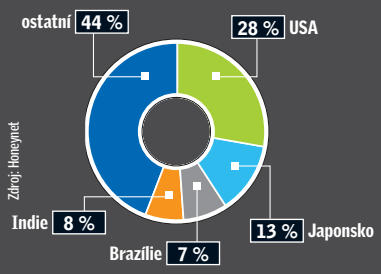
Barometr nebezpečí

Spam v blozích a fórech



Podobně jako u e-mailů jsou USA i v čele seznamu šiřitelů spamu v blozích a fórech.

Malwarový Top-ten

Malware	podíl v %
Troj/Pushdo	35,8 %
W32/Netsky	28,1 %
W32/Mytob	6,9 %
W32/Strati	5,3 %
Mal/Dropper	5,2 %
W32/Zafi	4,9 %
W32/MyDoom	3,5 %
Troj/Dloadr	2,6 %
W32/Bagle	1,7 %
W32/Sality	0,8 %
ostatní	5,2 %

Zdroj: Soplos

Dominuje stahovač Pushdo, který zavádí nové trojské koně.

BEZPEČNOSTNÍ WEB CHIPU

www.chip.cz

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

Nebezpečný trojský kůň si podmaní Windows

Za programem se zvučným jménem Backdoor Guard se skrývá „rogue antispyware" – tedy software, který jen předstírá, že počítač chrání. Žádný neobvyklý trik, jenomže tento malware se posléze projevil jako opravdu nebezpečný. Jakmile je program jednou nainstalován, zcela v rozporu se svým názvem otevře zadní vrátka a jeho programátor pak kdykoli získá přístup do infikovaného systému.

Backdoor Guard svou oběť navíc vydírá

Totální kontrola nad napadeným počítačem však tomuto gaunerovi zjevně nestačí. Jakmile oběť po instalaci programu počítač restartuje, škůdce zablokuje ovládací plochu a otevře webovou stránku, na níž se tvrdí, že byly zjištěny problémy s licencí – a že je nutno zatelefonovat na udané (samozřejmě vysoce zpoplatněné) číslo. Tento špás přijde oběť na 20 eur – programující zločinec si kvůli tomu dokonce zřídil německé číslo s předvolbou 0900. Na zmíněné webové stránce se zobrazí číslo PIN, které je nutno uvést při zavolání. Pak – tolik slib – obdrží volající aktivační číslo, jímž je možno zablokovanou plochu opět uvolnit. Ten, kdo nesídlí v Německu, a proto tam nemůže volat, musí použít satelitní číslo v USA. Pak je telefonát dokonce ještě dražší.

Složité pátrání: Komu patří číslo 0900...?

Německá zpoplatněná nebo také služební čísla a jejich poskytovatelé jsou vedeni ve vyhledávači Spolkové síťové agentury (dříve Regulační úřad pro telekomunikace a poštu). To má umožnit rychle přijít na stopu případnému zneužití. V případě čísla pro Backdoor Guard se však tato cesta ukázala málo schůdná. Údajně se totiž jedná o číslo poskytovatele služeb Atlas Interactive Deutschland. Po dotazu Chipu nás však firma odkázala na rakouského providera eTel Austria.

Ani od něj jsme ale až do redakční uzávěrky neobdrželi odpověď na dotaz, kdo je vlastně za inkriminované číslo odpovědný. Bylo nám však alespoň přislíbeno vyšetření celé věci.

„Trojana" se lze ostatně snadno zbavit: spusťte XP v nouzovém režimu a poté vymažte soubor locker.exe ve složce Windows.

Info: www.chip.cz

ZÁKEŘNOST: Trojský kůň ZeuS nepozorovaně připojí nebezpečný odkaz ke každému příspěvku do internetového fóra, který uživatel vytvoří.

UPGRADE PRODUKTU

První vlaštovka pro Vista SP1

Vzpomínáte si na problémy, které celé řadě uživatelů způsobil Service Pack 2? Nefunkční programy, problémy se stabilitou... Nejvíce „postižen" byl bezpečnostní software. Zdá se, že na SP1 pro Vistu jsou firmy připraveny lépe.

