Bezpečnost

Bezpečnostní programy

Nejlepší ochrana

Používání ochrany proti virům a dalším škodlivým programům by dnes mělo být samozřejmostí. Jaký program však vybrat? Jak co nejlepší ochranu zkombinovat? Je lepší používat samostatné programy specializované na jednotlivé oblasti, nebo komplexní balíky, které pokrývají vše?

Text: Pavel Baudiš, Alwil Software

Na tyto otázky neexistuje jednoznačná odpověď. Jedno je ale jisté – každý počítač by měl být chráněn, protože infiltrace nijak nechráněného počítače je podle posledních výzkumů otázkou pouhých několika minut po připojení k internetu.

Kritéria výběru

Pořízení antivirových či antispywarových programů dnes není nijak složité, nabídka je velmi široká, a zejména pro domácnosti nabízí řada renomovaných firem své produkty zdarma. Také aktualizace bývají velmi jednoduché a v některých případech zcela automatické. Konkrétní výběr však může být trochu složitější – dnes není na světě mnoho míst, která by byla schopna otestovat schopnost detekce a ochrany antivirových programů a v nějakém rozumném čase výsledky publikovat. Navíc je špička v této oblasti velmi vyrovnaná – například prestižní ocenění VB100% si v posledních letech odnášejí takřka všechny zúčastněné produkty, což samozřejmě výběr příliš neusnadní. Na řadu tak přistupují další faktory: cena, kompatibilita s dalšími programy, snadnost a dostupnost aktualizací, dokonce i grafické rozhraní a podobně.

Komplexní balíky

Ani otázka komplexních balíků není jednoduchá – je pohodlné mít jednu instalaci, stejné či podobné ovládání a případnou podporu pouze od jediného výrobce. Já však osobně dávám přednost specializovaným produktům, které patří ke špičce v dané užší oblasti. A netýká se to jen programů – mám radši kvalitní telefon, PDA, GPS a fotoaparát samostatně, než jediné zařízení, které obsahuje všechny výše uvedené prvky v jednom přístroji. Nejde jen o kvalitu jednotlivých částí, ale také o to, že když morálně zastará jedna z nich, →

Best Anti-Malware Solution: Slavnostní vyhlášení stálo za to...

nemusím měnit vše. Chápu ale, že někdo jiný může mít na věc zcela opačný názor a takové řešení mu může vyhovovat.

Důležité drobnosti

Ať už se rozhodnete pro jakékoli řešení, je potřeba, aby váš počítač obsahoval funkční firewall, antivirový a antispywarový program a aby tyto programy byly správně nainstalovány a nakonfigurovány a včas a pravidelně aktualizovány. Důležité je i aktualizovat kritické záplaty operačního systému a dalších aplikací, které často odstraňují klíčové bezpečnostní chyby a problémy, jež umožňují průnik škodlivých programů do vašeho počítače. Je jasné, že je navíc potřeba dodržovat zásady prevence a používat selský rozum – a hlavně neklikat na každý připojený soubor v elektronické poště či každý odkaz na webu. Pak se riziko infekce blíží k nule.

Nejlepší produkty

Zajímavý pohled na názor odborné veřejnosti přineslo nedávné vyhlášení cen časopisu Secure Computing. Jeho čtenáři hlasovali pro nejlepší produkty v řadě kategorií, odborná porota pak z výherců hlasování vybírala nejlepší produkt. Slavnostní vyhlášení evropské části soutěže se konalo koncem dubna v Londýně. Nás bude zajímat zejména kategorie "Best Anti-Malware Solution" (nejlepší řešení proti škodlivým programům), která měla celkem čtyři podkategorie: nejlepší antispyware, antitrojan, antivirus a antiworm. V kategorii nejlepší antispyware u čtenářů zvítězil Kaspersky Antivirus (porazil eSafe, eTrust PestPatrol a Spy Sweeper Enterprise), v kategorii antitrojan byl vítězem eSafe (porazil eTrust Antivirus, Kaspersky Antivirus a Trend Micro), v prestižní kategorii antivirus byl vybrán avast! antivirus (dalšími finalisty byli eSafe, AVG Antivirus, Kaspersky Antivirus a McAfee Antivirus) a v kategorii antiworm podruhé vyhrál Kaspersky Antivirus (finalisté Citrix NetScaler a CounterACT). Porota pak jako hlavního vítěze celé kategorie vybrala avast! antivirus. Je jasné, že boj byl velice vyrovnaný a že tyto ceny nemají absolutní platnost, nicméně názory čtenářů a poroty u tak renomovaného časopisu určitě mají svou váhu. A nás může těšit, že Česká republika měla v soutěži hned dva zástupce (avast! a AVG). Program avast! antivirus navíc vyhrál podkategorii nejlepší antivirus i ve Spojených státech.

