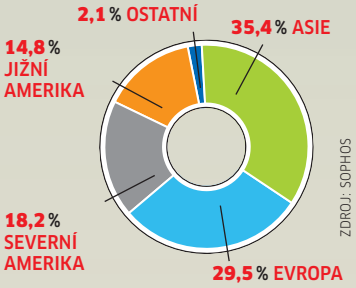
DATA A FAKTA

Barometr nebezpečí v srpnu

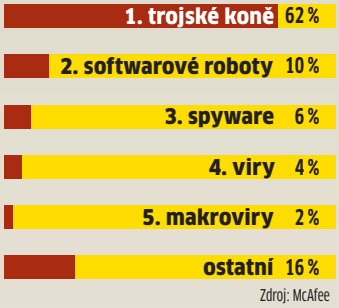
Také hackeři si berou dovolenou: V letních měsících bývá méně virů – přesto byste měli být opatrní!

Králové spamu



Celosvětově více než 35 % všech spamových zpráv pochází z asijských zemí.

Pomocníci hackerů



Zdroj: McAfee

Vzhledem k dobrým možnostem skrytí škodlivého kódu sázejí útočníci hlavně na trojské koně.

BEZPEČNOSTNÍ WEB CHIPU

www.chip.cz

I na našem novém webu najdete zajímavé informace a tipy a triky z oblasti bezpečnosti.

Útoky, proti nimž nic nepomůže

Po **NAPADENÍ DNS SERVERŮ** mohou hackeři přesměrovat veškerý internetový provoz na své vlastní servery a tam vyšpehovat utajovaná data.

FABIAN VON KEUDELL

DNS servery (Domain Name System) představují vlastně jakési telefonní seznamy webu. Bez nich byste nemohli otevřít žádnou webovou stránku, neboť vaše pécéčko by nevědělo, jak má danou URL interpretovat. Chcete-li například navštívit web chip.cz, spojíte se nejprve s nejbližším serverem DNS, který vašemu počítači sdělí, že za chip.cz se skrývá IP adresa 212.162.62.43. K ní pak PC zřídí spojení.

Nyní se útočníkům podařilo proniknout do DNS serverů a datový provoz z nich převést na vlastní počítače. Jejich cílem je samozřejmě vyslídit citlivé údaje, například hesla a čísla PIN/TAN pro internetové bankovnictví. Oběti o tom nemají sebemenší tušení, neboť se vždy ocitnou na správné stránce – data ovšem cestují oklikou přes špionážní server. Funguje to tak rychle, že zpoždění představuje jen několik desetin sekundy.

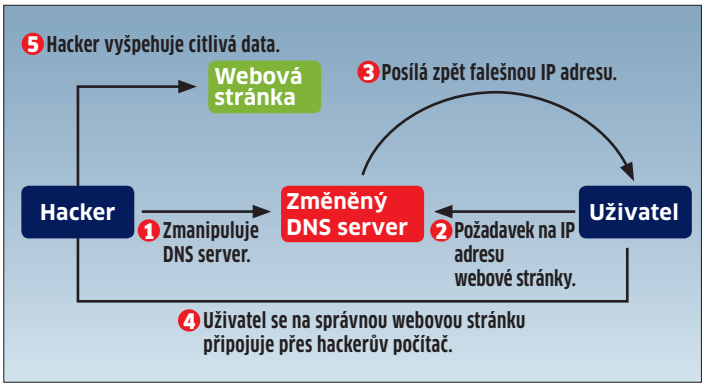
Marná obrana: Prolomeno je i zabezpečení DNS

Takovéto útoky umožnil hackerům prostý fakt – aby DNS servery minimalizovaly tok dat po internetu, ukládají svá data do vyrovnávací paměti. Bezpečnostní expert Dan Kaminsky nyní objevil způsob, jak lze tuto paměť zmanipulovat tak, aby pak byly počítačům posílány podvržené IP adresy.