Například společnost Trend Micro již ohlásila vydání aktualizovaných verzí svých spotřebitelských produktů pro rok 2008: Trend Micro Internet Security Pro, Trend Micro Internet Security 2008 a Trend Micro AntiVirus plus AntiSpyware 2008. Nejnovější verze již plně využívají výhod servisního balíčku Windows Vista Service Pack 1.

„Společnost Trend Micro úzce spolupracovala s Microsoftem, aby naše bezpečnostní produkty byly optimalizovány pro Windows Vista SP1," uvedla Carol Carpenterová, viceprezidentka společnosti Trend Micro pro spotřebitelský marketing a produktový management. V případě stávajících uživatelů spotřebitelských produktů Trend Micro 2008 na Windows Vista platí, že jejich produkty se prostřednictvím funkce Trend Micro Automatic Update automaticky aktualizují na verzi 16.10. Zákazníci, kteří chtějí zjistit, zda mají poslední verzi, mohou kliknout na tlačítko Help & Support na hlavní konzole a poté kliknout na Product Information.

Nová bezpečnostní rizika

REALPLAYER

Vysoce kritická bezpečnostní mezera nyní ohrožuje uživatele softwaru RealPlayer 11. Prostřednictvím zmanipulovaných mediálních souborů mohou útočníci propašovat do počítače škodlivý kód. Mezera už je využívána ke kriminálním účelům. Chybu odstraní aktualizace na aktuální verzi.
Info: **www.real.com**

FLASH VIDEA

Různé authoringové nástroje pro Flash generují animace náchylné k infiltraci škodlivým kódem. Hackeři by mezeru mohli využít k phishingovým útokům. K postiženým nástrojům patří i populární produkty jako Dreamweaver a Camtasia. Řešení je logické: bezpodmínečně aktualizovat Flash Player.
Info: **www.adobe.com**

MICROSOFT OFFICE 2003

V poslední aktualizaci deaktivuje Microsoft u některých souborových formátů možnost jejich otevření. Postiženy jsou tím hlavně starší verze CorelDraw a Lotus Notes. Opatření je zdůvodňováno bezpečnostními pochybnostmi. Microsoft proto doporučuje převést staré dokumenty na nový formát Office.
Info: **www.microsoft.com**

SYMANTEC DECOMPOSER

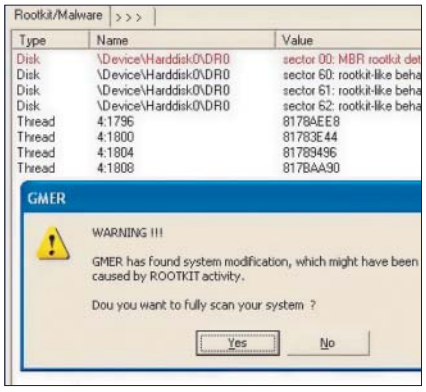
Symantec Decomposer obsahuje dvě chyby při zpracování RAR archivů, které mohou vést k pádu systému. Podrobnější informace o problému naleznete ve zprávě na **http://securityresponse.symantec.com.** Seznam aplikací postižených těmito chybami naleznete také v již zmiňované zprávě.
Info: **zpravy.actinet.cz**

ŠKODLIVÝ SOFTWARE

Nová technika rootkitů

Na internetu koluje velmi zvláštní nový škůdce: rootkit, který se zahnízdí v Master Boot Recordu (MBR) pevného disku. Poněvadž je proto škodlivý kód aktivní už před startem operačního systému, je MBR rootkit schopen rozvrátit a zmanipulovat všechna bezpečnostní opatření Windows. Jakmile je jednou nainstalován, změní rootkit funkce, které Windows poskytují pro přístup k souborům. Antivirové programy, které tyto funkce Windows využívají, pak už tedy nejsou schopny škůdce odhalit. Antirootkitový software Gmer tomuto triku čelí tak, že pro čtení obsahu disku používá ještě další nezmanipulovanou cestu.

