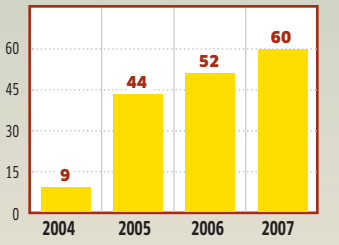
DATA A FAKTA

Barometr nebezpečí v červnu

Aby bezbranným uživatelům podstrčili svůj malware, rozesílatelé phishingových mailů s oblibou zneužívají velké události, jako jsou olympijské hry nebo EURO 2008.

Mezery v antivirech



Zdroj: http://invd.nist.gov

Počet bezpečnostních mezer v antivirových nástrojích roste. Toho by mohli hackeři využít ke svým útokům.

Rodiny virů

Název	Varianty
Win32/Zlob	84 910
HTML/IframeRed	33 428
Win32/Zonebac	31 685
Win32/Dialsnif	30 260
Win32/Vanti	20 369
Win32/Vxidl	16 607
Win32/SystemHijack	14 893
Win32/Virtualmonde	13 872
Win32/Renos	12 951
Win32/Bankrypt	12 934

Zdroj: Microsoft

Statistice momentálně vévodí Storm Worm (Zlob). Některé virové skenery rozpoznají jen zlomek variant.

BEZPEČNOSTNÍ WEB CHIPU

www.chip.cz

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

Hackeři se politicky aktivizují

Počet webových útoků, které nejsou motivovány finančně, stoupá. Internetoví aktivisté teď mají pro deptání politických protivníků nový prostředek: **„HACKTIVISMUS“**.

VALENTIN PLETZER

Vítejte ve frontových liniích informační války 21. století! – tak okomentoval Wall Street Journal internetový útok na servery rozhlasové stanice Radio FreeEurope. Celkem osm webových stránek tohoto vysílače nebylo po dobu několika hodin k dosažení. To, co nejprve vypadalo jako úplně obyčejný výpadek serveru, se později ukázalo jako cílený útok. 50 000 falešných „volání stránky“ za sekundu nedávno dokázalo srazit internetovou prezentaci do kolen.

Za možného objednatele tohoto kyberútoku je považován běloruský prezident Alexander Lukašenko. Prostřednictvím „hacktivismu“, tedy politicky motivovaného hackerství, se jeho režim podle všeho pokoušel zabránit vysílání opozičního pořadu, který měl připomenout rozpad Sovětského svazu – Lukašenko se často projevuje jako horoucí ctitel SSSR.

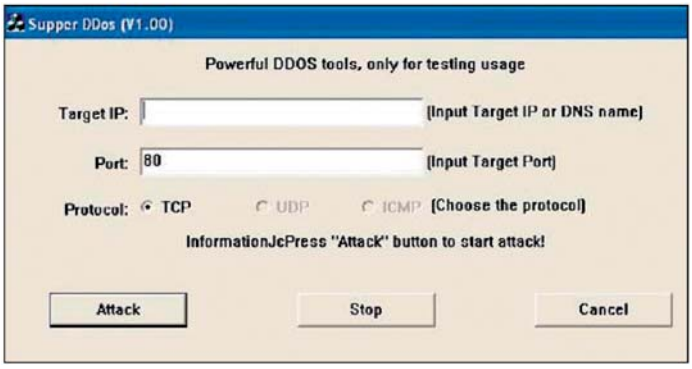
DDoS: Útoky, proti kterým prakticky neexistuje zbraň

Technika takových útoků je pokaždé skoro stejná. Například při tříhodinovém útoku na webovou stránku CNN činští hackeři nejprve rozeslali všem účastníkům protestu speciálně naprogramovaný nástroj. V předem stanoveném okamžiku pak účastníci jako v síti botů současně zahájili útok typu Distributed Denial of Service (DDoS). Nástroj při něm vysílal zcela legitimní požadavky na otevření webové stránky – jenomže úžasně rychle a v obrovském počtu. Servery CNN nedokázaly všechny požadavky zpracovat a zhroutily se.

Účinná ochrana před těmito útoky dodnes neexistuje. Americký vysílač situaci nakonec zvládl tak, že prostě silně limitoval počet požadavků z asijského prostoru. Tím však byl problém jen potlačen, nikoli vyřešen. A tak zatímco zbytek světa mohl webovou stránku vyvolávat jako obvykle, návštěvníci z Číny a Indie byli po dlouhé hodiny odblokováni.

