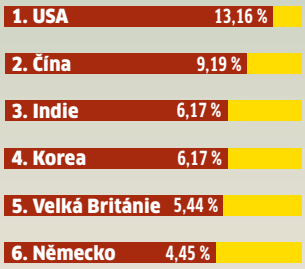
DATA A FAKTA

Barometr nebezpečí v květnu

Nebezpečí bohužel trvá. Ohrožení sítěmi botů vzdor novým ochranným technikám neklesá.

Největší šiřitelé virů



Zdroj: Kaspersky

Většina mailů s nebezpečnou přílohou nyní pochází z USA. Mezi prvními šesti je i Německo.

Nejpodlejší viry

Trojan.Peed.Gen	55,58 %
Win32.Netsky.P@mm	5,97 %
BehavesLike:Trojan.ShellHook	2,07 %
Win32.NetSky.D@mm	1,76 %
Win32.Netsky.AA@mm	1,54 %
Win32.Nyxem.E@mm	1,22 %
Win32.Netsky.B@mm	1,07 %
Win32.Netsky.C@mm	1,03 %
Trojan.Kobcka.CZ	0,83 %
Win32.Mydoom.M@mm	0,72 %
Ostatní	28,21 %

Zdroj: bitdefender

První místo na trhu s malwarem obsadil trojský kůň Peed, který je šířen stejnou sítí jako Storm Worm.

BEZPEČNOSTNÍ WEB CHIPU

www.chip.cz

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

Ošálené antiviry

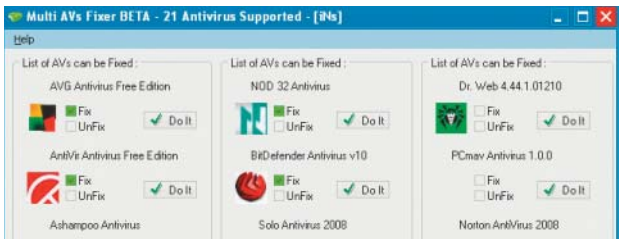
MALWARE se ve většině virových skenerů stejně jako dříve rozpoznává na základě signatur. „Antivirové“ nástroje to však znemožňují.

VALENTIN PLETZER

Je to nepřetržitý závod s časem. Cílem bezpečnostních firem je co nejrychleji rozpoznat nové škůdce a u známých malwarových verzí dát k dispozici jejich signatury. Tvůrci malwaru kontrují stále kratšími cykly vypouštění záškodnických programů. A nyní mají autoři virů v ruce novou, efektivní zbraň: nástroje, které už známé škůdce změní na povel tak, že je virové skenery hned nepoznají.

Chtěl-li mít autor malwaru v minulosti jistotu, že jeho „kreace“ nebude rozpoznána, musel ji umístit na webové stránky, jako např. na stránky Jotti nebo VirusTotal. Tam se pak řada skenerů pokoušela škůdce odhalit. Byl-li virus rozpoznán, zpravidla pak byl nasazen samorozbalovací komprimátor a ten jej nejen zmenšil, ale i změnil jeho signaturu.

Díky volbě „Vzorek nepředávat dál“ si autor viru mohl být jist, že se jeho nový záškodník neocitne v rukou výrobců antivirových programů, dokud nebude mít sám příležitost nasadit jej do oběhu. Od 3. ledna 2008 webová stránka VirusTotal na přání bezpečnostních firem tuto volbu už nenabízí. Vznikla tak sice „tržní mezera“, ale ihned ji zaplnily nové nástroje z produkce malwarové komunity. „Antiantivirové“ programy se jmény jako KIMS a AVFixer nejen otestují škůdce všemi běžnými antivirovými prostředky, ale na přání v něm hned také provedou změny, které pak znemožní jeho rozpoznání podle signatury.



Po kliknutí k nepoznání: V nástroji AV-Fixer potřebuje autor malwaru pouze určit skenery, které virus nemají umět rozpoznat.

Protiopatření: Heuristika, analýza chování a sandbox

Naštěstí pro potenciální oběti jsou sice stále používány skenery signatur, ale tvoří už jen součást celkové bezpečnostní koncepce. Už nějakou dobu dokážou skenery heuristickými metodami rozpoznat viry i vzdor malým změnám.

Relativně nové je nasazení systémů založených na analýze chování. Škodlivost programů zde není posuzována podle jejich vnější podoby, nýbrž podle jejich akcí. Zatím se však tato technologie ještě nezbavila dětských nemocí, jak ostatně dokládá i náš velký srovnávací test (► str. 62).

