Příručka mladých svišťů

Bobřík bezpečnosti

V poslední době se v našich redakčních e-mailových schránkách množí dotazy na volbu „dobrého“ bezpečnostního softwaru. Pojďme se podívat, co na tuto problematiku říká příručka mladých svišťů.

Text: Petr Kratochvíl, *petr.kratochvil@chip.cz*

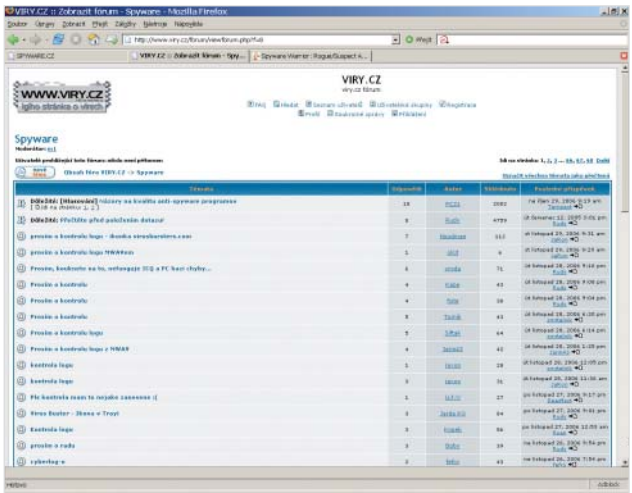
Zvolit ten správný bezpečnostní software není snadná záležitost. Ano, lze pochopitelně vsadit na jistotu a zvolit „starou dobrou klasiku“ od firem jako Symantec, McAfee nebo Kaspersky. Touto volbou určitě neprohloupíte, nicméně i zde lze narazit na určitá rizika. Stačí se jen podívat na server Secunia (www.secunia.com), kde lze najít i údaje o bezpečnostních mezerách v programech. Žádný ze zmiňovaných mohykánů nemá úplně čistý štít. Druhým zádrhelem je paradoxně jejich rozšíření. Protože je najdete „na každém druhém“ počítači, hackeři se na jejich prolomení mohou pořádně připravit. Ať už hledáte firewall, antivir, nebo antispyware, nemusí vám řešení od některého z gigantů vyhovovat. Je tedy čas na volbu méně známého bezpečnostního produktu? Pojďme si prolistovat výše zmiňovanou příručku.

Provaz nutností

Výběr dobrého programu je dobré neuspěchat. Proto si připravte pořádný kus provazu, který použijeme jako pomůcku pro rozhodování. Za každou drobnost, naznačující, že vybraný program by mohl být ten pravý, uděláme na provazu námořnický uzlík (viz bobřík vázání uzlíků). Pokud budete mít na konci rozhodování na provazu více než sedm uzlíků, můžete si s klidem program do počítače nainstalovat.

Zamotaný úvod

První uzlík si můžete zavázat, pokud má program svou kvalitní domovskou stránku. Za pojmem „kvalitní“ nehledejte žádný chyták – stačí se jen vyhnout stránkám typu „ahoj jsem džon, mám rád ferrari a taky jsem naprogramoval tenhle bezva antispyware program...“. Další uzlík můžete přidat, pokud na stránkách najdete historii verzí s podrobným seznamem oprav a bezpečnostních vylepšení. Není nic horšího než instalace první verze „rádobyskvělého“ programu s desítkou neobjevených chyb. Hned dva uzlíky přidejte, má-li výrobce na webu i diskusní fórum, na kterém se řeší problémy a hodnotí novinky. Všimněte si, zda nechybí i kritické příspěvky – promazávání kritiky nesvědčí o příliš vysoké úrovni autorů. Pokud se to navíc ve fóru jen hemží reklamními příspěvky lákajícími k nákupu viagry nebo k bezbolestnému prodloužení penisu, můžete jeden uzlík s klidným svědomím rozvázat. V tuto chvíli je asi vhodné podotknout, že pokud si nejste svým bezpečnostním kandidátem příliš jisti, doporučujeme vám uzlíky příliš neutahovat...



Diskusní fórum Viry.cz: **Pokud nenajdete odpověď zde, bude váš problém oříškem...**

Riziko je tu vždycky...