Proti tomu vlastně existuje rozsáhlá obrana – jenomže v daném případě nezasáhne. Aby nikdo nemohl falšovat odpovědní pakety DNS, každý požadavek na DNS je provázen 16 bitů dlouhou identifikací transakce. Odpověď od DNS pak musí obsahovat totéž ID. Šance, že by někdo tento klíč uhádl, je prakticky nulová – pokud ovšem nenasadí nějaký trik. Kaminsky jich používá hned několik. Například vygeneruje tisíce simultánních spojení k DNS serveru a pokryje jimi platné transakční ID. Tak dokáže lokalizovat až 50 % všech transakčních ID. Útočníkům přijde vhod také další slabina – webový prohlížeč v počítači potenciální oběti používá pro vysílání požadavků stále stejný port, namísto aby čísla portů střídal a tím znesnadnil napadení. Jakou lest Kaminsky dále používá pro změnu v paměti DNS, chce prozradit až poté, co výrobci softwaru pro DNS dají k dispozici záplatu.

Zatím se sice neobjevily žádné známky toho, že by taková bezpečnostní mezera u DNS už byla využita, ale podle informačního embarga dohodnutého mezi softwarovými firmami lze usuzovat, jaký potenciál by takový útok měl. Dokonce i Microsoft a Cisco sjednanou antikomunikaci dodržují. Než přijde pomoc, mohou provozovatelé DNS serverů na Kaminského webové stránce vyzkoušet, zda je jejich server zranitelný.

INFO: www.doxpara.com



Hackeři umějí zmanipulovat DNS server: Nepozorován nic netušícím uživatelem přesměruje hacker datový provoz přes svůj počítač.

INVEX 2008

Antivirová konference

S blížícím se termínem dalšího ročníku podzimního veletrhu ITC Invex bychom vás rádi pozvali na tradiční Antivirovou konferenci, kterou naše vydavatelství pořádá ve spolupráci s BVV a předními společnostmi v oboru počítačové bezpečnosti.

Konference se koná ve středu 8. 10. 2008 v administrativní (výškové) budově BVV, v přednáškovém sále 102, a to od 9.30 do 13.00 hodin.

V rámci dopoledního programu budou opět přednášet přední odborníci na antivirovou problematiku ze společností AEC, Alwil, Eset, Grisoft a McAfee. Ve svých přednáškách se budou věnovat antivirové ochraně v systémech řízení informační bezpečnosti, proaktivní ochraně, heuristice, přehledu současných typů virů a úrovni jejich nebezpečnosti, budování nejlepší antivirové ochrany, novým metodám virových útoků a dalším tématům, která jsou v dnešním světě počítačové bezpečnosti aktuální.

Na rozdíl od minulých ročníků bude program obohacen o soutěže o věcné ceny z produkce antivirových firem, navíc si každý účastník konference opět odnese malý dárek. Budete-li ve středu 8. 10. 2008 na brněnském výstavišti, nenechte si ujít příležitost naši konferenci navštívit. Nezapomínejte, že antivirová problematika a počítačová bezpečnost se týká každého z nás! Jste srdečně zváni, konference je pro každého účastníka zdarma.

JIŘÍ PALYZA

INFO

Nová bezpečnostní rizika

VIDEOLANCLIENT

Pomocí zmanipulovaných videí je možné bez oprávnění správce spouštět na PC libovolný kód. Útočníci k tomu využívají „integer overflow“ ve WAV modulu. Řešením je instalace aktuální verze 0.8.6i z webové stránky výrobce.
INFO: www.videolan.org

SUN JAVA

V javovském softwaru firmy Sun je několik programových chyb, například zranitelnost napadením typu DoS a buffer overflow, jimiž mohou útočníci propašovat do počítače škodlivé programy. Naše doporučení? Nainstalujte si verzi JRE Update 7.
INFO: www.sun.com

OPERA 9.5

V prohlížeči Opera 9.5 už byla odhalena první bezpečnostní mezera. Detaily však do uzávěrky nebyly známy. Bezpečnostní služba Secunia hodnotí mezeru jako kritickou. Slabinu odstraňuje verze 9.51, která je k dispozici na webové stránce Opery.
INFO: www.opera.com