Této formy útoku se ostatně nemusí vzdát ani ti „hacktivisté“, kteří nemohou motivovat dostatečný počet účastníků. Internetová mafie pronajímá své sítě botů za pouhých 100 dolarů denně – i pro politické akce. Obvykle však bývají útoky DDoS z botnetů využívány k vydírání. Oběti je nejprve předveden ukázkový běh akce, který dokáže sílu útoku, a pak následuje požadavek na zaplacení výkupného. Pokud na něj oběť nepřistoupí, jsou servery často umlčeny i na několik dní. Zejména pro internetové obchody je většinou finanční katastrofa, když zákazníci nemají přístup k jejich komerčním stránkám. Virtuální útoky na rozhlasové a televizní vysílače ovšem existovaly i před érou internetu. Například vysílání Svobodné Evropy rušili Sověti pomocí družic.

INFO: www.rferl.org



Jednoduché nástroje: S nástroji, jako je Super DDos, lze velké webové stránky při efektivní koordinaci citelně rušit i zcela ochromit.

STORM WORM

Síť botů infikována

Vědcům z univerzity v Mannheimu a z institutu Eurécom se podařilo infiltrovat jeden z celosvětově největších botnetů a dočasně jej ochromit. Bezpečnostní specialisté nejprve analyzovali komunikační protokol, aby pak do sítě podstrčili vlastní, sledovaný počítač. V síti Storm Wormu spolu jednotlivé počítače komunikují pomocí snadno modifikovatelné varianty protokolu Overnet, který je použit i u eDonkey. Jiné botnety jsou řízeny prostřednictvím webového nebo IRC serveru. Pokud je takový server odhalen a odstaven, žádný z příslušných botů už nenapáchá další škody. Technologie P2P sítě Storm Wormu však tento způsob boje znemožňuje. Vědci přesto našli cestu, jak činnost botnetu citelně narušit. Expertní tým prostě zaplavil síť falešnými příkazy, takže sledované počítače byly natolik zaneprázdněny, že se nestačily věnovat svému vlastnímu úkolu. Vědci doufají, že tak objevili cestu, která by v budoucnu mohla vést k likvidaci sítí botů.

INFO: www.uni-mannheim.de

Technologie: Síť botů využívá technologii P2P síte Storm Wormu.

INFO

Nová bezpečnostní rizika

OVLADAČ PRO REALTEK HD

Ovladač Realteku pro Vistu sužuje bezpečnostní mezera. Poněvadž se čipy Realtek vyskytují v mnoha onboard zvukových kartách, mezera se týká zvláště velkého počtu počítačů. Lze se tak obávat útoků, které obcházejí správu uživatelských účtů ve Vistě. Pod číslem verze 1.91 dodává výrobce aktualizaci, která problém odstraní.

INFO: www.realtek.com.tw

FOXIT READER

Prostřednictvím upravených PDF souborů může být do Foxit PDF Readeru propašován škodlivý kód. Postiženy jsou všechny verze včetně 2.3 Build 2822. Výrobce už ale na problém zareagoval a nabízí ke stažení aktualizovaný Build 2825.

INFO: www.foxitsoftware.com

WIRESHARK

V aplikaci Wireshark (výborný protokolový analyzér a paketový sniffer) verze 0.9.5 až 1.0.0 byly zjištěny zranitelnosti v GSM SMS, PANA, KISMET, RTMPT a RMI dissectors, které se mohou projevit při zpracování zákeřně pozměněných paketů. Útočník může způsobit pád aplikace nebo odhalit citlivé informace z paměti systému. Pokud nemůžete aktualizovat, můžete příslušné disektory vypnout. více naleznete na stránkách výrobce (**www.wireshark.org/security/wnpa-sec-2008-03.html**). Řešením je také aktualizace na verzi 1.0.1.

INFO: zpravy.actinet.cz

ZÁPLATY MICROSOFTU

Microsoft opět vydal pravidelné záplaty (**www.microsoft.com/technet/security/bulletin/ms08-jul.mspx**), mezi nimiž je i několik, kterým byste měli věnovat pozornost. Kromě opravy zranitelností v Microsoft SQL Serveru totiž balíček obsahuje i záplatu zranitelnosti Windows Exploreru dovolující vzdálené spuštění kódu a opravu dvou chyb ve Windows DNS (jak na straně serveru, tak klienta). Poslední důležitou záplatou je oprava zranitelnosti v Outlook Web Accessu pro Exchange Server dovolující navýšení oprávnění.

INFO: www.microsoft.com

CISCO

Produkty Cisco, které zpracovávají DNS zprávy, obsahují chybu v randomizaci DNS transakcí. Potenciální útočník tak může vyvolat útok typu Cache Poisoning. Bližší podrobnosti o zranitelnostech naleznete na webu výrobce.

INFO: www.cisco.com

XEROX CENTREWARE WEB

Internetová aplikace Xerox CentreWare Web 4.6 a starší obsahuje chybu v ověření uživatelských parametrů, která může vést k možnosti vykonat na aplikaci SQL injection. (Více informací najdete na webu výrobce na adrese **www.xerox.com/downloads/usa/en/c/cert_XRX08_008.pdf**). Řešením problému je aktualizace na verzi 4.4.46.