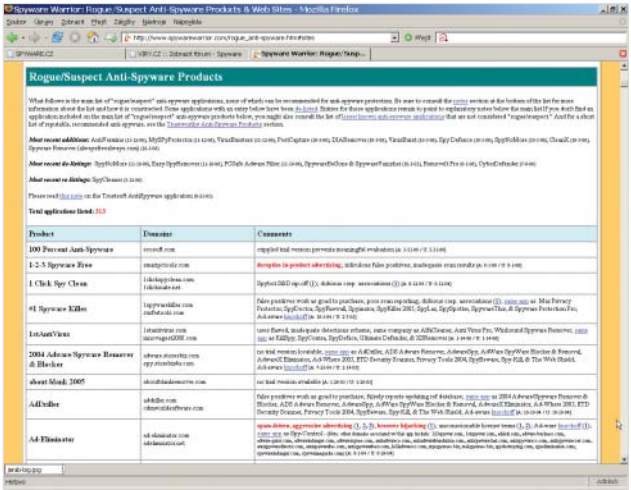
Volba programu nemusí být vždy jen záležitostí zhodnocení kladů a záporů nebo osobních preferencí. Poslední dobou se začínají množit i falešná „bezpečnostní upozornění“, která se vás především snaží nalákat na nebezpečnou „domácí stránku“ falešného bezpečnostního programu. Pokud se vám tedy po návštěvě stránky změnila domovská stránka, do IE se nainstalovaly dvě nové lišty a při surfování jste neustále zahlcováni reklamou, okamžitě zahoďte provaz a utíkejte, jak nejrychleji umíte.

Nutné uzlíky

Další zastávkou na vaší cestě za bobříkem bezpečnosti by měl být web Spyware Warrior, respektive stránka *www.spywarewarrior.com/rogue_anti-spyware.htm*. Už několik let patří tyto stránky mezi renomované zdroje v oblasti zabezpečení. My se sem vydáme zkontrolovat, zda vybraný program není v seznamu tzv. „rogue antispyware“. Pokud ho tam nenajdete, můžete si uvázat další uzlík. A jestliže na tomto serveru najdete o svém kandidátovi dokonce pozitivní zmínku, můžete uvázat hned dva uzlíky. Ti, kdo neumí anglicky, navštíví alespoň české servery *www.viry.cz*, *www.spyware.cz* a *http://trojanhelp.wz.cz/*. Na těchto stránkách (a především na diskusních fórech) najdete celou řadu informací, které pomohou při výběru dobrého bezpečnostního programu. „Uzlíky“ zde sice nezískáte, na druhou stranu zase máte jistotu, že nebudete muset rychle utíkat...

Kdo hledá...

Server www.spywarewarrior.com je sice rozsáhlým zdrojem informací a věnuje se i méně známým programům, ale ani zde nenajdete vše. A to je příležitost pro Google, aby vyčmuchal i to, co autoři chtějí skrýt. Nejprve zadejte (nejlépe jako slovní spojení) přesné jméno vámi zvoleného programu a zkuste najít ohlasy a reference. Poté postupně zkoušejte hledat kombinace, které by vám mohly prozradit potenciální slabiny nebo přímo rizika při jeho používání. Typickými dotazy tak mohou být: xxxxxxx problems (pokud se chcete dozvědět



Rogue Anti-Spyware: **Místo slibované ochrany vám tyto produkty spíše uškodí...**

o komplikacích při používání); xxxxxxx trojan (není v programu trojský kůň nebo backdoor, neobsahuje program spyware?).
Pro vyšší efektivitu vyhledávání doporučujeme použít další operátory (AND, NEAR...) zjednodušující nalezení lepších zdrojů informací.

Jak hodnotí okolí?