ADOBE PRESENTER

Adobe Presenter verze 6 a 7 obsahuje chyby, které zanesou do kódu vygenerovaného aplikací možnost Cross-site Scripting útoku. Výrobce doporučuje aktualizovat na verzi 7.0.1. Více informací naleznete v původním oznámení **(www.adobe.com/support/security)** na webu výrobce.
INFO: zprávy.actinet.cz

MCAFEE ENCRYPTED USB MANAGER

Společnost McAfee zveřejnila ServicePack 1 pro Encrypted USB Manager 3.1.0, který řeší možnost obejití autentizace v aplikaci za určitých podmínek. Bližší informace o Service Packu a odkaz na stažení naleznete na webu výrobce **(www.mcafee.com)** v původním oznámení.
INFO: zprávy.actinet.cz

MICROSOFT SECURITY BULLETIN

Zvýšenou pozornost doporučujeme věnovat záplatám Microsoftu na měsíc srpen **(viz www.microsoft.com/technet/security/bulletin/ms08-aug.mspx)**. Mezi nimi totiž najdete důležité opravy chyb umožňujících vzdálené spuštění kódu v MS Excelu, Powerpointu, Accessu a Microsoft Office Filters, dále opravy chyb v Microsoft Messengeru a bezpečnostní update pro Microsoft Outlook Express a Windows.
INFO: zprávy.actinet.cz

XINE-LIB

Zdá se, že mezi nejproblematičtější aplikace lze jednoznačně zařadit multimediální přehrávače. Nejprve bylo v jádru přehrávače xine (xine-lib) nalezeno několik zranitelností, které mohou vyústit v heap-based buffer overflow (přetečení haldy) a tím umožnit spuštění libovolného kódu. Chyby byly opraveny ve verzi 1.1.15. Více informací naleznete na webu Secunia.com **(http://secunia.com/advisories/31502/)**. Nedlouho poté ale byly v „opravené verzi“ nalezeny dvě nové zranitelnosti. V prvním případě se jedná o přetečení proměnné ve funkci open_ra_file() umístěné v src/demuxers/demux_ralaudio.c, které může být zneužito ke způsobení přetečení haldy přes upravený RealAudio soubor. Druhá chyba se týká ohraničení. Existuje ve funkci parse_block_group() ve stejném umístění, ovšem v souboru demux_matroska.c, a také může být zneužita ke způsobení přetečení haldy. Obě zranitelnosti tak dovolují spuštění libovolného kódu. Více informací najdete opět na webu Secunia.com **(http://secunia.com/advisories/31567/)**.
INFO: zprávy.actinet.cz

MS OFFICE

Útok na Word

Stačí otevření zmanipulovaného dokumentu Wordu – a hned má hacker váš počítač kompletně pod kontrolou. Do redakční uzávěrky neposkytl Microsoft o této slabině žádné bližší informace. Postižen je Word 2002 s nainstalovaným Service Packem 3. V současnosti útočníci tuto mezeru využívají pouze k cíleným útokům na jednotlivé osoby. Je však jen otázkou času, kdy hackerům taková programová chyba poslouží k napadení v masovém měřítku.

Ale není to jediná vstupní brána, kterou Word útočníkům nabízí. Microsoft musí ještě odstranit dvě další chyby: slabé místo prvku ActiveX v Office a mezeru v řadiči domény. Bugfix pro oba problémy zatím není k dispozici. Redmondští však podle vlastního vyjádření intenzivně pracují na záplatách pro všechny tři kritické mezery.

INFO: www.microsoft.com

FIREFOX

12 chyb!

Uživatelé prohlížeče Firefox 2 nesurfují bezpečně – celkem 12 mezer mohou hackeři využít k proniknutí do domácího počítače. Verze 3 Firefoxu postižena není. U osmi z těchto mezer hodnotí sama Mozilla nebezpečnost jako „kritickou“, respektive „vysokou“. Ohroženi jsou rovněž uživatelé poštovního programu Thunderbird, neboť aplikace je založena na jádru Firefoxu. Slabina postihuje uživatele, kteří v mailech aktivují javaskript. Pak mohou hackeři prostřednictvím přetečení bufferu spustit škodlivý kód. To může například nastat, pokud jsou k mailu „přibaleny“ extrémně veliké obrázky. Kdo nehodlá přestoupit na aktuální verzi 3, měl by si nainstalovat verzi Firefoxu 2.0.0.16. Uživatelé Thunderbirdu použijí verzi 2.0.0.14 poštovního programu.