Napadené počítače lze poměrně snadno zase vyčistit. Stačí k tomu přepsat MBR nástrojem fixmbr ve Windows. Co se však Microsoftu líbit nebude, je to, že techniku MBR rootkitu lze využít k proražení DRM a protikopírovací ochrany Windows.



Nová bezpečnostní rizika

ICQ 6

V populárním instant messengeru ICQ (verze 6.X) byla objevena kritická zranitelnost, která dovoluje útočníkovi kompromitovat systém **(viz http://secunia.com/advisories/29138/)**. Zranitelnost je způsobena chybou v generování HTML kódu pro zobrazení zpráv v komponentě Microsoft Internet Exploreru. To může být zneužito k zaslání speciálně upravené zprávy. Útočník tak může na systému spustit libovolný kód.
Info: **zpravy.actinet.cz**

JAVA PROBLÉMY

Společnost Sun oznámila chyby v Java WebStart, které mohou vést k přetečení paměti a následně ke spuštění kódu s vyššími právy. Zároveň s tím byly vydány i nové updaty Java Runtime Environment, opravující tyto chyby. Postiženými systémy jsou JDK a JRE 6 Update 4, JDK a JRE 5.0 Update 14, SDK a JRE 1.4.2_16, SDK a JRE 1.3.1_21 a verze předcházející. Více informací a updaty naleznete přímo na stránkách společnosti Sun.
Info: **zpravy.actinet.cz**

F5 BIG-IP

V F5 BIG-IP Web Management Console verze 9.4.3 byla objevena zranitelnost, která dovoluje potenciálním útočníkům vykonat na systému útok typu cross-site scripting. Více informací, včetně náznaku exploitu, naleznete v příspěvku na www.securityfocus.com/archive/1/489290. Firma F5 Networks se ke zranitelnosti ještě nevyjádřila.
Info: **zpravy.actinet.cz**

MICROSOFT WINDOWS

Lednovou aktualizací uzavřel Microsoft dvě kritické mezery. Obě lze využít prostřednictvím sítě, ale jen jedna z nich se týká Visty. Vždy jsou postižena XP, Windows 2000 a 2003. Online aktualizace Windows naštěstí odstraňuje tuto vadu automaticky.
Info: **www.microsoft.com**

KERIO MAILSERVER

V Kerio MailServeru byly objeveny zranitelnosti (viz www.kerio.com/kms_history.html), které útočníkovi umožňují způsobit na postiženém systému Denial of Service, případně tento systém kompromitovat. V první řadě se jedná o chybu v ošetření hranic v pluginu Visnetic antivirus, která může mít za následek přetečení vyrovnávací paměti. Dále se jedná o chybu vyskytující se při dekódování souborů aplikací uudecode, která může být zneužita k útoku a narušení paměti. Mezi dalšími zranitelnostmi se vyskytují například problémy s AVG plug-inem. Chyby jsou opraveny ve verzi 6.5.0.
Info: **zpravy.actinet.cz**

MICROSOFT WINDOWS

Byla nalezena zranitelnost v systému Microsoft Windows, která může být zneužita ke kompromitaci uživatelova sytému (viz www.microsoft.com/technet/security/Bulletin/MS08-008.mspx). Zranitelnost má na svědomí VBScriptový a JScriptový engine a objevuje se během práce s určitými skriptovými žádostmi při používání OLE (Objektové linkování a vkládání) automatizace. Toto dává útočníkovi možnost poškodit heap paměť. Úspěšný útok umožňuje spuštění libovolného kódu například při návštěvě zákeřné webové stránky. Uživatelé, jejichž účty mají nastaveny nižší oprávnění na systému, mohou být zasaženi méně než uživatelé s administrátorským přístupem.
Info: **zpravy.actinet.cz**

NOVINKY OD SYMANTECU

Updaty pro bezpečí dětí i pošty

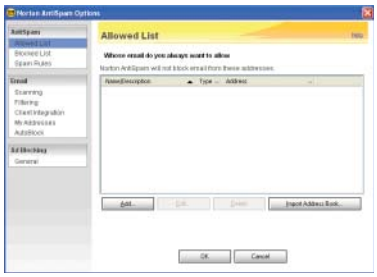
Společnost Symantec, výrobce bezpečnostního softwaru Norton, oznámila uvolnění updatů pro aplikace Norton AntiVirus 2008 a Norton Internet Security 2008. Další novinkou jsou nové verze nadstavbového softwaru Norton Add – On Pack. Update produktů Norton 2008 nabízí plnou podporu pro Microsoft Windows Vista Service Pack 1 a vylepšuje nástroj Identity Safe, umožňující bezpečné uchování hesel a přihlašovacích údajů pro webové formuláře.