Ve chvíli, kdy vašemu čmuchání na internetu odolaly pouze korejské a čínské weby, a přesto jste nic kompromitujícího nenašli, můžete si na svém hodnoticím laně uvázat další uzlík. Poslední návštěvou by měly být renomované weby se softwarem (nabízející od freewaru přes shareware až po trial verze renomovaných produktů), kde se poohlédněte po hodnocení vašeho kandidáta. Za každou hvězdičku „nad tři“ (na serverech typu Download.com) nebo kravičku (na serverech Tucows.com) si může udělat jeden uzlík. ■ ■ ■

OPERAČNÍ SYSTÉMY A ZRANITELNOSTI

Mac OS X

Chyba ve zpracování DMG image

Plně zaplátovaný operační systém Mac OS X obsahuje zranitelnost ve zpracování DMG image, které obvykle obsahuje aplikace k instalaci. Při spuštění záškodně upraveného DMG image může dojít k tzv. „Memory Corruption“ a možnosti vykonat kód na uživatelově systému. Na tuto chybu už byl zveřejněn exploit, proto doporučujeme následující opatření: v internetových prohlížečích vypněte volbu „opening safe files after downloading“. Podrobnější informace naleznete například na *http://projects.info-pull.com/mokb/MOKB-20-11-2006.html*.

Info: *zpravy.actinet.cz*

Microsoft Windows

Důležité záplatování

Společnost Microsoft vydala dalších šest záplat pro své systémy. Tentokrát jde ale o záplaty na velmi závažné zranitelnosti, pět z nich je klasifikováno jako „critical“ a poslední nese označení „important“. Dvě ze zranitelností jsou v současné době aktivně zneužívány. Více informací a odkazy na podrobnosti naleznete v bulletinu Microsoftu *(www.microsoft.com/technet/security/bulletin/ms06-nov.mspx)*.

Info: *zpravy.actinet.cz*

ZRANITELNÉ PROGRAMY

Nové bezpečnostní mezery

Microsoft Office

Záplaty mezer

Microsoft zveřejnil tři záplaty kritických mezer v MS Office. Krátce předtím, než přijdou na trh Windows Vista a Office 2007, musí koncern ještě napravovat staré hříchy – po internetu koluje škodlivý kód. Řešením je neodkladná instalace aktualizací!
Info: *www.microsoft.com*

Internetová fóra

Prolomená ochrana

Internetová fóra se nyní ocitají pod silnější palbou. Hackeři v příslušných mailing listech zveřejnili kritické mezery pro Invision Power Board, WoltLab Burning Board a phpBB. Řešením je alespoň dočasné vyhýbání se stránkám s neopravenými fóry.
Info: *www.securityfocus.com*

AVG Anti-Virus

Vzdálené spuštění kódu

Problémy se tentokrát nevyhnuly ani oblíbenému antiviru od Grisoftu. AVG Anti-Virus verze starší než 7.1.407 totiž obsahuje více vzdáleně zneužitelných chyb, které dovolují útočníkovi spouštět kód na systému uživatele. Více podrobností naleznete na stránkách komunity bezpečnostních profesionálů SecurityFocus *(www.securityfocus.com/bid/21029)*. Řešením je aktualizace na novější verze, podle pokynů na webu výrobce na *www.grisoft.cz*.
Info: *zpravy.actinet.cz*

Wikipedia

Phishing útočí

Pověstná „Nigeria Connection“ má novou phishingovou strategii. Aby svým mailům propůjčila zdání legitimity, odkazuje skupina na předem zmanipulované položky Wikipedie v anglické části on-line lexikonu. Řešení je prosté – stačí přezkoušet položky pomocí jiného zdroje, jako je například Encarta Online.
Info: *www.wikipedia.org*

Firefox

Password manažer ohrožen

Byla oznámena zranitelnost webového prohlížeče Firefox *(http://it.slashdot.org/article.pl?sid=06/11/21/2319243&from=rss)*, spočívající v nedostatečné kontrole URL password manažerem Firefoxu před automatickým vyplněním hesla do webového formuláře. Zranitelnost může být zneužita k podvodnému získávání hesel zákeřnými formuláři umístěnými na WWW stránkách ve stejné doméně jako legální formuláře, kterých obsah má password manažer uložen. Možnou obranou je zakázání zapamatovávání hesel v nastavení prohlížeče.
Info: *zpravy.actinet.cz*

Bezpečnostní monopol

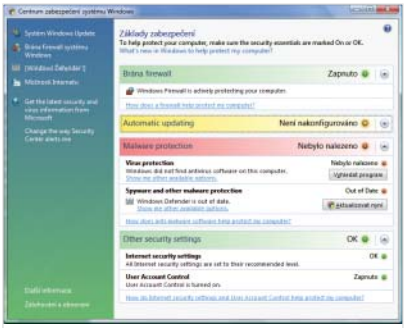
Symantec: Vista blokuje bezpečnostní balíky

Protože bude operační systém Windows konečně bezpečný, nebude se smět v Evropě prodávat. Zní to paradoxně, ale mohlo by se to stát skutečností, pokud bezpečnostní firmy jako Symantec nebo McAfee svou stížnost, kterou pohrozily, skutečně předloží Evropské komisi. Namítají totiž, že Microsoft omezuje volnou soutěž na trhu v oblasti bezpečnosti informačních technologií.