INFO: www.xerox.com

AUTOMATICKÝ HACKING

Nebezpečné aktualizace

V budoucnu by uveřejňování záplat mohlo vést k tomu, že během několika minut se na internetu začnou šířit nové útoky. Podle vlastních vyjádření se americkým výzkumníkům podařilo vyvinout systém, který analyzuje rozdíly mezi dvěma verzemi softwaru a na základě těchto informací samočinně vytvoří škodlivý kód. Vědci proto žádají výrobce softwaru, aby zvážili své aktualizační mechanismy.

INFO: www.cs.cmu.edu

NOVINKA OD FIRMY TREND MICRO

Bezpečné šifrování e-mailů

Společnost Trend Micro Incorporated ohlásila svůj vstup na trh s řešeními pro šifrování e-mailů a uvedla software Trend Micro Email Encryption Client 5.0 a e-mailové šifrování pro InterScan Messaging Hosted Security (IMHS). Toto řešení umožňuje malým, středním i velkým podnikům šifrovat e-mailovou komunikaci na jakoukoli platnou e-mailovou adresu bez předběžné registrace příjemce nebo toho, že by byla zapotřebí správa certifikátů.

Řešení pro šifrování e-mailů je postaveno na technologii firmy Identum, kterou společnost Trend Micro získala v lednu 2008. Řešení je integrováno s IMHS a poskytuje automatizované šifrování e-mailů filtrovaných hostovaným řešením pro zabezpečení e-mailů. Trend Micro také nabízí zásuvný softwarový modul Trend Micro Email Encryption Client 5.0, který podporuje rozšířené e-mailové klienty a umožňuje „výkonným uživatelům“, kteří vyžadují maximální bezpečnost, šifrování od jednoho desktopu ke druhému. Tato hostovaná a klientská šifrovací řešení se dají kombinovat tak, aby poskytovala kompletní šifrovací funkce včetně šifrování podle daných politik na perimetru.

Trend Micro Email Encryption Client 5.0 podporuje oblíbené e-mailové klienty, jako je Microsoft Outlook a Microsoft Outlook Express. E-mail může být zašifrován a odšifrován pomocí Trend Micro Email Encryption Client nebo mohou příjemci využít samostatně dodávanou prohlížečovou čtečku, prostřednictvím které si mohou lokálně šifrovaný mail prohlédnout.

INFO: www.trendmicro.com

Šifrování: Toto řešení umožňuje šifrovat e-mailovou komunikaci na jakoukoli platnou e-mailovou adresu.

ADWORDS

„Loginový“ phishing

Firmy, které využívají Google AdWords k šíření internetové reklamy, by nyní měly být zvláště opatrné. Pomocí zfalšovaných e-mailů a webových stránek se totiž hackeři pokoušejí získat hesla co největšího množství uživatelů služby AdWords. S odcizenými účty pak spustí další reklamu, která odkazuje na nebezpečné webové stránky. Cílem útočníků je dostat pod kontrolu co nejvíce počítačů.

INFO: www.google.com

INFO

Nová bezpečnostní rizika

ADOBE PHOTOSHOP

Zmanipulované BMP soubory mohou být v produktech Photoshop CS3, After Effects CS3 a Photoshop Album Starter Edition využity k propašování trojského koně do XP. Photoshop Album spouští škodlivý kód dokonce s náhledem. Do redakční uzávěrky ještě firma Adobe ve svých automatických aktualizacích žádné bezpečnostní záplaty nenabídla.

INFO: www.adobe.com

ADOBE READER/ACROBAT

V produktech Adobe Acrobat a Adobe Reader byla nalezena zranitelnost zaviněná implementací nespecifikované javascriptové metody. Zranitelnost může být zneužita k vyvolání pádu systému nebo ke spuštění libovolného kódu speciálně upraveným PDF souborem. Bližší popis zranitelnosti najdete na adrese **www.adobe.com/support/security/bulletins/apsb08-15.html**, záplaty na jednotlivé aplikace pak na webu firmy Adobe.

INFO: zpravy.actinet.cz

MOZILLA FIREFOX

Podle informací serveru Secunia (**http://secunia.com/advisories/30761/**) byly ve Firefoxu objeveny zranitelnosti, které umožňují kompromitaci zranitelného systému. Tyto zranitelnosti jsou zapříčiněny blíže nespecifikovanou chybou a v případě návštěvy „speciálně upravené stránky“ může útočník na počítači oběti spustit libovolný kód. Více informací o problému najdete na adrese **http://dvlabs.tippingpoint.com/blog/2008/06/18/vulnerability-in-mozilla-firefox-30**. Postiženy jsou verze 3.0 a 2.0.x. Řešení problému zatím není známo, a tak lze jen doporučit omezení návštěv nedůvěryhodných a rizikových stránek.