Ať už si vyberete jakýkoli program, přeji vám, aby splnil svůj účel a aby se žádný škodlivý kód do vašeho počítače nedostal! ■ ■ ■

KRÁTCE

Microsoft a Interpol v honu na „rhybáře“

Microsoft chce do poloviny roku kvůli internetovým podvodům obžalovat 100 osob po celém světě. Softwarového obra přitom podporuje i Interpol. První obžaloby už byly podány. Mezi pravděpodobnými podvodníky jsou i němečtí programátoři, kteří z uživatelů vylákali údaje z kreditních karet a informace o bankovních účtech.
Zdroj: *www.microsoft.com*

Chyby webových aplikací

Server Securityfocus přináší přehled nejčastějších chyb *(www.securityfocus.com/infocus/1864/1)*, kterých se dopouští programátoři webových aplikací. Na názorných příkladech popisuje pět nejčastějších zranitelností (Remote code execution, SQL injection, Format string vulnerabilities, Cross Site Scripting (XSS), Username enumeration) a ukazuje možné způsoby jejich zneužití.
Zdroj: *www.securityfocus.com*

Malware Evolution 2005

Pohled na to, jaký byl rok 2005 pro systémy založené na Unixu z pohledu škodlivého kódu, přináší analýza antivirové společnosti Kaspersky Lab *(www.viruslist.com/en/analysis?pubid=184625030)*. O rostoucí popularitě této platformy pro autory virů svědčí 100% nárůst škodlivého kódu na linuxové systémy. Velkou neznámou se může stát přechod společnosti Apple na intelovské systémy a samozřejmě nástup mobilních technologií, kde představují alternativu k systémům Symbian a Windows Mobile.
Zdroj: *www.kasperskylabs.com*

VIROVÝ TOP 5

Stav: únor 2006

1 MyTob.C (33,38 %)
Rozesílá se na položky v adresáři Outlooku.

2 LovGate.w (8,07 %)
Umožňuje přístup do počítače třetím osobám.

3 Zafi.d (5,87 %)
Mění systémový registr a rozesílá se na položky v adresáři Outlooku.

4 NetSky.t (5,09 %)

5 NetSky.b (4,77 %)
Oba tyto viry hledají v počítači e-mailové adresy, aby se na ně dále rozesílaly.

Rootkit

Supervirus – made by Microsoft

Svět už je opravdu vzhůru nohama: Microsoft vyvíjí rootkit podvracející samotná Windows. A co víc, „Virtual Machine Based Rootkit“ (VMBR), pojmenovaný SubVirt, je „superrootkit“, proti němuž jsou virové skenery bezmocné. Neběží totiž v napadeném operačním systému, nýbrž paralelně k němu ve virtuálním prostředí.

Microsoft samozřejmě nepřešel na druhou stranu barikády. Tento scénář má jen ukázat, co by v budoucnu také mohlo přijít na mysl hackerům – a že jsou v Redmondu na takové ohrožení připraveni. Přesto je SubVirt důvodem ke zneklidnění: Co když Microsoft na principu VMBR začne kontrolovat počítače uživatelů? Způsob, jakým rootkit funguje, je upotřebitelný i pro počínání „Velkého bratra“: základem pro SubVirt je software VirtualPC (rovněž od Microsoftu), který emuluje PC. VMBR se nainstaluje „pod“ operační systém a po restartu počítače jej spustí ve virtuálním prostředí PC. Instalační soubor by se při objemu necelých 100 MB dal šířit po sítích P2P, na pevném disku zabere nenápadných 250 MB. Uživatel téměř nepocítí pokles výkonu, nanejvýš se možná podiví nad poněkud delším zaváděním systému. Dokonce i jeden z pracovníků Microsoftu údajně pracoval s infikovaným systémem, aniž by si toho povšiml.

