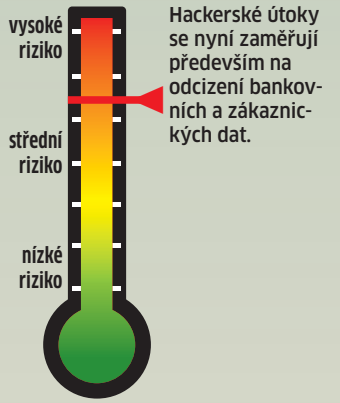
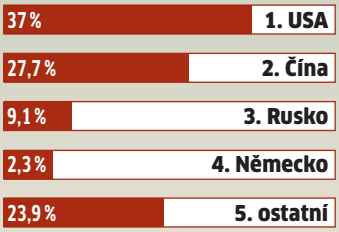
DATA A FAKTA

Barometr nebezpečí



Hackerské útoky se nyní zaměřují především na odcizení bankovních a zákaznických dat.

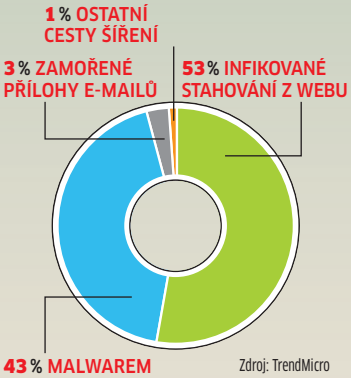
Infikované stránky



Zdroj: Sophos

Většina škodlivých programů se vyskytuje na amerických stránkách – stránky domény .cz jsou ještě relativně bezpečné

Největší zdroje virů



Zdroj: TrendMicro

Nebezpečí z webu: Více než polovina všech virů se skrývá ve stahovaných souborech.

Číslo měsíce

82,1 %

všech e-mailů jsou spamové zprávy. Ukázala to výroční zpráva Symantecu za rok 2008.

Hackeři čtou vaše data

Pomocí jednoduchého trojského koně vnikají do sítí, **SLÍDÍ V ELEKTRONICKÉ POŠTĚ** a v údajích o bankovních účtech. Obrana proti těmto útočníkům je obtížná.

FABIAN VON KEUDELL

Dbali jste všech bezpečnostních zásad: aktualizovali virový skener, aktivovali firewall a nainstalovali všechny aktualizace Windows. Přesto mohou hackeři váš kompletní provoz na síti odposlouchávat – díky nové metodě, proti níž se lze jen těžko bránit. Neboť trojský kůň Trojan.Flush.M zmanipuluje síťovou komunikaci. Myšlenka útoku je přitom velmi jednoduchá a funguje děsivě dokonale. Záškodník na napadených PC prostě spustí vlastní DHCP server. Za tím účelem nainstaluje síťový ovladač (NDISPro) a následně odpovídá na všechny DHCP požadavky počítačů. Fatální přitom je, že i když na počítačích běží antivirový program, pécéčka důvěřují falešnému DHCP serveru, neboť odtud za normálních okolností nemohou viry přicházet – jenomže zfalšované datové pakety ano.

Jakmile si jednou útočníci takto počítače podmaní, mohou celý síťový provoz přesměrovat. A tak se třeba při internetovém bankovnictví můžete náhle namísto pravé stránky své banky ocitnout na k nerozeznání podobné stránce hackerů, která lační po informacích o vašich účtech.

Internetové kavárny: Snadná kořist pro Trojan.Flush.M – během nejkratší doby se pécéčka nakazí působením DHCP serveru simulovaného škůdcem.

Detailně postupují útočníci takto: Napadenému PC přiřadí nové DNS servery a tak přesměrují každé volání webové stránky, dejme tomu **www.banka.cz**, přes hackerský server. Tam si mohou číst hesla, jimiž se uživatel přihlašuje k webovým stránkám, nebo i maily, které odesílá prostřednictvím protokolu POP3. Chip už má k dispozici zprávu jedné velké zahraniční firmy, jejíž celou síť škůdce přesměroval. Dokonce ani dobře zabezpečené sítě tedy hackerům neodolají.