Sandboxy (pokusná „pískoviště“) dnes nasazují jen profesionálové. Ale také internetové bezpečnostní soupravy by se v budoucnu měly postarat o to, aby neznámý programový kód neběžel na vlastním počítači, nýbrž ve virtuálním prostředí – věrném obrazu toho skutečného. Pokud pak uživatel nebo antivirový software později zjistí, že se jedná o virus nebo podobnou neplechu, je možné všechny změny jednoduše vrátit zpět.

INFO: www.0-security.de

ZPRÁVA SPOLEČNOSTI ESET

Nárůst virových hrozeb z USB disků

Podle expertů se vrací stará éra šíření hrozeb, jen diskety byly nahrazeny přenosnými USB disky. V Česku v posledních týdnech prudce stoupl počet virových hrozeb šířících se prostřednictvím USB disků, na Slovensku využívá tohoto typu distribuce dokonce až třetina všech infiltrací. Za tímto prudkým nárůstem stojí podle společnosti ESET konec školního a akademického roku: Hlavně studenti přenášejí na USB velké množství souborů, ale jen málo studentů využívá účinnou antivirovou ochranu. Tomuto šíření také nahrávají nízké ceny USB disků. Od začátku roku 2008 zaznamenaly virové laboratoře antivirové společnosti ESET znatelný nárůst elektronických hrozeb, které využívají soubor Autorun.inf, spouštěný automaticky po vložení přenosných USB pamětí do počítače. V současnosti je v Česku přes 13 % počítačových hrozeb, nejčastěji trojských koní, doplněno o schopnost šířit se prostřednictvím přenosných médií. Na Slovensku je to již celá třetina ze všech zachycených hrozeb.

Šíření uvedeného malwaru umožňují především vlastnosti operačního systému. Systém Windows ve svém standardním nastavení automaticky otevře paměťový USB klíč ihned po jeho vložení do počítače. Vykoná přitom všechny instrukce načtené ze souboru Autorun.inf. Tím u nakaženého média aktivuje přítomnou počítačovou hrozbu. Uživatelská přívětivost funkce automatického otevírání vloženého média je tak vyvážená značným rizikem. Nenáročné přenášení infikovaného USB klíče z počítače do počítače ve výsledku znamená i velmi jednoduchou a účinnou metodu přenášení počítačových hrozeb. Podle vyjádření vedoucího virové laboratoře ESET Juraje Malcha můžeme mluvit o návratu staré éry, kdy se viry šířily na disketách. „USB disky jsou ale ještě jednodušší prostředník k jejich přenášení a zároveň poskytují dostatečně velký prostor pro uložení atraktivních obsahů, jako jsou hry, hudba či filmy,“ říká Juraj Malcho.

Mezi ty, kdo nejvíce využívají přenosné USB disky k úschově a přenosu rozmanitého obsahu, patří mladí lidé a studenti. V souvislosti s vysokým rozšířením tzv. „USB hrozeb“ není možné vyloučit, že tito lidé často pracují na počítačích bez antivirové ochrany, anebo že používají neaktualizované antivirové programy, získané často nelegálně.

INFO

Nová bezpečnostní rizika

ADOBE FLASH PLAYER

Nespecifikovaná zranitelnost v Adobe Flash Playeru dovoluje vzdálené spuštění libovolného kódu v kontextu postižené aplikace. Neúspěšný útok pravděpodobně vyústí v Denial of Service. Podle společnosti Symantec na nebezpečné Flash applety odkazuje v tuto chvíli minimálně 20 000 webových stránek. Podle vyjádření výrobce je zranitelnost momentálně vyhodnocována a na jejím odstranění spolupracují jak Adobe tak Symantec. Více informací najdete na adrese www.securityfocus.com/bid/29386. Podle posledních šetření jde o již jednou (nedostatečně) zazáplatovanou chybu, která je stále jistým způsobem zneužitelná. Adobe také oznámilo, že zranitelnost je vyřešena v poslední verzi Adobe Flash Playeru (9.0.124.0), přesto doporučujeme obezřetnost při prohlížení neznámých a podezřelých webů.
INFO: zprávy.actinet.cz