Bezpečnost jenom od Microsoftu?

Spor spočívá ve skutečnosti, že nová funkce ve Windows Vista „Kernel Patch Protection“ znemožňuje přístup do jádra operačního systému. Microsoft se tak snaží zabránit neplechám hackerů a škodlivého softwaru – blokuje tak však zároveň i činnost externích bezpečnostních souprav. Například Symantec tvrdí, že kvůli tomuto obrannému mechanismu nebude moci nasadit technologie jako „behavior blocking“ (rozpoznávání malwaru na základě jeho chování). Až dosud měl Symantec přístup přímo k jádru a mohl v něm tak sledovat každou probíhající akci počítače. Je-li přístup znemožněn, taková ochrana už ovšem nefunguje. Symantec proto od Microsoftu požaduje otevřené rozhraní, které potřebný přístup nadále umožní. Ne všechny bezpečnostní firmy v tom ale spatřují problém: například Sophos podle vlastního vyjádření k účinné ochraně počítače žádný přístup do jádra nepotřebuje.

McAfee a Symantec kromě toho kritizují „bezpečnostní centrum“, které do Windows XP zavedl Service Pack 2 a které je ve Windows Vista už pevnou součástí. S novým operačním systémem je centrum tak pevně provázáno, že se nedá odstranit a nahradit jiným bezpečnostním softwarem – což podle názoru zmíněných firem zjednává Microsoftu konkurenční výhodu odporující pravidlům obchodní soutěže. Pokud si uživatel přesto nějakou bezpečnostní soupravu koupí a nainstaluje, musí se pak potýkat se dvěma různými bezpečnostními centry – a s varovnými zprávami, podle okolností třeba i protichůdnými.



Kámen úrazu: **Bezpečnostní centrum ve Windows Vista nelze odstranit a nahradit jiným bezpečnostním softwarem.**

Pro uživatele tyto spory prozatím žádné důsledky nemají: dokud není systém Vista na trhu, nemůže Evropská komise proti Microsoftu nic podniknout.
Info: *www.symantec.com*

PHISHING

Nezabezpečená čísla transakcí u Citibank

Práce s čísly PIN/TAN v on-line bankovnictví je bezpečná jen do té doby, dokud hacker nemá k dispozici seznam transakcí. Právě z tohoto důvodu je u Citibank seznam čísel transakcí generován náhodně. Avšak už první pohled na tento seznam ukáže, že „náhodnost“ TAN zde není dostatečná. Program, který čísla transakcí vytváří, totiž nevyužívá celý číselný prostor, který má k dispozici. Dokonce i laik pozná, že jednotlivá TAN leží velmi těsně u sebe. To ovšem drasticky zvyšuje šanci platné číslo transakce uhodnout – dokonce i poté, co bylo spotřebováno. Definitivní důkaz o nedostatečném zabezpečení těchto čísel poskytl hacker Felix „FX“ Leitner ze Sabre Security pomocí jednoduchého programu v Perlu, který nejistotu naprosto jasně ukazuje.
Info: *www.citibank.com*

TROJSKÉ KONĚ

Falešný antispyware v oběhu

Když jde o šíření malwaru, je internetové mafii každý prostředek dobrý. Zvláště podlým trikem je zamaskovat spyware jako prostředek proti spywaru. Jak sděluje bezpečnostní firma Sunbelt Software, skupina, od níž už pochází i spyware „SpySheriff“, dala

do oběhu novou pohromu: software nazvaný „PestCapture“ slibuje, že se spywarem učiní krátký proces. Ve skutečnosti však nainstaluje tytéž „trojské“ DLL soubory jako už jeho předchůdce „SpySheriff“. Jakmile se jednou usídlí v systému, klame důvěřivého uživatele hned dvěma způsoby: za prvé požaduje 80 dolarů za „lifetime-account“, za druhé nejen že nehledá a neodstraňuje spyware a adware, nýbrž je přes bezpečnostní mezery dokonce instaluje.