Nadstavbový software Norton Add – On Pack přináší výrazná vylepšení v oblasti rodičovské kontroly a ochrany proti nevyžádané poště. Pravidla rodičovské kontroly lze nyní nastavit zvlášť pro jednotlivé uživatelské účty. Antispamový modul disponuje zvýšeným výkonem a rozšířeným nastavením.

„Aktualizace procházejí neustálým vývojem i v období mezi uvedením jednotlivých verzí produktů Norton," říká Vladimír Špička ze společnosti Symantec ČR & SR. „Pomocí Norton Update Centre nabízíme uživatelům možnost opět o něco vylepšit jejich software, a to jak na straně ochrany, tak na straně výkonu."

Update softwaru Norton AntiVirus a Norton Internet Security na verzi 2008.5 mohou na internetových stránkách **www.symantec.com** bezplatně provést všichni držitelé platných licencí. Nadstavbový software Add – On Pack je zdarma dostupný pro majitele platných licencí Norton Internet Security a Norton 360, a to pomocí odkazu v uživatelském rozhraní nebo prostřednictvím internetových stránek společnosti Symantec.

Komentář redakce:
Bezpečnostní balík Norton Internet Security považujeme za jeden z nejlepších (což potvrdily i naše nedávné testy), k jeho slabinám však dosud patřila nedostatečná ochrana dětí. Díky tomuto vylepšení (obsahujícímu funkci Norton Parental Control) ho lze konečně doporučit i rodičům, kterým záleží na tom, kde a jak tráví jejich děti svůj volný čas na internetu...



ADD – ON PACK: Další vylepšení je v oblasti ochrany proti nevyžádané poště.

DŮLEŽITÉ AKVIZICE

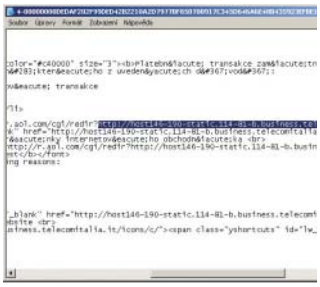
Trend Micro bude šifrovat

Společnost Trend Micro ohlásila akvizici britské firmy Identum, tvůrce technologie pro šifrování e-mailů a také prvního kryptografického systému čtvrté generace na světě. Společnost s novým názvem Trend Micro (Bristol), Ltd., bude integrovat svou šifrovací technologii do existujících řešení Trend Micro. Podle Evy Chenové, CEO a spoluzakladatelky společnosti Trend Micro, je cílem této akvizice zajistit ještě bezpečnější využívání internetu globálními zákazníky společnosti. „Náš tým odborníků na kryptografii se těší na spolupráci se společností Trend Micro, která je proslavená svými novátorskými bezpečnostními řešeními," řekl Andy Dancer, CTO firmy Identum.

Stávající produkty Identum budou dále nabízeny pod značkou Trend Micro.

PHISHING

Očkování českého internetového bankovnictví



FALEŠNÝ MAIL: Ačkoliv se mail na první pohled tváří důvěryhodně, nemá s Českou spořitelnou nic společného. Při zobrazení zdrojového kódu si nelze nevšimnout, že odkazy vedou kamsi na web telecomitalia.it...

Ne nepodobná klasickému očkování je v současné době situace v oblasti internetového bankovnictví. V několika posledních týdnech rapidně vzrostl počet phishingových mailů snažících se vylákat z důvěřivých uživatelů citlivé údaje. Momentálně jsou cílem především klienti České spořitelny, ale phishingové maily plní schránky všech uživatelů.