INFO: zpravy.actinet.cz

OPERA

Ve webovém prohlížeči Opera bylo nalezeno několik zranitelností. Některé mohou být zneužity k získání citlivých informací a jiné k vedení spoofing útoků. Zřejmě nejpodstatnější chyba se vyskytuje v chybném zpracování určitých znaků v adrese webu. Tato chyba může být zneužita k vydávání se za stránky jiného webu. Bližší informace o jednotlivých zranitelnostech naleznete na stránkách výrobce: **www.opera.com/docs/changelogs/windows/950/#security**. Chyby jsou opraveny v poslední verzi.

INFO: zpravy.actinet.cz

OPEN OFFICE

Nebezpečná chyba byla objevena v populárním kancelářském balíku Open Office. Zasaženy jsou všechny verze 2.0 až 2.4 pro veškeré platformy. Zranitelnost je způsobena funkcí rtl_allocateMemory(), která může dovolit vzdálenému uživateli spustit libovolný kód s právy aktuálního uživatele. Ke zneužití zranitelnosti je potřeba přesvědčit uživatele k otevření zákeřného souboru. Chyba byla opravena ve verzi 2.4.1. Více informací naleznete ve zprávě iDefense Labs (**http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=714**), případně přímo na webu Open Office.org (**www.openoffice.org/security/cves/CVE-2008-2152.html**).

INFO: zpravy.actinet.cz

STATISTIKA FIRMY ESET

Trojský kůň vykrádající údaje z on-line her

Česko ovládá nevyžádaná reklama, světovým hrozbám vévodí trojský kůň

Trojský kůň Win32/PSW.OnLineGames je stále nejčastěji odhalovanou hrozbou v celosvětovém měřítku. V rámci České republiky se mu zdaleka tak nedaří a lokálnímu žebříčku v červnu vévodily aplikace zobrazující nevyžádanou reklamu v čele s rodinou Virtumonde.

V květnu zaznamenal v žebříčcích nejrozšířenějších počítačových hrozeb razantní nástup trojský kůň Win32/PSW.OnLineGames. Tato hrozba se šíří hlavně prostřednictvím USB médií, k čemuž využívá automaticky spustitelný soubor autorun.inf. V květnu byl tento trojan rozpoznán téměř v 18 % ze všech zaznamenaných hrozeb. Na prvním místě se tento škůdce umístil i v měsíci červnu, když dosáhl 13,12 % ze všech detekcí škodlivých kódů. Vyplývá to z aktuálních výsledků statistického systému ESET ThreatSense.Net.

Druhé místo celosvětově v červnu obsadil Win32/Adware.Virtumonde (4,90 %). Tato infiltrace reprezentuje specifickou rodinu potenciálně nechtěných aplikací používaných k zobrazování nevyžádané reklamy v počítači uživatele. Adware z rodiny Virtumonde umí mimo jiné otevírat velké množství oken obsahujících nevyžádané reklamní materiály a je navržen tak, aby jej bylo velmi obtížné automaticky odstranit z počítače. Nevyžádaná reklama je stále velkým generátorem zisků pro tvůrce škodlivých kódů, což lze vysledovat i z dlouhodobé přítomnosti adwarových aplikací jako Virtumonde, Toolbar.MyWebSearch či Adware.SearchAid v první desítce nejrozšířenějších hrozeb.

INF/Autorun (4,60 %), tedy směs infiltrací, která vládla žebříčku hrozeb v průběhu letošní zimy, se v červnu umístila na třetím místě. Čtvrtou příčku stejně jako v květnu okupuje **Win32/Pacex.Gen**, který slouží jako nosič pro různé druhy infiltrací, využívající charakteristicky zašifrovaný obal.

Nejúspěšnější nováček WMA/TrojanDownloader.Wimad.N se s 2,34 % vyšvihl na červnové páté místo. Tato hrozba je šířena v podobě Windows Media souboru, který přesměruje mediapřehrávač na cizí webovou stránku, odkud následně stáhne škodlivé komponenty včetně adwaru. **WMA/TrojanDownloader.Wimad.N** je běžně prezentován na P2P výměnných sítích jako nejrůznější populární MP3 skladby a tím láká uživatele ke stažení.

Česká republika a nadvláda adwaru

Lokální statistika ESET ThreatSense.Net pro Českou republiku registruje v červnu na prvním místě dnes již klasickou počítačovou hrozbu **Win32/Adware.Virtumonde** (8,03 %). Její dlouhodobá popularita je způsobena těžkou odstranitelností jednotlivých variant z počítače a neustálou tvorbou nových a nových variant. I proto byl v měsíci červnu zaznamenán nárůst detekcí této hrozby o více než jedno procento.