Info: *sunbelt-software.com*

GRISOFT

AVG Rescue CD

Grisoft uvedl na konci listopadu na trh AVG Rescue CD, produkt určený IT profesionálům pro záchranu zavirovaných a jinak napadených počítačů s operačním systémem Windows XP a Server 2003. AVG Rescue CD vychází z aktuální verze AVG Anti-Malware 7.5 a stejně jako tento produkt nabízí možnost přímé aktualizace virových a spywarových definic při spuštění.

„AVG Rescue CD přináší profesionálům nástroj, který usnadní odstraňování nebezpečných programů a kódů z napadených počítačů, a to s plnou podporou, která je u produktů AVG standardem,“ uvedl Karel Obluk, technický ředitel a jednatel společnosti Grisoft. „AVG Rescue CD navíc přináší možnost aktualizovat databázi škodlivých kódů po spuštění záchranného CD; doposud bylo nutné CD s aktuální virovou databází vypálit předem.“

Produkt AVG Rescue CD je založen na operačním systému MS Windows PE a obsahuje antivirus, antispyware a komplexní sadu administrátorských nástrojů. Mezi podporované funkce patří správa souborů, editor záznamů registrů operačního systému Windows, testování integrity pevných disků a možnost detailní konfigurace síťového prostředí. AVG Rescue CD je dostupný jak v obchodech, tak i prostřednictvím partnerů a distributorů společnosti Grisoft, a to za 3490 Kč. Majitelé platné licence na jakýkoliv komerční produkt AVG mohou AVG Rescue CD získat za zvýhodněnou cenu 2490 Kč. AVG Rescue CD je nabízen pouze s jednoletou licencí.

SYMANTEC CORP.

Norton pro Vistu

Společnost Symantec Corp. oznámila dostupnost veřejných beta verzí aplikací Norton Internet Security 2007 a Norton AntiVirus 2007, kompatibilních s operačním systémem Windows Vista. Tyto bezpečnostní nástroje jsou určeny k proaktivní ochraně počítačů před širokou řadou on-line hrozeb, včetně spywaru, virů, červů, hackerů, phishingových webů a crimewaru. Uživatelům, kteří mají nainstalovanou beta verzi operačního systému Microsoft Vista, jsou veřejně k dispozici beta verze aplikací Norton Internet Security 2007 a Norton AntiVirus 2007, které jsou připraveny ke stažení na adrese *www.symantec.com/home_homeoffice/publicbeta/index.jsp*.

Předpověď McAfee

Hrozby pro rok 2007

Společnost McAfee, Inc., a její laboratoře Avert Labs oznámily svou předpověď deseti největších bezpečnostních hrozeb pro rok 2007.

Více webových stránek pro zcizení hesel

V roce 2007 se objeví ještě více útoků, jejichž cílem je prostřednictvím falešných přihlašovacích stránek získat přihlašovací jména a hesla uživatelů služeb. Tyto útoky se zaměří hlavně na populární on-line služby, jako je např. eBay. Po zkušenostech s phishingovými útoky po hurikánu Katrina McAfee Avert Labs také očekávají další útoky využívající ochoty lidí pomáhat druhým.

Více spamu obsahujícího obrázky

V listopadu 2006 tvořil spam obsahující obrazové soubory 40 % celkového množství spamu, před rokem to bylo méně než 10 %. V posledních několika měsících zaznamenal obrazový spam velký nárůst a některé jeho druhy, například výzvy k nákupu akcií, léků a falešných univerzitních diplomů, se nyní objevují výhradně v této podobě. „Obrázkový spam“ zabírá až třikrát více místa než srovnatelná textová informace, takže tento vývoj představuje značné zvýšení kapacity připojení, které spamy zabírají.

Sdílení videa zneužité hackery

Rostoucí popularita videosouborů na výměnných serverech, jako je MySpace, YouTube a VideoCodeZone, bude jistě přitahovat autory malwaru usilující o snadný přístup do rozsáhlých sítí. Na rozdíl od podezřelých souborů zasílaných v příloze e-mailů otevírá většina uživatelů multimediální soubory bez zaváhání. Video je také lehce použitelný formát a autoři malwaru se pravděpodobně zaměří na další funkce, jako je padding, pop-up reklamy a přesměrování na jiné internetové stránky. Kombinace těchto nástrojů umožní autorům malwaru efektivně využít multimediální soubory k šíření svých útoků.