Ať už je však za maily skryt kdokoliv, jeho činnost je více prospěšná než nebezpečná. Pravděpodobně neexistuje nikdo, kdo by těmto zprávám (často s oslovením Drahoušek zákazník) uvěřil. Nemalá část zpráv je v angličtině, zbytek v neobvyklé směsici češtiny a ruštiny (Ceská Spořitelna Služba účastníkům). V podobném duchu jsou i zprávy „pozor na neprovedenou transakci" nebo „výhru desítek dolarů".

Pozitivní přínos vlny phisingu je především v tom, že si existenci tohoto problému uvědomili i lidé, pro které byl phishing jen jakýmsi bezpečnostním problémem týkajícím se „zahraničí". Tyto komické phishingové pokusy také lidem „polopatisticky" objasnily, že ne každému „oficiálnímu" mailu lze důvěřovat.

Tři kroky k bezpečnému bankovnictví

1) Banka po vás nikdy bezdůvodně nevyžaduje více bezpečnostních údajů, než je obvyklé. Pokud na takový požadavek narazíte a nechcete ho ignorovat, raději použijte telefon a požadavek si ověřte na help lince banky.

2) Než kliknete na jakýkoliv odkaz v mailu, ověřte si, kam vede. Ve webmailech obvykle stačí nad odkazem „podržet" kurzor, např. v Outlooku je lepší prohlédnout si zdrojový kód dopisu (po kliknutí pravým tlačítkem na příkaz Zobrazit zdrojový kód).

3) Po načtení stránky banky prověřte certifikát (kliknutím na symbol zámku v pravé části adresové lišty) a zkontrolujte informace o stránce (např. ve Firefoxu nabídka *Nástroje* | *Informace o stránce*).

ŽEBŘÍČEK HROZEB

Nástup adwaru

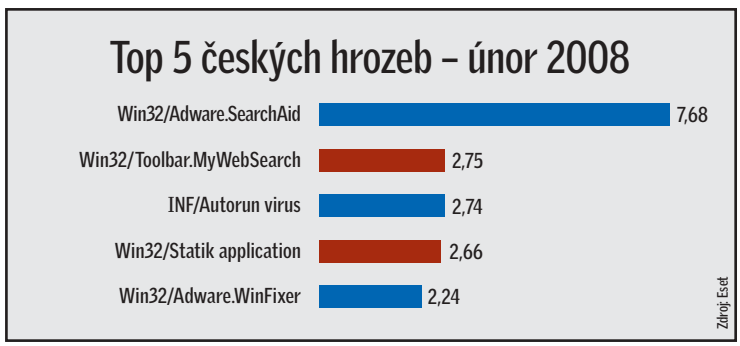
Globálně i lokálně se v únoru 2008 nejvíce šířil adware, tedy škodlivé kódy doručující na počítače uživatelů nevyžádanou reklamu. Statistický systém ESET ThreatSense.Net, který je součástí bezpečnostních řešení ESET a který sbírá statistické balíčky obsahující informace o typu a počtu infiltrací zachycených na počítačích 20 milionů dobrovolných uživatelů, vyhodnotil v únoru 2008 jako nejvíc rozšířenou hrozbu směs škodlivých kódů, které ESET detekuje jako INF/Autorun (9,43 %). Stejně jako v lednu 2008 obsadil i v únoru INF/Autorun první místo a dosáhl alarmující hranice téměř 10 % z celkového počtu všech zachycených hrozeb.

INF/Autorun je směs počítačových hrozeb využívajících soubor autorun.inf jako prostředek k napadení počítače. Tento soubor obsahuje informace umožňující automatický start programů poté, co je vyměnitelné médium (typicky USB disk, CD či DVD) vloženo do počítače.

V průběhu února získal INF/Autorun agilního konkurenta. Druhé místo obsadila hrozba označovaná jako WIN32/Adware.SearchAid, která ještě v lednu nebyla vůbec detekována a která za jediný měsíc dosáhla 8,05 % celosvětové rozšířenosti. Jedná se o varianty adwaru, které modifikují výsledky vyhledávání (reklamy) nebo podsouvají uživateli vlastní vyhledávače. Podobná aplikace s označením Win32/Toolbar.MyWebSearch (3,11 %) skončila na třetím místě.