Druhá nejrozšířenější lokální červnová hrozba je označována jako **Win32/Adware.SearchAid** (3,92 %). Hrozba **INF/Autorun** (2,70 %) se u nás, stejně jako celosvětově, i přes svůj setrvalý procentuální pokles umístila v červnu na třetím místě.

INFO: www.eset.cz

STUDIE FIRMY TREND MICRO

Datové úniky

Společnost Trend Micro Incorporated uvedla, že datové úniky se stávají nejpalčivějším problémem amerických, britských, německých a japonských společností. Ukazují to výsledky její studie, která zkoumala vnímání a zkušenosti podnikových uživatelů počítačů s bezpečnostními hrozbami.

Průzkum, v němž bylo dotazováno 1 600 firemních uživatelů ve Spojených státech, Spojeném království, Německu a Japonsku, zjistil, že ztráta firemních dat a informací je považována za druhou nejhorší hrozbu po virech a za mnohem závažnější hrozbu než spam, spyware a phishing. Mnoho dotazovaných zdvihlo při zmínce o únicích podnikových dat varovně prst: zatímco šest procent koncových uživatelů přiznalo, že má k dispozici uniklé podnikové informace, 16 procent věří, že za úniky dat mohou druzí zaměstnanci. Koncoví uživatelé ve Spojených státech, Spojeném království a Německu přiznávají, že způsobili únik dat, ať už záměrně, nebo náhodou, ochotněji než koncoví uživatelé v Japonsku.

Studie také zjistila, že zhruba 46 procent společností v současnosti nemá pravidla zamezující únikům dat. Společnosti v Německu a Japonsku častěji než firmy ve Spojeném království zavádějí pravidla pro ochranu před úniky dat. Ve všech sledovaných zemích aplikují preventivní pravidla častěji větší společnosti než malé firmy.

„Většina úniků dat se děje zvnitřku, ať už jde o náhodu, nebo o záměr. Viníky jsou právoplatní uživatelé, kteří mají přístup k datům v podnikové síti. Úniky dat mohou zapříčinit udělení pokut, vyšetřování, poškození dobrého jména značky a negativní reakce okolí.

INFO: www.trendmicro.com

INTERNETOVÝ TERORISMUS

Kybernetický útok na Litvu

Společnost Symantec se vyjádřila k víkendovému koordinovanému kybernetickému útoku hackerů na několik tisíc webových serverů, a to jak vládních institucí, tak i soukromých litevských společností.

Podle našich analýz, kterými disponujeme, se s největší pravděpodobností jedná o útok cíleně vedený z Ruska. To, že za útokem stojí ruští hackeři, potvrzuje i podvržený obsah plný komunistických a nacistických symbolů a nacionálních replik. Ostatně napjaté vztahy mezi Litevci a silnou ruskou menšinou žijící v Litvě tuto domněnku potvrzují.

Navenek deklarovanou příčinou zmíněných útoků je to, že litevským parlamentem prošel nový zákon (dosud nejpřísnější ze všech postsovětských republik), který zakazuje a přísně trestá publikování komunistických a nacistických symbolů, jako jsou obrazy představitelů těchto režimů, emblémy, vlajky, odznaky a označení, ale také srp a kladivo nebo třeba svastika. Z politického hlediska má útok proti několika tisícům litevských webových stránek podobný charakter jako zhruba rok starý útok na Estonsko. Ten byl však svým rozsahem i dopadem mnohem citelnější. Značné dopady loňského útoku na estonský život byly zapříčiněny i velkým pokrokem v oblasti egovernmentu, jehož Estonsko dosáhlo – a tím také podstatě větší závislostí na těchto službách.

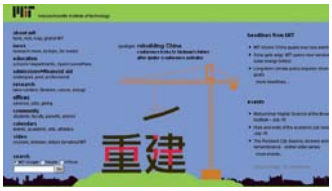
Kromě již zmiňovaného nacionálního rozměru lze však v Litevsku vysledovat i druhý „rozměr“ útoku. Máme za to, že hackeři paralelně s viditelným útokem, kdy zaměňují obsahy stránek a umísťují na ně komunistické a jiné symboly, skrytě podnikají i útoky neviditelné. Pronikají na nedostatečně chráněné webové servery a umisťují tam škodlivé skripty, jejichž pomocí lze infikovat počítače, které tyto stránky navštěvují, a následně z nich vykrádat citlivé a osobní údaje. Situace je o to horší, že tyto infekce následně nakazí i lokálně uložené, privátní webové stránky uživatelů. Ty se pak po jejich nahrání na soukromé webové servery v internetu stávají dalším šiřitelem útoků proti novým návštěvníkům. Politicky motivovaná a pozornost vzbuzující část útoku se tak propojuje s ekonomicky motivovanou a ukrývanou částí útoku.