INFO: www.mozilla.org

STUDIE INTERNETOVÉ BEZPEČNOSTI

On-line nebezpečí číhající na děti

Common Sense Media a tým Trend Micro Internet Safety for Kids & Families radí rodičům i dětem na téma vhodnosti webových stránek z hlediska věku a internetového zabezpečení.

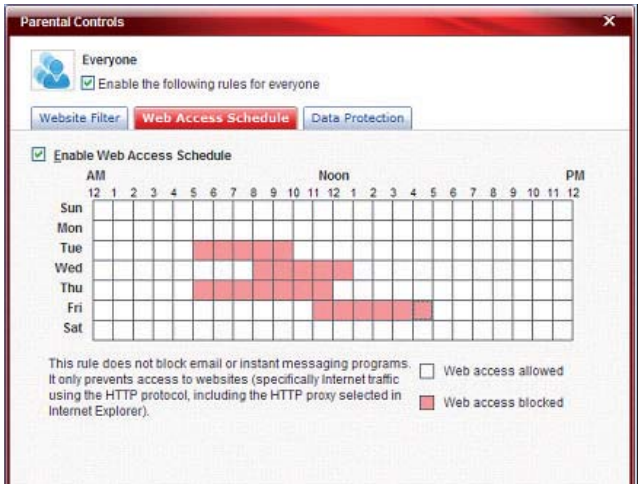
Partnerství oznámily společnost Trend Micro Incorporated, důležitý hráč v oblasti zabezpečení internetového obsahu, a Common Sense Media, významná národní nezisková organizace zaměřená na zlepšení dopadů médií na děti. Tato spolupráce by měla pomoci rodičům a mladým lidem lépe porozumět možnostem, jak co nejlépe využít potenciál internetu pro kreativitu, spolupráci a výuku. Partnerství by zároveň mělo zvýšit povědomí o problémech internetové bezpečnosti, jako jsou kyberzločin, krádeže identity, spam, spyware a adware.

Common Sense Media nabízí rodičům tipy na využívání médií a recenzuje média a zábavu z hlediska rozvoje dětské osobnosti. Toto partnerství s týmem Trend Micro Internet Safety for Kids & Families je součástí programu Trend Micro Global Citizenship Program (Globální občanský program Trend Micro). „Jedním z cílů Common Sense Media je vychovávat dětskou generaci, která vytváří a využívá on-line média, ale zároveň je v bezpečí, chytrá a etická,“ řekl Jim Steyer, CEO a zakladatel Common Sense Media.

I když mnoho rodičů ví o on-line nebezpečích ve formě nevhodného webového obsahu, kyberšikany nebo on-line predátorů, výzkumní pracovníci Trend Micro zabývající se internetovými hrozbami hovoří o méně známých nástrahách, kdy se na zdánlivě neškodných webových stránkách tajně skrývá škodlivý kód, umístěný tam kyberzločinci zaměřenými na zisk. Výsledkem je infiltrace uživatelova počítače a zcizení osobních dat, jako jsou čísla sociálního pojištění, informace o bankovních účtech a čísla kreditních karet.

Například weby sociálních sítí jsou velmi populární u mladých lidí mezi devátým a sedmnáctým rokem, z nichž mnozí uvádějí, že na nich tráví stejně času jako před televizní obrazovkou. Tyto stránky obvykle bývají vytvořeny na základě technologií Web 2.0 a jsou prvořadými cíli kyberzločinců a autorů malwaru, kteří využívají jejich interaktivnosti ke spouštění škodlivých útoků. Podle nedávno vydané zprávy Trend Micro Threat Report & Forecast se počet hrozeb v prostředí Webu 2.0 vyšplhal v lednu 2008 přes 1,5 milionu měsíčně ve srovnání s 1,0 milionu v prosinci 2007.