Takový VMBR sice nenapíše kdejaký skriptující teenager, pokročilí programátoři však už ano. Jakmile je jednou nainstalován, může rootkit spouštět jakékoli myslitelné aplikace. Při pokusu Microsoftu tak běžel phishingový mailserver a keylogger, teoreticky by se tak ale dala realizovat i nezbytná ochrana proti kopírování – nebo také kontrolní mechanismus, který by zabraňoval spouštění opensourcových programů.

ZÁVĚR: Nic proti novým antivirovým strategiím – jestliže však vývojáři Microsoftu předvádějí, jak dokážou kontrolovat počítače uživatelů, nahání to strach. Otázka, jak si jako uživatel udržet vládu nad počítačem, zůstává nezodpovězena. Vágním poukazem na hardwarově orientovaná antivirová řešení Microsoft jen odehrál míč dále od své branky. ■ ■ ■

Jak se dá podkopat systém

„Virtual Machine Based Rootkit“ (VMBR) se v podstatě vklíní mezi operační systém a hardware. Počítačový systém pak běží ve virtuálním prostředí, současně je ale také aktivní VMBR – aniž by si toho operační systém povšiml.

STUDIE

První virus na RFID čipu

Je vaše kočka nakažena počítačovým virem? Není to vyloučeno. Mnozí majitelé domácích zvířat totiž dávají svým mazlíčkům implantovat RFID čip, aby je snáze našli, pokud se jim zaběhnou. Vědec Andrew S. Tanenbaum nyní využil informace z takového čipu, aby – jak líčí ve své studii s „kočičím“ námětem – napsal RFID virus. Prostřednictvím čteček RFID čipů dokázal napadnout připojenou databanku a měnit ji. V ještě poměrně nevinném případě by se pomocí zavirovaných RFID etiket daly měnit ceny v supermarketech. Mnohem dramatičtější by například bylo, jak dále vyvozuje Tanenbaum, kdyby tuto techniku začali využívat teroristé, aby tak obešli bezpečnostní systémy na letištích.
Info: *www.rfidvirus.org*

FLASH DISK

Bezpečný transport dat

Mezi nejpoužívanější média pro uchovávání a transport informací patří v současné době flash disky. Pokud však jde o „citlivá“ data, pak je používání standardních médií rizikové. Řešením je buď tzv. biometrická ochrana (otisk prstu), nebo použití šifrování. A právě druhou metodu používají USB disky SafeBoot USB2Go/Standart, které jsou od dubna letošního roku k dispozici i na našem trhu.

Tyto USB disky poskytují nejen ochranu přístupu pomocí hesla, ale zároveň data „on-line“ šifrují pomocí algoritmů jako AES – 256. USB disky SafeBoot také umožňují nastavení volitelné „veřejné“ nešifrované oblasti informací. USB disky SafeBoot USB2Go jsou na českém trhu dostupné prostřednictvím výhradního zástupce značky SafeBoot, společnosti FreeDivision. Ceny se pohybují od 1400 Kč. Dražší alternativou mohou být USB disky ClipDrive Bio od firmy Biometric, které mají navíc ještě zmiňovanou biometrickou ochranu pomocí otisku prstu.

Keylogger zaznamenává kliknutí

Nová varianta trojského koně PWSteal.Bankos.Q protokoluje akce myši – třeba zadávání TAN pomocí virtuální klávesnice. Jedinou obranou je udržovat virové signatury v aktuálním stavu!
Zdroj: *www.pctools.com*

Autoři virů „údernicky“

Hackeři využívají softwarové slabiny stále rychleji. Podle údajů Internet Security Systems bylo v loňském roce 3,13 % škodlivých programů dáno do oběhu během 24 hodin od oznámení bezpečnostní mezery – bezmála dvakrát více než v roce 2004.
Zdroj: *http://xforce.iss.net/xforce/threat_insight_quarterly/index.php*

TROJSKÝ KŮŇ

Vydírání jako ve filmu

Trojský kůň „Cryzip“ trápí svou oběť neobvyklým způsobem – zašifruje soubory a pak požaduje výkupné za heslo pro jejich dešifrování. Maskován jako ZIP soubor si škůdce počíná jako protřelý filmový padouch: vyhledává dokumenty Wordu, tabulky Excelu, PDF soubory a JPEG obrázky, shromáždí je v blokovaném ZIP souboru – a originály vymaže.