Celá situace ukazuje, že zranitelnost webových serverů je i v internetově vyspělých zemích, ke kterým se pobaltské země nesporně dají počítat, velkým problémem. Pouze za posledních šest měsíců roku 2007 jsme zjistili 11 253 zranitelností webových serverů, které umožňovaly provést webové útoky tohoto typu. To ukazuje na vysoký nárůst atraktivnosti a zranitelnosti webových serverů, o které se jejich správci nedokáží dostatečně starat. Pro srovnání: všech ostatních, tradičních zranitelností bylo za stejné období 2 134. K tomu si připočtěte, že 73 % z uvedených zranitelností je klasifikováno jako snadno zneužitelné a průměrná expozice, to je doba mezi jejich zveřejněním a následným uvolněním opravných záplat od výrobců příslušného softwaru, činila plných 46 dnů,“ sdělil k tomuto tématu country manažer Radek Smolík.

Komentář redakce:
Pro většinu z nás je podobná situace jen „zajímavou událostí na divokém východě“ a zpráva brzy zanikne v záplavě „důležitých“ informací o poprsí našich celebrit či o skandálech našich politiků. Přemýšlivější čtenáři, kteří si vzpomenou na snahy vlády o stále větší elektronickou agendu a na nepříliš vřelé „radarové“ soužití s Ruskem, si však musí položit otázku: Jak by dopadl podobný útok na Českou republiku?

Na konci loňského roku se internetovou kriminalitou zabývalo jen pár policistů, od ledna jich mělo být v každém kraji několik. Jen málokdo bude tak naivní, aby si myslel, že se pár amatérů z řad policie (doposud řešící pod taktovkou BSA převážně softwarové delikty) může postavit profesionálům z druhé strany barikády.

Nově zřízená organizace CSIRT (Computer Security Incident Response Team), o které jsme vás již několikrát informovali, je prozatím spíše amatérským pokusem (s nulovými pravomocemi). Nezbývá nám tedy než doufat, že si příště ruští hackeři opět vyberou někoho jiného…



ZÁPLATY JÁDRA

Větší komfort

Uživatelé Linuxu nebudou v budoucnu muset po aktualizaci restartovat počítač. Nový software Ksplice zavede bezpečnostně relevantní záplaty do systému přímo za provozu – za předpokladu, že se přitom nemění datové struktury nebo sémantika kódu. První extrapolace ukazují, že Ksplice může pomoci v 84 % případů. Uživatelé Windows mohou jen přihlížet – obdobného oznámení se od Microsoftu dosud nedočkali.
INFO: http://web.mit.edu

ROGUE ANTI-SPYWARE

Falešné nástroje

Bezpečnostní experti varují před novou vlnou falešných kodeků a rogue anti-spywaru. Názvy jako AntiVir Gear, VirusProtect, SpyDown, SpywareQuake a VirusHeat mají důvěřivým obětem vsugerovat, že se jedná o opravdové antivirové nástroje. Ve skutečnosti se však za nimi skrývá trojský kůň Zlob, který špehuje uživatele a instaluje další adware i spyware. Většinou anglickojazyčný software imituje nejen vzhled legitimních virových skenerů, ale propaguje jej také pomocí zvláště pro tento účel vytvořených stránek. Návštěvník tam uvidí flashovou animaci, která simuluje virový skener. Na konci se pak objeví většinou zfalšovaná varovná zpráva Windows, která má uživatele přesvědčit, aby si falešný bezpečnostní software nainstaloval. Regulérní antivirové nástroje škůdce rozpoznají.
INFO: www.0-security.de

TROJSKÉ KONĚ

Olympijské hackování

Olympijské hry v Pekingu jsou velkou událostí nejen pro sportovce a diváky. Od začátku roku se hromadí útoky z asijského prostoru, které zneužívají právě tohoto tématu. Prostřednictvím e-mailů s předmětem jako „Štafetový běh s olympijskou pochodní“ se snaží propašovat do počítačů adresátů trojské koně. Zvláštní je na těchto záškodnících formát souboru: Microsoft Office Database (MDB).

Otevře-li příjemce přílohu, rozbalí se EXE soubor, nainstaluje se a ihned se spustí. Tyto maily také nejsou jako jiný spam rozesílány do tisíců počítačů, nýbrž záměrně jen na e-mailové účty vedoucích pracovníků podniků.
INFO: www.messagelabs.com

PODOBA BUDOUCNOSTI

Počítačový svět podle Intelu

V kalifornském Muzeu počítačové historie odhalila firma Intel více než 70 projektů, na kterých ve svých laboratořích právě pracuje. Projekty spadají do různých odvětví: od ochrany životního prostředí přes zdravotnictví až po bezdrátové mobilní technologie.