Kyberzločinci také využívají tzv. „typo-squatting“ a lákají nic netušící uživatele, kteří omylem zadají chybnou URL adresu, na škodlivé webové stránky. V minulosti byly často takovým způsobem děti přesměrovány na pornografické stránky. „I když se mladý člověk nikdy nestal terčem útoku on-line predátorů nebo kyberšikany, stále existují rizika spojená se surfováním po webu, která mládeži nebo jejich rodičům nemusí být zřejmá,“ uvedla Lynette Owensová, ředitelka společnosti Trend Micro pro záležitosti on-line komunit. „Naší snahou je, abychom ve spolupráci s Common Sense Media byli schopni rodičům ukázat, jak mají uvažovat o podstatě a bezpečnosti obsahu, který si prohlížejí on-line.“



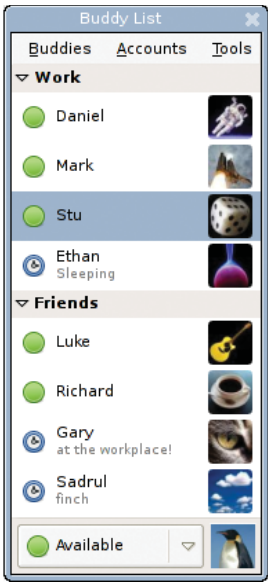
Chvályhodné: Ochrana dětí už začíná být standardním doplňkem většiny bezpečnostních balíků.

Komentář redakce:

*Problémy s nástrahami internetu má v současnosti i celá řada dospělých uživatelů a zkušených surfařů. Každý z nás si tedy jistě dokáže představit, v jakém ohrožení se děti na internetu mohou ocitnout. Až donedávna byl tento problém řešen alibistickým odkazováním na „nutnost dozoru rodičů“. Teprve v poslední době se začínají objevovat aktivity směřující k poučení dospělých, ale i dětí. Sem patří i český projekt Bezpečně bludištěm internetu **(www.saferinternet.cz)**. Problémem ovšem zůstává praxe – zatímco teoretických rad najdete na každém webu spousty, praktických tipů jen velmi málo. To platí i pro zmiňovaný český projekt – tam, kde byste čekali tipy a rady, jaký program zvolit pro bezpečnost dětí, najdete jen nic neříkající obecné recenze. My se na tuto oblast podíváme v jednom z příštích Chipů a poradíme vám ideální cestu k bezpečnému internetu (nejen) pro děti.*

MESSENGERY

Nebezpečné chatování



Bezpečnostní mezera v komunikačním programu Pidgin umožňuje hackerům donutit program ke zhroucení a na počítači spustit programový kód s lokálními uživatelskými právy. Podle objevitele slabiny musí uživatel akceptovat přenos souborů po síti MSN – útočníci přitom sázejí na chybu v programové knihovně Pidginu. Pak postačí, když hacker spustí přenos dat, který obsahuje speciální název souboru. Fatální je přitom skutečnost, že Pidgin podporuje více chatovacích protokolů jako AIM nebo ICQ; pak je totiž docela možné, že mezerou bude postižen nejen MSN protokol. Bezpečnostní služba Secunia prověřovala Pidgin rovněž a bezpečnostní mezeru potvrdila u verzí 2.4.1 a 2.4.2. Mezitím zareagoval výrobce a na své webové stránce nabízí aktualizovanou verzi Pidginu (2.4.3). V zásadě byste však vždy měli dbát na to, abyste datové přenosy po síti messengerů přijímali jen od důvěryhodných osob.

INFO: www.pidgin.im

INFO

Nová bezpečnostní rizika

VLC MEDIA PLAYER

V minulém čísle Chipu jsme vás upozornili na zranitelnost ve VLC Media Playeru, která byla opravena ve verzi 0.8.6i. Bohužel zranitelnost byla nalezena i v této verzi. Tato chyba může být zneužita ke spuštění libovolného kódu. Bližší informace hledejte na webu Secunia.com (http://secunia.com/advisories/31512/). Chip doporučuje přejít na některý z konkurenčních produktů...