CORE FTP

V FTP klientu Core FTP byla nalezena zranitelnost umožňující anonymním útočníkům zapisovat do libovolné lokace na uživatelském systému Windows. FTP klient nedostatečně ošetřuje jména souborů obsahující Directory traversal sekvence (/.. a \..), které obdržel od FTP serveru jako odpověď na příkaz LIST. Jeden z příkladů možného zneužití je například zápis libovolného kódu mezi aplikace spouštěné při přihlášení se do systému. Podrobnější informace o zranitelnosti najdete například zde: http://vuln.sg/coreftp211565-en.html. Chyba je opravena ve verzi 2.1 Build 1568.
INFO: zprávy.actinet.cz

APPLE QUICKTIME

Ani po záplatě na verzi 7.4.5 se videokodek QuickTime nestal bezpečnějším. Hacker David Maynor v něm i po aktualizaci objevil četné mezery. Kdo si chce být opravdu jist, u důležitých systémů by se měl produktu QuickTime vyhnout.
INFO: www.apple.com

CROSS-SITE-SCRIPTING

Mezery v Googlu

Několik slabin v různých službách Googlu zdokumentoval během několika dnů hacker Billy Rios. Jedna z nich se týká konkurenta Excelu, tedy produktu Google Tabulky. Pomocí speciálního odkazu mohou útočníci surfařům, kteří používají Internet Explorer, ukrást jejich cookies. Důsledkem je plný přístup ke všem webovým službám, jako je třeba Google Mail.

Metoda známá jako Cross-Site-Scripting (krátce XSS) patří do speciálního oboru Billyho Riose. Už před ním uveřejnil jiný hacker informace o podobné mezeře v kódu Googlu a o mezeře v grafickém editoru Picasa.

Jako ochrana před útoky typu XSS většinou postačí vypnout javaskript s plug-iny, jako je např. NoScript. Pak ale mnohé webové služby přestanou fungovat.
INFO: www.google.com

BOTNET

Síť „Kraken“

Internet nyní ohrožuje nová, obrovská síť botů. Se svými zhruba 400 000 počítači je síť pokřtěná „Kraken“ (chobotnice) dvakrát větší než nechvalně známá síť šířící červa Storm Worm.

Trojský kůň, jímž je oběť infikována, se zpravidla maskuje jako obrazový soubor. Poněvadž síť pracuje decentralizovaně, řídicí počítač, který síť botů ovládá, není možné vypnout.

Až dosud rozesílala síť botů jen spam pro internetové lékárny. Výzkumníkům firmy Damballa se podařilo pozorovat, jak jednotlivé zotročené počítače rozesílaly až 500 000 spamových zpráv. Poněvadž škůdci disponují aktualizačním mechanismem, nejsou v budoucnu vyloučeny ani jiné aktivity, například útoky typu DDoS nebo nasazení phishingových serverů.
INFO: www.damballa.com

Trend Micro Worry-Free

Společnost Trend Micro Incorporated rozšířila svá bezpečnostní řešení Worry-Free o novou a vylepšenou řadu produktů, určených pro malé podniky a pro weby z oblasti e-komerce. Tito zákazníci dnes vyžadují propracovanější a výkonnější technologie: Jejich pomocí pak mohou bojovat proti vyspělým webovým hrozbám, jejichž možnosti daleko přesahují možnosti konvenčních virů a spamu. Řada Worry-Free Business Security 5.0, vytvořená pro malé podniky, a řada Worry-Free SecureSite, první řešení společnosti Trend Micro pro e-komerci, byly navrženy v souladu se závazkem společnosti Trend Micro vytvářet bezpečnější, inteligentnější a jednodušší řešení speciálně pro malé podniky. Vedle běžné ochrany před spywarem, viry, spamem, phishingem a nevhodným webovým obsahem disponují tato rozšířená řešení i funkcemi, které nejen eliminují měnící se webové a e-mailové hrozby, ale také se odlišují způsobem, jakým s nimi lidé pracují, ve srovnání s dobou před čtyřmi roky. Například ti mobilní zaměstnanci zákazníků, kteří používají Worry-Free Business Security 5.0, budou chráněni funkcí „location-awareness“ (fungování v závislosti na místě), která bezpečnostní nastavení Worry-Free v noteboocích automaticky změní podle toho, zda je zaměstnanec v sídle firmy, nebo venku. Data společnosti jsou chráněna dokonce i tehdy, když zaměstnanci používají venkovní bezdrátové připojení. E-mail je stále hlavní formou komunikace ve společnostech, takže spam, zahlcující sítě, je pro většinu z nich obtížný problém. Nová řada Worry-Free disponuje vícevrstvou ochranou proti spamu a blokuje ho ještě předtím, než se dostane do sítě. Nové řešení SecureSite z řady Worry-Free je určeno pro webové obchody, jejichž tržby a reputace jsou závislé na zabezpečení jejich webových stránek. Worry-Free SecureSite je hostovaná služba, která chrání on-line nakupující před hackery, kteří se snaží získat čísla jejich kreditních karet, hesla a další důležité digitální informace. Prostřednictvím celosvětové sítě odborníků společnosti Trend Micro jsou webové hrozby rychle identifikovány a odvráceny.