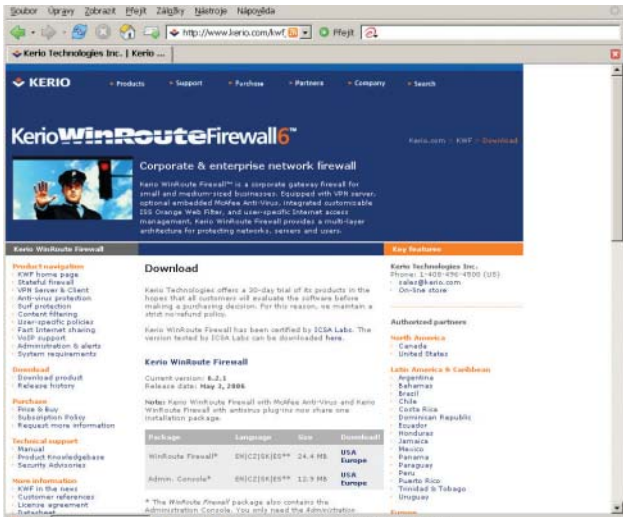
V textovém souboru pak své oběti předloží návod, jak se může opět dostat ke svým dokumentům: „Zaplaťte 300 dolarů!“ – anonymně přes internetovou platební službu e-gold. Autor své „dílko“ naštěstí zatím příliš nerozšířil. Kdyby však došlo i na vás, bezpečnostní experti firmy Sophos heslo vypátrali – zní jako cílový adresář ZIP souboru: „C:\Program Files\Microsoft VisualStudio\VC98“.
Info: *www.sophos.com*

DENIAL OF SERVICE

Chyba ve firewallu

Nepříjemnou chybu objevila firma Kerio Technologies Inc ve svém WinRoute Firewallu. Ve verzi 6.2.0 a nižší může být software úspěšně napaden pomocí útoku typu Denial of Service. Zranitelnost způsobuje inspekce e-mailových protokolů (SMTP a POP3) a při zaslání speciálně upraveného e-mailu může způsobit pád systému. Opravená verze 6.2.1 je k dispozici na stránkách výrobce *(www.kerio.com/kwf_download.html)*.

Info: *zpravy.actinet.cz*

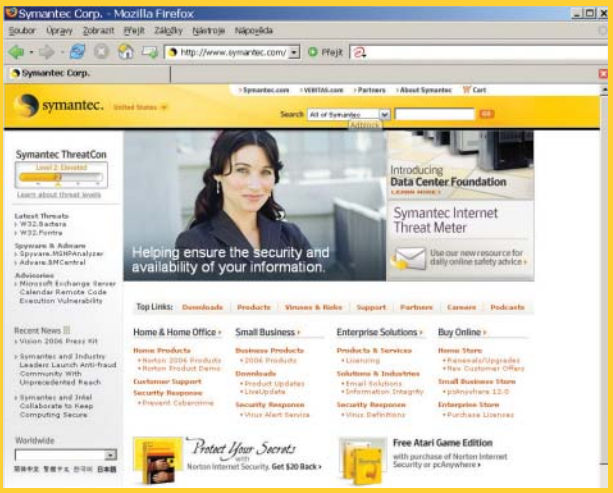


ZRANITELNOSTI

Symantec Scan Engine

Symantec Scan Engine ve verzi 5.0 obsahuje tři nové zranitelnosti. První chyba se týká špatně provedené autentizace uživatele, který je přihlášen přes web. Druhá chyba může potenciálně způsobit útok typu man-in-the-middle, a to kvůli statickému soukromému DSA klíči pro SSL komunikaci, který nemůže být uživatelem změněn a který se dá lehce získat. Poslední chyba umožní útočníkovi stáhnout z instalačního adresáře Symantec Scan Engine libovolný soubor. Opravy jsou k dispozici ve verzi 5.1.