Pětici globálně nejrozšířenějších hrozeb uzavírají agresivní infiltrace Win32/AdwareVirtumonde (2,09 %) a Win32/Adware.Virtumonde.FP (1,69 %), které způsobují otevírání pop-up oken s nevyžádanou reklamou a snaží se vyhnout detekci antivirových programů.

V České republice se v únoru nejvíce šířil adware s označením Win32/Adware.SearchAid (7,68 %), druhé místo pak obsadil již jmenovaný nováček Win32/Toolbar.MyWebSearch (2,75 %). Celosvětově nejrozšířenější INF/Autorun virus útočil na české počítače téměř třikrát častěji než v lednu tohoto roku a s 2,74 % postoupil z osmnáctého na třetí místo žebříčku.



ZPRÁVA SPOLEČNOSTI TREND MICRO

Předpověď hrozeb pro rok 2008

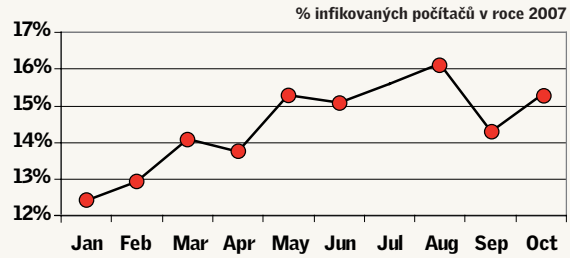
Ve svých publikacích 2006 Annual Roundup a 2007 Forecast (The Trend of Threats Today) společnost Trend Micro předpovídala, že převládající bezpečnostní hrozbou pro rok 2007 budou webové hrozby, které se projeví v plné síle. Webové hrozby současnosti zahrnují širokou škálu nebezpečí, obvykle se skládají z více než jednoho souboru, vyskytují se ve velkém počtu variant a zaměřují se na relativně menší skupiny lidí. Původní předpověď vycházela z chování některých útoků v roce 2006, u kterých se vyskytovala kombinace vysokého zaměření a nízkého rozptylu.

Společnost Trend Micro také předpovídala, že růst a rozšíření botnetů během roku 2007 budou v převážné míře založeny na nových metodách, důmyslném sociálním inženýrství a využití softwarových zranitelností. V přehledu rovněž uváděla, že bude pokračovat nárůst případů crimewaru a převládající motivací se v roce 2007 a letech následujících stane nezákonné obohacování. Pokud se zaměříme na hrozby, které byly v roce 2007 nejviditelnější, je zřejmé, že všechny z těchto předpovědí se opravdu splnily, přičemž mnohé z nich nabraly překvapující podobu.

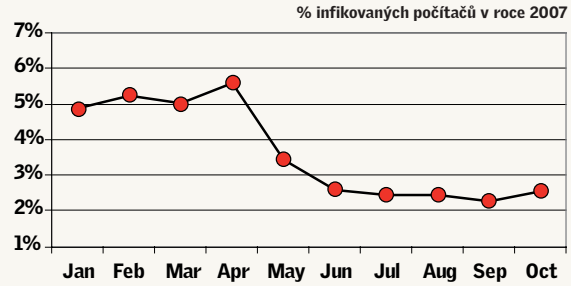
Měnící se svět hrozeb vyžaduje posun od tradičního konceptu škodlivého kódu. Digitální hrozby dnes zabírají další a další teritoria. Mohou se k uživateli dostat přes zranitelné pécéčko, návštěvou důvěryhodných webových stránek, které byly potichu a nenápadně zneužity, kliknutím na nevinně vypadající odkaz nebo tak, že uživatel je součástí sítě, na kterou se právě zaměřil útok DDS (Distributed Denial of Service).