Automobily mohou vidět

Procesory, které bude Intel v budoucnu vyrábět, povedou k masivnímu rozšíření paralelního computingu. Tento způsob souběžného zpracování dat umožňuje zpracovávat mnoho úloh najednou. Takové paralelní výpočty rozšiřují možnosti vizuálního computingu. „Dočkáme se tak dokonale realistického ztvárnění objektů v 3D prostředí či okamžitých analýz videozáznamů. Komunikace mezi lidmi a jejich přístroji bude přirozenější a snazší," řekl tiskový mluvčí společnosti Pavel Svoboda.

Společnost Intel, společně s firmou Neusoft, předvedla speciální aplikaci, která dává automobilům zrak. Systém využívá kamery stejným způsobem, jakým člověk používá oči, a vícejádrové procesory přebírají roli mozku. Automobily budoucnosti tak získávají schopnost mnohem přesněji identifikovat ostatní, kriticky se přibližující vozidla nebo chodce. Mohou tak vyslat řidiči odpovídající varování nebo automaticky provést kroky nutné k zamezení nehody.

Snižováním spotřeby ke zlepšení životního prostředí

Vědci chtějí pokračovat nejen ve zvyšování výkonu procesorů, ale také ve výrazném snižování jejich spotřeby a energetické náročnosti. Specialisté z oddělení výzkumu a vývoje společnosti Intel zkoumají novou techniku správy napájení (power management). Technologie blízké budoucnosti se nazývá „Platform Power Management" (platforma správy napájení). Průběžně monitoruje změny v činnosti počítače a inteligentně snižuje (nebo zcela vypíná) dodávku energie do těch částí systému, které zrovna nejsou využívány, například USB portů. První zkoušky této technologie ve stavu, kdy je počítač v nečinnosti či je mírně vytížen, vykázaly energetické úspory převyšující 30 procent. „V průběhu několika příštích let předpokládají vědci společnosti Intel dosažení až 50procentní úspory – nehledě na to, zda je počítač nečinný, či plně vytížený," dodal Pavel Svoboda. Nová platforma správy napájení by jednou mohla přinést výhody celé škále produktů Intel, od mobilních internetových zařízení (MID) až po servery s velkým výkonem.

INFO: www.intel.com/cz

Chytrý vůz: Technologie Smart Car používá počítačové zpracování obrazu k rozpoznání a sledování objektů na silnici a přispívá tak k lepší bezpečnosti řidiče.

PHOTO OPTIMIZER 2

Jednoduchá editace fotografií

Program Photo Optimizer 2 od Ashampoo je zaměřen na ty amatérské fotografy, kteří chtějí obrazy optimalizovat jedním kliknutím. V tomto softwaru ani není možné dělat o mnoho více: vybavení programu je více než skromné, například Photoshop Express od Adobe nabízí více funkcí.
S nástrojem od Ashampoo je možné obrázky pouze otáčet nebo pomocí posuvníků měnit jas, kontrast nebo gama-hodnoty. Nástroj stojí kolem 300 Kč.

INFO: www.ashampoo.com

ORIGINÁLNÍ PREZENTACE

Vybuchne Bomba.cz?

Počátkem července byl oficiálně představen nový komunitní videoportál Bomba.cz. Novinka, která doplňuje portfolio vydavatelství Internet Info o ryze zábavní server, nabídne svým uživatelům výběr toho nejlepšího, co kdy vzniklo v oblasti krátkého videa na internetu. Služba je založena na principu sdružování videí z nejznámějších videoserverů celého světa. Videa jsou externě přehrávána (neboli streamována) v okně přehrávače. To umožňuje jednoduchou obsluhu i lokalizaci obsahu speciálně pro české prostředí.

Bomba.cz je postavena na silném komunitním principu. Uživatelé mohou prostřednictvím serveru sdílet a hodnotit oblíbená videa, navazovat navzájem kontakty, posílat si vzkazy interní poštou a samozřejmě také diskutovat nebo chatovat. Specifickou službou je tzv. epicentrum neboli automatizované sledování aktivit okruhu přátel. Systém uživatele informuje, jaká videa se komu líbí, či nelíbí, kdo přispívá do diskusí, jaká videa přidali do databáze ostatní a jaké jsou jejich další aktivity na serveru. Kromě zábavních videí bude pro uživatele silným lákadlem také propracovaná databáze hudebních videoklipů, doplněných texty písní a přehledy interpretů. Chybět nebude ani hudební hitparáda s jednoduchým systémem hlasování.