INFO: zprávy.actinet.cz

FIREFOX 3

Společnost Radware oznámila, že v populárním internetovém prohlížeči Firefox 3 našla závažnou bezpečnostní chybu. Její zneužití může vést k útoku DoS (Denial of Service, odepření služby) – v daném případě k pádu prohlížeče. Objev uskutečnilo středisko SOC (Security Operations Center) společnosti Radware. Aktivní zneužití chyby vede k okamžitému pádu prohlížeče a ke ztrátě všech neuložených dat. Oficiální oprava problému není k dispozici, nicméně zákazníci společnosti Radware jsou již ochráněni díky službě Security Update Service. Přesné detaily zranitelnosti ve Firefoxu 3 nebyly zveřejněny, aby se zabránilo jejímu masovému zneužití, které je údajně velmi jednoduché. Týká se ovšem základní verze 3.0, stejně jako aktualizované verze 3.0.1.

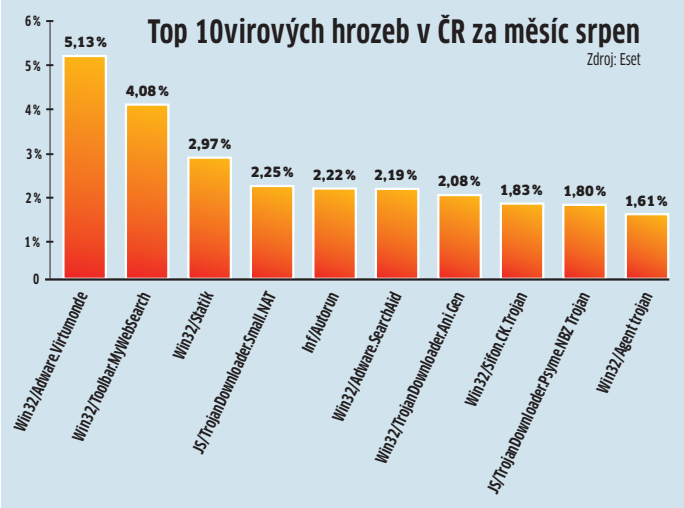
INFO: zpravy.actinet.cz

STATISTIKA HROZEB

Trojské koně s agresivní reklamou

Trojský kůň označovaný jako Win32/PSW.OnLineGames je stále nejčastěji odhalovanou hrozbou v celosvětovém měřítku. V Česku však v srpnu do první desítky nepronikl, a lokální žebříčky tak stále ovládá agresivní nevyžádaná reklama.

Rodina trojských koní vykrádajících údaje uživatelů on-line her Win32/PSW.OnLineGames stále posiluje. V srpnu překonala již 16 % a je stále nejčastěji detekovanou infiltrací na světě. Vyplývá to z aktuálních výsledků statistického systému ESET ThreatSense.Net. Agresivita tvůrců této hrozby je varováním pro všechny uživatele, kteří využívají služeb nejrůznějších on-line aplikací, ať už jde o virtuální světy typu Second Life, nebo herně zaměřené servery jako World of Warcraft. Ztráta přihlašovacích údajů, jejich následné obchodování (i na serverech jako eBay) a zneužití jsou již běžnou záležitostí. Na druhé místo světových statistik se v srpnu vrátila skupina infiltrací INF/Autorun (3,74 %), využívající automatického spouštění vložených médií (CD, DVD), které načtením pozměněného souboru autorun.inf automaticky infikují počítač. Třetí a čtvrté místo obsadily klasické adwarové aplikace Win32/Adware.Virtumonde (3,33 %) a Win32/Toolbar.MyWebSearch (3,16 %).



Jedinou novinkou mezi celosvětově nejrozšířenějšími hrozbami se tak v srpnu stal Win32/TrojanDownloader.Swizzor.D, u kterého statistický systém ESET ThreatSense.Net zjistil nárůst detekcí z nuly až na 1,89 %. Swizzor.D je nástrojem, který útočníci využívají ke stahování nejrůznějších škodlivých komponent na již infikovaný počítač. Na mnoha napadených či podezřelých stránkách byly detekovány kopie Swizzor.D, předstírající, že jsou optimalizačním nástrojem pro P2P (peer-to-peer) výměnné sítě, jako například BitTorrrent, a proto by měli být na pozoru především uživatelé těchto aplikací.

