách.

Výskyt spamu v roce 2006



Zdroje spywaru: USA je exportérem číslo jedna, druhé místo patří Německu.

Trend phishingu

Červencový pokles: Po červnovém rekordu všech dob přišel mírný útlum.

VIROVÝ TOP 5

Stav: listopad

1. MyTob.C (25,43 %)
2. Nyxem.e (14,42 %)
3. NetSky.b (8,06 %)
4. LovGate.w (6,36 %)
5. Mytob.u (3,264 %)

Zdroj: Kaspersky Lab.

CÍLENÝ SPAM

Nemocniční podraz

Vynalézavost spammerů nezná mezí. Zajímavý příklad cíleného spamu se stal v americkém nemocničním centru, kdy někteří zaměstnanci dostali výpověď zaslanou přes e-mail. Díky tomu, že e-mail měl zfalšovanou adresu a obsahoval řadu výrazů z nemocničního prostředí, spamové filtry jej vyhodnotily jako relevantní a předaly jej uživateli. V e-mailu byl odkaz na stránku, která nabízela informace ohledně zaměstnání. Při kliknutí na odkaz se ovšem do počítače stáhl keylogger.

Info: *www.networkworld.com/news/2006/110106-spam-spear-phishing.html?page=1.*

Opera

Přetečení bufferu

Prohlížeč Opera ve verzi 9.01 a 9.00 má problémy při parsování URL. Při parsování tagů, které obsahují URL, může dojít k přetečení bufferu a ke spuštění libovolného kódu s právy přilogovaného uživatele nebo k pádu prohlížeče. Podmínkou pro úspěšné zneužití této zranitelnosti je navštívení zákeřně upravené stránky. Podle vyjádření výrobce je Opera verze 9.02 bezpečná.

Info: *zpravy.actinet.cz*

Kaspersky Anit-Virus

Eskalace práv

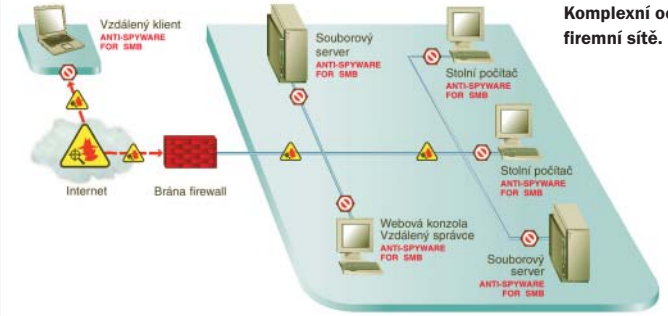
Byla nalezena zranitelnost v Kaspersky Anti-Virus Personal (Pro) v. 5.0 a Kaspersky Anti-Virus v. 6.0. Jedná se o chybu, která umožní vzdálenému útočníkovi získat vyšší systémová práva skrz řadiče KLIN a KLICK. Více podrobností se dozvíte v původním ohlášení *(http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=425).* Aktualizace můžete stahovat na webu výrobce *(www.kaspersky.com/productupdates).*

ŘEŠENÍ PRO MALÉ A STŘEDNÍ PODNIKY

Ochrana proti spywaru s automatickou obranou

Trend Micro Anti-Spyware for Small and Medium Businesses nově nabízí technologii pro ochranu proti spywaru. Produkt je navržen pro zjednodušení nasazení a pro správu s automatickou detekcí a odstraněním spywaru na síťově propojených počítačích a serverech – aniž by rušil zaměstnance.

Řešení Worry-free Anti-spyware od společnosti Trend Micro chrání také před adwarem, programy pro sledování používání klávesnice a deaktivátory zabezpečení. Program si poradí i se záškodníky blokujícími kontrolu nad webovým prohlížečem (např. CoolWebSearch), kteří mohou být zdrojem krádeží citlivých informací.



Worry-free: **Komplexní ochrana firemní sítě.**