Komentář redakce: *Většina komentářů k tomuto projektu na internetových diskusích balancuje od nadšených hodnocení až po nařčení z parazitizmu a vykrádačství. Nás překvapilo, že má někdo odvahu spustit takovýto projekt, aniž by nabídl cokoliv zajímavého nebo něco, čím by se server odlišoval od svých konkurentů. Instantní postup ve stylu „vytvořte jednoduché stránky, ‚nalinkujte' do nich videa z YouTube a spol. a modlete se, aby se našlo aspoň pár zvědavců" vyžaduje opravdu „hroší povahu". Dokonce i stahování videí je řešeno „externím řešením" (přes server vixy.net) a otázkou je, nakolik jejich oblíbená hláška „Error: Sorry, server is too busy.." potěší uživatele.*

ACER G24

Širokoúhlý displej pro hráče

Acer nabízí nové širokoúhlé LCD monitory G24, které jsou určeny pro hráče a uživatele, kteří požadují obraz ve vysokém rozlišení a zobrazení plynulého pohybu při hraní akčních her s vysokými grafickými nároky. LCD displej G24 doplňuje nový stolní osobní počítač Aspire Predator, navržený pro hraní těch nejnáročnějších her. Širokoúhlý 24" panel CrystalBrite s rámečkem měděné barvy podporuje rozlišení 1 920 × 1 200 a má kontrastní poměr 50 000:1, jas 400 cd/m^2 a krátkou dobu odezvy – 2 ms. Je vybaven digitálním portem HDMI s podporou HDCP. Široký úhel pohledu 176° umožňuje sledovat obraz na displeji i několika uživatelům najednou.

INFO: www.acer.cz

OKI C3600

Kompaktní barva

Firma OKI Printing Solutions představila novou barevnou tiskárnu C3600 pro malé a střední kanceláře, které ke své práci potřebují kompaktní postscriptový model. Rychlost tisku je až 20 stránek za minutu, první stránka se v případě černobílého dokumentu vytiskne již za 10 sekund, v případě barevného dokumentu za 12 sekund. Model C3600 se dodává s oddělenými vysokokapacitními zásobníky toneru a válci. Doporučená koncová cena tohoto nového postscriptového modelu činí 7 200 Kč bez DPH.

INFO: www.oki.cz

KOMUNITNÍ OCHUTNÁVKA

Telefónica O2 spouští Ochutney.cz

Nově spuštěný portál Ochutney.cz slučuje nejlepší funkce komunitních webů do jediného celku. Ochutney.cz zdaleka nebude jen místem, kam lidé budou moci chodit pasivně za zábavou. Portál by měl být místem, kde si uživatelé budou moci sami vytvořit svůj vlastní prostor podle svých zájmů, života a koníčků a interaktivně ho upravovat a sdílet s přáteli. Na Ochutney.cz je možné sdílet s přáteli například fotografie z dovolené, videa z festivalu nebo nejnovější demo své kapely. Největší výhodou pak je, že bude jen na uživateli, jestli například fotografie z dovolené nebo večírku s přáteli nahraje rovnou na akci ze svého telefonu, anebo v klidu po návratu z Kanárských ostrovů doma u počítače. Díky svému vlastnímu prostoru na Ochutney.cz tak bude možné sdílet svůj život prakticky minutu po minutě s ostatními, a to bez ohledu na to, jestli uživatel sedí zrovna v obývacím pokoji, nebo na druhém konci světa. Možnost nahrávání přímo z mobilních telefonů bude spuštěna již v druhé polovině roku 2008.

Komentář redakce: *Komunitní servery rostou jako houby po dešti, manažeři zodpovědní za jejich růst si malují do grafů stoupající křivky návštěvnosti a uživatelé si nechápavě klepou na hlavu. Ani po důkladném prozkoumání jsme nepřišli na jediný důvod, proč dávat svá videa právě sem. A poté, co se při pokusu o zhlédnutí videa navíc objevil text „Požadovaná stránka nebyla nalezena“, nás nenapadá ani důvod, proč si zde videa prohlížet. A to už je co říci…*

PS: Než se rozhodnete na komunitní server umístit své „výtvory“, nejprve „ochutnejte“ podmínky použití. Abyste nebyli po „ochutnávce“ překvapeni.

TOSHIBA SECURED

Bezpečný a odolný externí pevný disk

Společnost Toshiba Computer Systems Division rozšířila svou rodinu externích 2,5“ disků a představila nový, bytelně stavěný externí harddisk s připojením přes rozhraní USB 2.0. Disk SecuRed nabízí kapacitu 200 GB a je chráněn čidlem volného pádu (v případě pádu oddálí čtecí hlavy od ploten) a krytem, který je odolný proti polití. Je vybaven čtečkou otisků prstů, zabezpečením pomocí hesla a šifrováním uložených dat. Zabezpečení pomocí hesla je založeno na silném šifrovacím algoritmu AES-256 a na vestavěném softwaru, jenž zajišťuje šifrování celého harddisku. SecuRed má rozměry 130 × 85 × 19 mm a v ČR se bude prodávat za doporučenou koncovou cenu (včetně DPH) 4 510 Kč.

INFO: www.toshiba.cz