Info: *www.rfidvirus.org*



JAVA A ZRANITELNOSTI

MAC OS X

V Apple Mac OS X verze 10.4.6 a starších byly objeveny chyby (http://secunia.com/advisories/19686/), které mohou vyústit v DoS nebo kompromitaci uživatelova počítače. Chyby mohou nastat při manipulaci se zákeřně upraveným zip archivem pomocí BOMArchive-Helepru nebo při prohlížení zákeřně upravených webových stránek (jak html, tak i obrázky – gif, bmp, tiff) pomocí Safari prohlížeče. Výrobce v současné době neuvolnil opravy. Secunia doporučuje nenavštěvovat nedůvěryhodné webové stránky a neotevírat obrázky a zip archivy z nedůvěryhodných zdrojů. Naopak zveřejněny již byly bezpečnostní záplaty pro Mac OS X verze 10.4.5 a Mac OS X Server verze 10.4.5. Aktualizace se týkají Javy, která umožňovala útočníkovi zvýšit svoje systémová oprávněn.

Info: *zpravy.actinet.cz*

OPRAVA CHYBY

Firefox 1.5.0.3

Světlo internetu spatřila nová verze Firefoxu a označením 1.5.0.3. Nehledejte v ní však žádné nové funkce – jde jen o opravu chyby, kterou například Secunia *(http://secunia.com/advisories/19802/)* hodnotí jako vysoce kritickou. Tato chyba umožňovala pád prohlížeče a v některých případech i kompromitování počítače uživatele. Problém se týká pouze verzí 1.5 – 1.5.0.2 (a to včetně české „mutace"), proto je upgrade na novou verzi více než doporučeníhodný.

Info: *www.mozilla.com/firefox*

NOVÉ BEZPEČNOSTNÍ MEZERY

INTERNET EXPLORER 6
Krátce po březnovém „záplatovacím“ dnu Microsoftu objevil Michal Zalewsky v jeho browseru novou mezeru *(http://secunia.com/advisories/19269/)*, která útočníkům umožňuje nahrávat programový kód. Postižen je Internet Explorer 6 i IE7 beta 2, které běží na Windows XP s SP2.
➜ Aplikace patchů z webu Microsoftu.
Info: *www.microsoft.com*

ADOBE FLASHPLAYER
Kritická slabina v programu FlashPlayer umožňuje hackerům převzít kontrolu nad počítačem. Stačí k tomu přehrát zmanipulovaný soubor ve formátu Shockwave. Postiženy jsou všechny verze FlashPlayeru až do 8.0.22.0.
➜ Adobe naléhavě doporučuje update na novou verzi 8.0.24.0, která je připravena ke stažení.
Info: *www.macromedia.com/go/getflashplayer/*

AVIRA ANTIVIR
Bezpečnostní díra v programu Avira AntiVir umožňuje lokálním uživatelům získat administrátorská práva v případě, že běží integrovaný plánovač – například během aktualizace signatur. Mezeru vykazuje jak bezplatný AntiVir Personal Edition Classic, tak i verze Premium tohoto softwaru.
➜ Update na Build 143 (Classic), resp. 128 (Premium).
Info: *www.free-av.de/antivirus/allinoned.html*

OPEN OFFICE 2.0
Do starších verzí Open Office je možné propašovat programový kód a spustit jej. Stačí k tomu vložit do dokumentu upravenou adresu URL, která vyvolá přetečení bufferu. Takový dokument by se do počítače mohl dostat například elektronickou poštou.
➜ V Open Office 2.0.2 už je chyba odstraněna. Ke stažení na:
Info: *http://de.openoffice.org/downloads/quick.html*

Nejnebezpečnější viry

Poznej svého nepřítele

O viry a antivirová řešení se většina z nás začne zajímat až s prvním infikovaným souborem. Pokud však nemáte zájem o podobné zkušenosti, nabídneme vám informace o nejrozšířenějších a nejnebezpečnějších virech, které mohou váš počítač ohrozit.

Staří známí

Na vrcholu celé řady najdete **W32/Netsky-P.** Nejde ovšem o klasický vir, ale spíše o červa, který se šíří pomocí elektronické pošty. Po otevření dopisu se tento červ nakopíruje do složky Windows pod jménem FVPROTECT.EXE a změní údaje v registru Windows. Poznáte to tak, že v klíči HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ najdete položku Norton Antivirus AV.