Rozšíření útoků na mobilní telefony

S pokračováním konvergence různých platforem bude docházet i k nárůstu útoků na mobilní telefony. Používání technologie smartphone hraje klíčovou úlohu v procesu migrace hrozeb ze stacionárních nebo přenosných počítačů na ruční a kapesní přístroje. S rostoucí konektivitou přes Bluetooth, SMS, instant messaging, e-mail, Wi-Fi, USB, audio, video a internet se zvyšuje počet možností pro napadení různých druhů přístrojů.

Adware se stane normou

V roce 2006 zaznamenaly McAfee Avert Labs vzestup komerčních PUP programů, doprovázený ještě větším množstvím trojských koňů, keyloggerů, krádeží hesel, botů a „zadních dveří“. Kromě toho roste i počet zneužití komerčního softwaru pomocí malwaru s dálkově ovládaným nasazením adwaru, keyloggerů a dálkově ovládaného softwaru.

Krádeže identity a ztráty dat budou pokračovat

Podle americké Federal Trade Commission se obětí podvodů s falešnou identitou stane každý rok zhruba 10 milionů Američanů. Tyto podvody jsou často umožněny krádeží počítačů, ztrátou záloh nebo nedostatečně chráněnými informačními systémy.

Rozšíří se používání botů

Boty, programy, které provádějí automatické operace, jsou na vzestupu, avšak očekává se jejich odklon od Internet Relay Chat (IRC) komunikačních mechanismů k méně nápadným metodám. V posledních několika letech se komunita virových autorů zaměřila zvláště na IRC kanály. Byl to důsledek přístupnosti IRC skriptů a relativní snadnosti koordinace infikovaných počítačů ze struktur chatových serverů.

„Mezci“ (Mules) se rovněž zařadí mezi důležité aspekty výdělečné činnosti související s boty. „Mezci“ jsou lákáni na práci z domova, která je nabízena profesionálně vypadajícími internetovými stránkami, inzeráty, a dokonce instant messaging programy. To je důvodem, proč tolik botů funguje z mnoha míst na světě. Při nákupu zboží za účelem dalšího prodeje a při získávání peněz pomocí kradených údajů z kreditních karet se zločinci musí podrobit přísnější kontrole, pokud takové zboží či peníze zasílají přes hranice. Aby tomu zabránili, používají „mezky“ v zemích původu.

Vzroste podíl parazitického malwaru

I když parazitující malware představuje jen 10 % veškerého malwaru (90 % malwaru je statického typu), vypadá to, že se do našich počítačů opět vrací. Parazitující viry jsou viry, které modifikují stávající soubory na disku a přidávají do nich škodlivý kód. Když uživatel takto infikovaný soubor otevře, je spuštěn i virus. Příkladem jsou W32/Bacalid, W32/Polip a W32Detnat, tři polymorfní parazitické infikátory souborů.

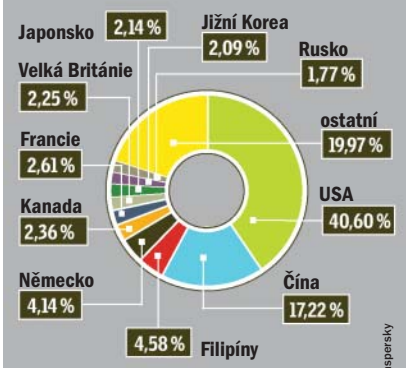
Zvýší se počet rootkitů pro 32bitové platformy

Zároveň se však zlepší ochrana před nimi. Bohužel pro 64bitové platformy, hlavně Windows Vista, jsou trendy v oblasti ohrožení malwarem těžko předvídatelné. Předpokládá se však také alespoň krátkodobý pokles počtu kernel-mode rootkitů, než autoři malwaru vyvinou nové techniky pro překonání PatchGuardu

Více slabých míst v OS

V roce 2007 očekáváme další zvýšení počtu známých slabých míst. V průběhu roku 2006 oznámil Microsoft v rámci svého měsíčního patch programu již 140 slabých míst. McAfee Avert Labs očekávají, že v důsledku zvýšeného používání fuzzer programů, které dovolují velkoobjemové testování aplikací, a odměn lidem, kteří slabá místa objeví, se počet těchto oznámení ještě zvýší. Do září 2006 již Microsoft vyřešil více kritických slabých míst než v letech 2004 a 2005 dohromady.