V předkládaném přehledu Trend Micro shrnuje hrozby, malwarové trendy a nejsledovanější bezpečnostní události roku 2007. Skutečnými, reálnými oběťmi těchto bezpečnostních hrozeb se stali jednotlivci, skupiny, organizace a v některých případech i celé země. Tyto příklady společně ilustrují potřebu zlepšit metody boje s webovými hrozbami. Všechna data uvedená v této zprávě byla shromážděna organizací TrendLabs – globálními laboratořemi Trend Micro pro vyšetřování, výzkum a analýzu hrozeb a podporu jejich obětí.

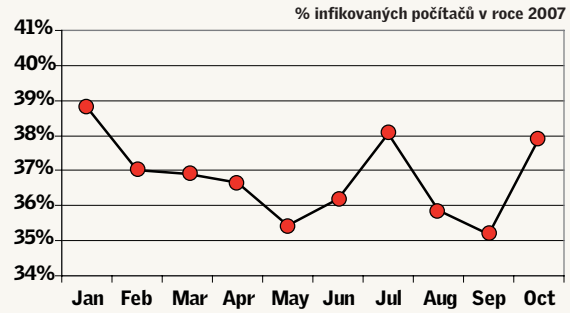
Nejrozšířenější malware roku 2007	
1	WORM_SPYBOT.IS
2	WORM_GAOBOT.DF
3	PE_LUDER.CH
4	TROJ_AGENT.ACSF
5	PE_PARITE.A
6	HTML_IFRAME.KQ
7	WORM_NETSKY.P
8	EXPL_ANICM00.GEN
9	EXPL_WMF.GEN
10	WORM_NYXEM.E



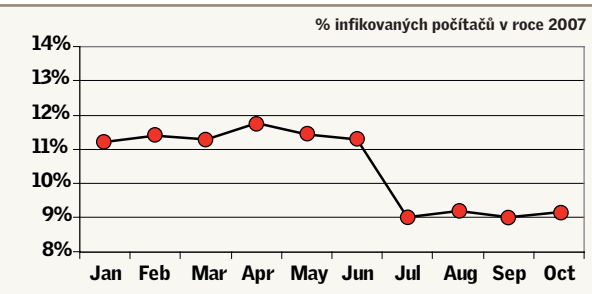
HACKING TOOLS: Hacking tools jsou programy navržené k prolomení ochrany počítače nebo sítě.



ADWARE: Adware zobrazuje reklamní obsah, často s nežádoucími efekty (vyskakovací okna, únosy browseru...).



KEYLOGGERS: Keyloggery monitorují stisk kláves, dokáží zaznamenávat vkládání údajů do on-line formulářů a tyto údaje z napadeného počítače odesílat svým tvůrcům.



BROWSER HELPERS: Browser Helpers jsou rozšíření browserů, která mohou monitorovat pobyt na internetu, nebo dokonce manipulovat s obsahem prohlížeče. Často se vyskytují ve formě nástrojových lišt.

AVAST! SLAVÍ

50 000 000 uživatelů

Společnost Alwil Software oznámila registraci 50 000 000. uživatele antiviru avast! Eduard Kučera, spoluzakladatel a CEO Alwil Software, komentuje dosažení této hranice takto: „Je to významná událost pro celý tým Alwil Software. Padesát milionů uživatelů Avastu dokazuje, že děláme svoji práci dobře."

Zajímavostí je, že první registrace proběhla v lednu 2002, 40 000 000. uživatel se registroval v říjnu 2007. Avast! antivirus je pro osobní počítače dostupný ve dvou verzích. Verze avast! Home Edition je nabízena zdarma pro domácí nekomerční použití, ke stažení je dostupná na serverech avast.com a download.com. Použita může být po bezplatné registraci na avast.com. Verze avast! Professional Edition může být použita v domácím i komerčním prostředí, tvoří i součást Professional Family Packu, který slouží pro ochranu až deseti uživatelů a jednoho Windows Home Serveru.

K oslavě 50 000 000. registrace bude na nákupy přes internetový obchod Alwil Software i přes resellery do 31. března 2008 poskytována 25% sleva. K získání této slevy je nutné použít během objednávky slevový kód 50 Million.