Jeho binárním příbuzným je **Win32/Netsky-B,** který se šíří podobným způsobem – elektronickou poštou a sdílením v P2P sítích. Po spuštění infikovaného souboru se na obrazovce objeví chybové hlášení „The file could not be opened!“. Poté se do adresáře Windows zkopíruje pod jménem „services.exe“ a do registrů (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) přidá klíč pro spuštění souboru "services.exe" při startu Windows. Červ se

poté kopíruje do složek obsahujících ve jménu slova share nebo sharing.

Třetím kandidátem hodným vaší pozornosti je **Win32/Zafi-D.** Jde také o e-mailového červa, který ovšem kromě „rozmnožování“ plní také funkci trojského koně. Dokáže totiž vypínat bezpečnostní programy a znemožňuje spouštění nástrojů pro správu procesů a úpravu registrační databáze. Je schopen se šířit i P2P sítěmi. Po spuštění vytvoří červ soubor „Norton Update.exe“ a několik dalších souborů s náhodnými jmény a příponou .dll v systémovém adresáři (Windows\System nebo Windows\System32) s vlastními kopiemi a dále datový soubor C:\S.cm. Další vlastní kopie se jmény „winamp 5.7 new!.exe“ a "ICQ 2005a new!.exe“ červ vytváří v adresářích, jejichž jména obsahují řetězec „shar“. Tato vlastnost umožňuje červu šířit se pomocí P2P sítí.

Červa můžete identifikovat podle položky v registrech – v klíči HKLM\Software\Microsoft\Windows\CurrentVersion\Run najdete položku Wxp4, která má hodnotu %System%\Norton Update.exe.

Nová krev

Čas se nezastavil ani u autorů virů. Mezi novinkami se objevil například **Pe_Kitty-kat.A.** Ten patří mezi klasické viry šířící se pouze spuštěním nakaženého souboru. Tento vir se skrývá v souboru s příponou rar a k jeho aktivaci je nutné spustit v něm ukrytý soubor start.bat. Ohroženy jsou systémy Windows 2000/XP/Server 2003, ve kterých může vir nakazit další rar archivy.

O něco nebezpečnější novinkou je Troj_Arhiveus.A, který si můžete stáhnout z vybraných serverů na internetu. Jak už název napovídá, jde o trojského koně napadajícího operační systémy Microsoftu – od Windows 98 až po Windows XP. Jeho identifikace není příliš obtížná – nejprve vytvoří image všech souborů ve složce My Documents, které pak smaže. Posléze se začnou objevovat hlášení typu „READ INSTRUCTIONS HOW TO GET YOUR FILES BACK“, která vám napoví, že heslo dostanete e-mailem, až si něco koupíte ve vybraném internetovém obchodu.

Posledním nováčkem, o kterém se zmíníme, bude další varianta červa WORM_BAGLE, tentokrát s koncovkou eo **(Worm_Bagle.Eo)**. Tento červ (známý také jako Trojan.Lodear.D) se šíří jak elektronickou poštou (jako příloha), tak i P2P sítěmi. Rozesílá se na adresy z vašeho mailboxu a také vytvoří kopie, které nakopíruje do složek obsahujících řetězec SHAR. Po „dokončení práce“ se virus zkopíruje do složky Windows pod jménem winhost.exe a do registrů přidá klíč zajišťující jeho automatické spuštění po startu.

Info: *www.avast.com*

Žebříček nejrozšířenějších virů

Kdo nás trápí?

Společnost Panda Software zveřejnila dubnový žebříček nejrozšířenějších virů, sestavený na základě detekce bezplatného antivirového řešení Panda ActiveScan *(www.activescan.com).*

Duben byl z hlediska aktivity škodlivých kódů poměrně klidný. Nejčastěji detekovanou hrozbou se stal opět skript z rodiny Sdbot. Na druhém místě můžete najít dva roky starého červa jménem Netsky.P a třetí místo "obhájil" kód Metafile, využívající zranitelnost WMF souborů ve Windows. Tento žebříček opět potvrdil starou pravdu o tom, že nejrozšířenější škodlivé kódy ve velké míře využívají starší zranitelnosti, a také to, že velká část uživatelů používá svůj počítač (připojený k internetu) bez jakékoliv aktualizace. Tím se stává zdrojem šíření dalších nebezpečných kódů a potenciálním ohrožením každého z nás.