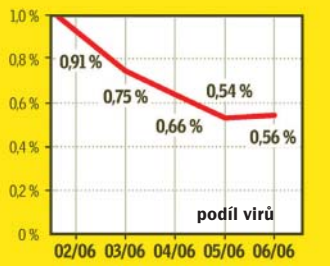
Země hackerů v roce 2006



Zdroj: Kaspersky

Překvapení: Z Ruska přichází velmi málo útoků – vedou USA a Čína.

Spam bez virů



Zdroj: www.symantec.com

Trend: Spam přestává používat viry k oklamání filtrovacích programů.

On-line ochrana

ActiveScan zdarma proti rootkitům

Firma Panda Software připravila novou verzi bezplatného on-line řešení Panda ActiveScan, které nyní dokáže nejen detekovat a eliminovat viry, trojské koně a spyware, ale i detekovat a dezinfikovat rootkity. Tuto novou verzi najdete na adrese *www.activescan.com*.

Panda ActiveScan je on-line antivir, který kontroluje a dezinfikuje vybrané složky, disky, komprimované soubory nebo e-maily – to vše pochopitelně zdarma. Česká verze bohužel není k dispozici, uživatelé bez znalosti angličtiny však určitě ocení „slovenskou verzi“, kterou najdete na *www.pandasoftware.sk*.

Nový ActiveScan obsahuje modul genetické heuristiky. Jedná se o technologii genetické detekce, která spojuje princip závislosti digitálního genetického podpisu a hloubkového zkoumání kódu algoritmem, jenž analyzuje kód a DNA charakteristiky škodlivého kódu. Modul genetické heuristiky je součástí technologie TruPrevent, proaktivních technologií vyvinutých firmou Panda Software pro rychlou detekci neznámých hrozeb. Nová verze Panda ActiveScan je již nyní plně kompatibilní s Microsoft Internet Explorerem 7.

ActiveScan: Rychlou instalaci a snadné použití scanneru ocení nejen začátečníci.

TREND MICRO

Ochrana nejen pro váš mobil

Společnost Trend Micro rozšířila řešení Mobile Security o nové funkce. Nová verze nyní blokuje malware a pomáhá zabraňovat nežádoucím průnikům a únikům dat prostřednictvím nového firewallu a nové technologie detekce útoků. Řešení Trend Micro Mobile Security 3.0 nejen rozšiřuje ochranu před hackery, ale zároveň vylepšuje dosud dostupnou ochranu před nebezpečnými mobilními kódy, malwarem a nevyžádanými zprávami SMS.

Společnost IDC předpokládá, že dodávky „mobilních zařízení“ dosáhnou v roce 2006 téměř 100 milionů jednotek a počet hrozeb zaměřených na tato zařízení neustále poroste. Vzhledem k rostoucímu šíření telefonů smartphone, ke zvyšující se dostupnosti sítí Wi-Fi a možnostem rychlejšího stahování vzrůstá nebezpečí vážnějšího útoku.

Řešení Mobile Security 3.0 se vyznačuje snadným používáním a nabízí uživatelům jednoduché rozhraní pro zajištění maximálního zabezpečení. Nové funkce firewallu a detekce průniku pomáhají blokovat nebezpečné útoky prostřednictvím ochrany, kterou lze nastavit na nízký, střední nebo vysoký stupeň s rozšířenou možností blokování konkrétních IP adres a portů. Řešení Trend Micro Mobile Security 3.0 pro operační systém Windows Mobile 5.0 (telefony smartphone a kapesní počítače) je k dispozici za cenu od 34,95 USD za zařízení. Řešení Trend Micro Mobile Security 3.0 pro operační systém Symbian/S60, 3. vydání, bude dostupné v roce 2007. Další informace a úplný seznam podporovaných zařízení je k dispozici na webu *www.trendmicro.com/mobilesecurity*.