INFO: www.trendmicro.com

Pro zvídavé: Podrobnější infomace o novém řešení najdete i na www.worryfree.com

IT BEZPEČNOST
Cyberoam UTM Firewall

V oblasti bezpečnosti IT se na český trh dostává nové řešení bezpečnostní brány Cyberoam UTM Firewall. Toto řešení najde využití především v malých a středních firmách, a to díky komplexnosti ochran v rámci jednoho boxu a příznivé cenové politice. Cyberoam nabízí firewallové funkce s možností řízení provozu založeného na identitě uživatele, volitelnou integraci s Active Directory, podporu VPN, řízení šířky pásma, URL filtraci, antispam, antivirus a IPS. Produktová řada sedmi modelů UTM appliancí nabízí komplexní zabezpečení vstupu do vnitřní sítě organizace a chrání proti hrozbám zevnitř i vně sítě, jako jsou spam, spyware, phishing, pharming, viry, červi, trojské koně, DoS útoky a další. Nastavení pro jednotlivé uživatele snadno určí, jaké aplikace mohou uživatelé spouštět, jaký obsah mohou využívat, kdy se mohou připojovat vzdáleně, jakou šířku pásma mají přidělenu nebo jaký objem dat mohou stáhnout či uploadovat.

INFO
Nová bezpečnostní rizika

MICROSOFT WINDOWS CE

Byly nalezeny zranitelnosti v Microsoft Windows CE, které potenciálně mohou být zneužity ke kompromitování postiženého systému. Více informací na stránkách Microsoftu: **(http://support.microsoft.com/kb/948812)**. Zranitelnosti jsou zavíněny nespecifikovanými chybami při zpracování JPEG obrázků (GDI+) a v GIF zobrazovacích komponentách. Úspěšné zneužití může dovolovat spuštění libovolného kódu.

INFO: zprávy.actinet.cz

MICROSOFT WINDOWS

V dubnovém aktualizačním termínu uveřejnil Microsoft celkem 11 oprav bezpečnostních mezer. Pět z nich je hodnoceno jako kritických. Znamená to, že mohou být využity k „únosu“ počítače po internetu a k jeho zapojení do sítě botů. Řešením je bezpodmínečně aktivovat automatickou aktualizaci Windows. Teprve pak bude počítač v bezpečí.

INFO: www.microsoft.com

WORDPRESS UPLOAD FILE PLUGIN

Plugin Upload File pro redakční systém WordPress je náchylný k SQL injection zranitelnosti, protože nedokáže dostatečně ošetřit uživatelem poskytnutá data před použitím v SQL dotazech (viz. **www.securityfocus.com/bid/29352/info**). Zneužití tohoto problému dovoluje útočníkovi kompromitovat aplikaci, číst nebo měnit data, nebo zneužít dalších zranitelností v základové databázi.

INFO: zprávy.actinet.cz

DEBIAN BASED OS OPENSSL

V operačních systémech Debian GNU/Linux a systémech na nich postavených byla objevena chyba v generátoru náhodných čísel, která vede ke slabosti šifer OpenSSL. Chyba v generátoru spočívá v tom, že generovaná náhodná čísla jsou jednoduše predikovatelná a nejsou tedy náhodná. Chyba vznikla již v roce 2006 při tvorbě záplaty jiného problému pro openssl v operačním systému Debian GNU/Linux. Důrazně doporučujeme aktualizaci na opravenou verzi a výměnu vadných šifer (SSH, OpenVPN, DNSSEC klíčů, ...) ve všech systémech, kde došlo ke generování na systému Debian GNU/Linux nebo na systému z Debian GNU/Linuxu vycházejícího. Více informací, včetně utilitky pro kontrolu již vygenerovaných klíčů, naleznete v oznámeních k OpenSSL a OpenSSH na Security konferenci Debianu.