Název viru	Incidenty [%]
W32/Sdbot.ftp	2,1
W32/Netsky.P.worm	1,1
Exploit/Metafile	0,8
Trj/LowZones.RI	0,6
W32/Tearec.A.worm!CME-24	0,6
Trj/Qhost.gen	0,5
Trj/Torpig.AY	0,5
W32/Parite.B	0,5
Trj/Torpig.AZ	0,5
W32/Gaobot.gen.worm	0,5

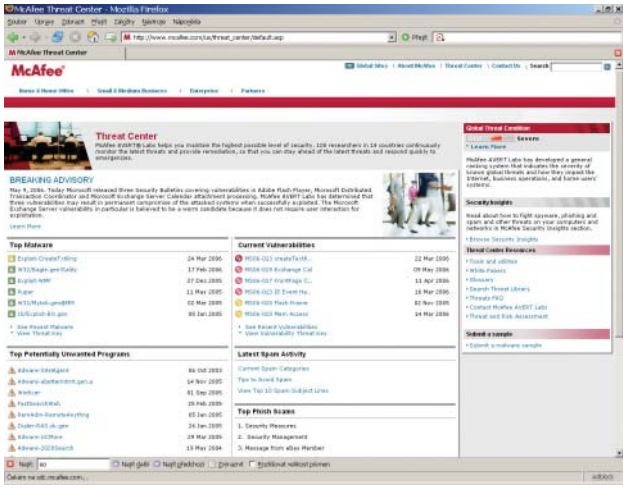
Nový bezpečnostní portál

Vše o bezpečnosti

Společnost McAfee, Inc., představila nový centrální portál hrozeb – Threat Center Portal. Tento portál nabízí přístup k nejaktuálnějším informacím, nástrojům a hodnocením zranitelností, dále pak varování před malwarem, phishingem, spamy a hoaxy. Threat Center je součástí nově upravených webových stránek, které najdete na adrese *www.mcafee.com/us/threat_center/default.asp*.

Nejdůležitější součásti nabídky portálu:

- zjednodušená navigace k informacím o hrozbách sledovaných McAfee AVWERT® Labs;
- Library – knihovna obsahující databázi AVERT týmu. Obsahuje definice více než 180 000 malwarů, zranitelností, hrozeb a potenciálně nevyžádaných programů;
- nové informace o spamu, phishingu a zranitelnostech – zahrnují kategorie spamů, tipy, na které spamy si dát pozor, přehled top ten nejčastějších názvů předmětů ve spamu, současné zranitelnosti a největší phishingové podvody;
- Security Insights – bezpečnostní přehledy. Nová sekce poskytující aktuální a důležité názorové články expertů ze společnosti McAfee;
- Free Tools – volné nástroje ke kontrole a odstranění malwaru, popis DAT souborů a seznam malwaru;
- AVERT Virus Alerts – nabídková sekce pro registraci předplatného servisu zdarma, která přímo distribuuje aktuální informace včetně stupně ohodnocení hrozby.



Jednotlivé komponenty nové webové stránky McAfee budou nadále rozvíjeny a doplňovány během následujících měsíců. McAfee také připravuje nový design, strukturu i obsah chce postupně implementovat do regionálních stránek po celém světě.

Komentář redakce:
Na něco podobného už český internet čeká delší dobu. V současné době je jediným rozsáhlejším zdrojem „anglická" Secunia (http://secunia.com/), *české stránky jsou buď amatérské, nebo nabízejí pouze omezený rozsah informací. Bezpečnostních informací chtivý Čech tak musí sledovat Igiho* www.viry.cz *a stránky Microsoftu* (www.microsoft.com/technet/security/current.aspx).

BUFFER OVERFLOW

Servant Salamander

Secunia Research objevila *(http://secunia.com/advisories/19612/)* zranitelnost v unacev2.dll souboru, jenž je součástí Servant Salamanderu. Zranitelnost je způsobena chybou při rozbalování ACE archivu obsahujícího příliš dlouhý název souboru. Při úspěšném zneužití dojde k tzv. BO chybě a k potenciálnímu spuštění cizího kódu. Chyba byla potvrzena ve verzích 2.0 a 2.5 beta 11 a opravena ve verzi 2.5 RC1
Info: *zpravy.actinet.cz*