Srpnové hrozby v ČR

Statistika ESET ThreatSense.Net pro Českou republiku označila v srpnu na prvním místě opět rodinu agresivního adwaru Win32/Adware.Virtumonde (5,13 %). Ve srovnání s červnovými více než osmi a červencovými sedmi procenty úspěšnost této hrozby po dlouhé době v ČR klesá.

Letní posilující trend potvrdil v červenci adware Win32/Toolbar.MyWebSearch, který skončil na druhém místě a šířil se na úrovni 4,08 % ze všech detekcí. Infiltrace se tak vrátila na své pozice ze zimních měsíců. Jedná se o poměrně neškodný adware, který instaluje přídavnou vyhledávací lištu do internetového prohlížeče a veškeré vyhledávání následně směruje přes webovou stránku shodnou se svým názvem.

Třetí srpnovou příčku obsadila směs malwarových infiltrací označovaná systémem ESET ThreatSense.Net jako Win32/Statik. Zbytek první desítky se v srpnu poměrně vyrovnal kolem hladiny rozšířenosti na úrovni dvou procent.

Komentář redakce:
Vývoj v oblasti šíření virů je logickým důsledkem vývoje hardwaru a on-line aktivit. 4GB SD karta za necelých 300 Kč nebo 8GB flash disk za 500 Kč stojí za rozšířením malwaru šířícího se pomocí přenosných médií a popularita internetových her nebo P2P programů zase ovlivňuje další místa v žebříčku hrozeb. Všimněte si, že například e-mail hraje v šíření malwaru takřka zanedbatelnou roli – moderní antivirové programy spolupracující s většinou klientů dokáží spolehlivě zablokovat většinu nebezpečí. Je tedy jen otázkou času, kdy na problematické aktivity zareagují výrobci antivirů a nabídnou jednoduché nástroje chránící před infekcí z přenosných médií.

SOFTWAROVÁ NOVINKA

Kerio WinRoute Firewall 6.5

Společnost Kerio Technologies oznámila vydání produktu Kerio WinRoute Firewall 6.5, komplexního síťového firewallu s novými funkcemi. Kerio WinRoute Firewall 6.5 umožňuje rozložit internetovou komunikaci mezi několik internetových linek, čímž zajišťuje vysokou dostupnost služeb a maximální rychlost internetového připojení pro jednotlivé uživatele.

Firewall také nabízí dvojnásobnou antivirovou kontrolu na internetové bráně, filtrování obsahu WWW stránek, služby VPN a SSL-VPN, omezování šířky pásma, široké možnosti řízení přístupu, podrobnou analýzu síťové komunikace a reportovací nástroje. Oddělený administrační program umožňuje systémovým administrátorům spravovat firewall a řídit přístup do internetu lokálně i vzdáleně. Integrovaný reportovací modul Kerio StaR dává správcům přehled o historii síťové komunikace, aktivitách uživatelů a typickém využívání internetu. Sledování komunikace v reálném čase dává informace o přeneseném objemu dat a WWW stránkách navštívených jednotlivými uživateli. Na základě těchto informací lze pak nastavit efektivní omezení přístupu do internetu. V kombinaci s modulem ISS OrangeWeb Filter provádí Kerio StaR také analýzu navštívených stránek podle typu obsahu. Kerio WinRoute Firewall lze jednoduše integrovat s Active Directory, a tak může být nasazen do libovolné sítě s doménou Windows.

INFO: www.kerio.cz

HARDWAROVÁ NOVINKA

Firewall Cyberoam

Společnost Comguard představila pod značkou Cyberoam nové řešení bezpečnostní brány – UTM firewall, který je vhodný především pro malé a střední firmy. Přístroj nabízí podporu pro VPN, antispam, antivirus, IPS nebo integraci s Active Direktory. Produktová řada zahrnuje sedm modelů a nabízí komplexní zabezpečení vstupu do vnitřní sítě a chrání proti hrozbám zevnitř i vně sítí.

INFO: www.comguard.cz