INFO: zprávy.actinet.cz

INSTANT SUPPORT HPISDATAMANAGER.DLL

Byly nalezeny potenciální zranitelnosti v ActiveX ovladačích v HP Instant Support HPISDataManager.dll běžícím na libovolné verzi Microsoft Windows (více informací na webu HP na adrese **http://h20000.www2.hp.com**). Zranitelnosti mohou být zneužity ke vzdálenému spuštění libovolného kódu. HP tyto zranitelnosti adresovalo v updatu na verzi 1.0.0.24.

INFO: zprávy.actinet.cz

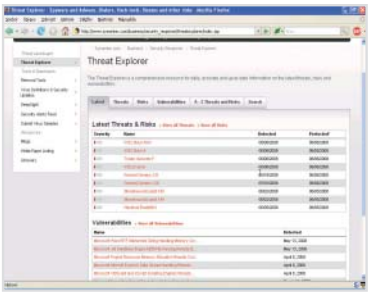
CHYBY V PRODUKTECH VMWARE

V produktech společnosti VMware bylo nalezeno několik chyb. Zranitelnosti mohou být zneužity lokálními uživateli k obcházení určitých bezpečnostních opatření nebo ke zvýšení svých oprávnění. Další informace a odkazy na stažení oprav naleznete na adrese **www.vmware.com/security/advisories/VMSA-2008-0009.html**.

INFO: zpravy.actinet.cz

SYMANTEC ONLINE FRAUD PROTECTION

Internetová ochrana značky



Bezpečněji: Informace o hrozbách z internetu najdete i na webu Symantecu.

Společnost Symantec Corp. oznámila dostupnost programu Symantec Online Fraud Protection. Tento komplexní systém zahrnuje služby, vzdělávání a různé možnosti trvalého sledování a správy. Symantec Online Fraud Protection je určen k ochraně podniků, které provádějí velké množství finančních transakcí, a jejich zákazníků před ztrátami vzniklými v důsledku on-line podvodů. Řešení by mělo pomoci podnikům chránit jejich zákazníky před širokou řadou on-line hrozeb, včetně phishingu a pharmingu.

Program podporuje také globální zpravodajská síť společnosti Symantec, která poskytuje komplexní přehled o útocích z internetu, vycházejících z bezpečnostních dat shromážděných z celého světa. Součástí globální zpravodajské sítě společnosti Symantec je 11 středisek reakce na bezpečnostní incidenty, která analyzují data z více než 2 milionů e-mailových účtů, ze 120 milionů systémů a z více než 40 000 zařízení ve více než 200 zemích. Program Symantec Online Fraud Protection zahrnuje tyto oblasti:

- **Sledování phishingu:** Vyhledávají se nové phishingové útoky a jiné útoky na obchodní značku klienta.
- **Sledování transakcí:** Vyhodnocují se transakce na serverových systémech a blokují se podvodné aktivity.
- **Odezva na on-line podvody a protiopatření:** Poskytuje se rychlá reakce na útoky, aby se minimalizovaly ztráty a ochránila se pověst značky, a je vedena spolupráce s poskytovateli internetových služeb, jejímž cílem je omezit činnost podvodníků.
- **Zjišťování informací o škodlivém kódu a analýza škodlivého kódu:** Sleduje se škodlivý kód zaměřený na konkrétní značku a analyzuje se chování nového škodlivého kódu.
- **Vzdělávání a ochrana spotřebitelů:** Organizacím je nabízena pomoc v oblasti vzdělávání a ochrany jejich koncových zákazníků před on-line hrozbami – minimalizuje se tak riziko podvodu.
- **Odborník v místě:** Nabídka zahrnuje také odborníka společnosti Symantec v místě. Tento specialista má přístup k různým zdrojům bezpečnostních dat a spolupracuje se zaměstnanci klienta. Předává jim odborné znalosti a slouží jako primární kontakt, organizující veškerou práci na ochraně před on-line podvody.

„Nejnovější zpráva Internet Security Threat Report společnosti Symantec ukazuje, že 80 % obchodních značek napadených phishingovými útoky bylo součástí finančního sektoru," řekl Ted Donat, produktový ředitel Symantec Consulting Services. „Podvody on-line jsou stále na vzestupu, a společnost Symantec proto nabízí zákazníkům ochranné nástroje. Program Symantec Online Fraud Protection je dostupný globálně ve všech regionech. Cena je dána počtem chráněných obchodních značek, počtem uživatelů on-line a požadovaným rozsahem podpory v místě. Další informace najdete na webových stránkách společnosti Symantec.

INFO: http://go.symantec.com/onlinefraudprotection