Nové metody útoků: Výrobci antivirů musí jednat

Důvod, proč tento trojský kůň může způsobit tolik škod, aniž by byl odhalen, je prostý: Tato metoda napadení je úplně nová. Až dosud výrobci antivirových programů vlastním DHCP serverům v síti plně důvěřovali. V případě škůdce Trojan.Flush.M stačí infikovat jediný počítač, který pak funguje jako domněle důvěryhodný server a všechny ostatní počítače přesměruje.

Dokonce i když uživatel nakažený počítač vypne, mnoho jiných PC pak až do příštího restartu používá DHCP data trojského koně. Chcete-li svou síť zabezpečit, nainstalujte si nejnovější aktualizace signatur pro antivirový program a proskenujte jím všechny počítače. Potom počítače v síti restartujte. V internetových kavárnách byste vždy měli zkontrolovat síťovou konfiguraci svého počítače. Pokud IP adresy DNS serverů znějí »85.255.112.36« nebo »85.255.112.41«, je síť infikována trojským koněm Trojan.Flush.M!

INFO: www.symantec.com

GOOGLE MAIL

Přístup pro každého

Bezpečnostní mezera v mailové službě Googlu poskytuje hackerům možnost zřizovat v cizích poštovních schránkách vlastní přesměrovací filtry. Jimi pak mohou jménem oběti rozesílat zprávy na mailové adresy. Útočníci k tomu využívají slabinu označovanou jako CSRF (Cross-Site-Request-Forgery): Uživatel musí být přihlášen ke své poštovní schránce a současně v jiném okně browseru vyvolat hackerskou stránku. Pak může záškodnický skript nakonfigurovat googlovské mailové filtry. Pomoc zjedná plug-in do browseru nazvaný NoScript. Kromě toho by uživatelé měli k vašemu účtu přistupovat jen prostřednictvím zabezpečeného spojení HTTPS. K tomu ovšem nejprve musíte Google přemluvit: Přihlašte se ke svému mailovému účtu a klikněte na »Nastavení | Obecné«. Pod »Připojení browseru« zvolte »Vždy používat https«.

INFO: www.googlemail.com

Gmail: Bezpečně jen přes HTTPS.

INFO

Nová bezpečnostní rizika

VMWARE

Útočníci mohou na virtualizovaný hardware vyslat speciální požadavek a pak bez oprávnění správce přenášet data a spouštět programy. Problém odstraní aktuální verze VMware Workstation 5.5.9 a VMware Player 1.0.9.
INFO: www.vmware.com

JAVA

K propašování škodlivého kódu do PC prostřednictvím Javy využívají hackeři více bezpečnostních mezer. Nová verze Java 6 Update 11 je nejen chráněná, ale hned také z počítače vymaže starší nezabezpečené instance programu.
INFO: http://java.sun.com

TRILLIAN MESSENGER

Hned třemi kritickými mezerami v multimessengeru Trilian mohou útočníci pomocí přetečení bufferu nahrát do počítače škodlivý kód. Hackeři k tomu využívají soubory s příliš dlouhými názvy. Řešení je snadné: z webové stránky výrobce si nainstalujte novou verzi 3.1.12.0.
INFO: www.ceruleanstudios.com

SUN SOLARIS

Podle informačního serveru Secunia potvrdila společnost Sun výskyt zranitelnosti v Sun Solaris, jejíž zneužití umožní potencionálním útočníkům provádět utoky typu spoofing. Více podrobností najdete na stránce výrobce **(http://sunsolve.sun.com/search/document.do?assetkey=1-66-250826-1)**, kde jsou i informace o možném řešení problému.
INFO: zpravy.actinet.cz

CISCO SECURITY MANAGER

Cisco Security Manager obsahuje zranitelnost v případě, že je užíván s Cisco IPS Event Viewer (IEV). To má za následek otevření TCP portů na klientovi i serveru. Zneužití této chyby může vést k zpřístupnění IEV MySQL databáze nebo IEV serveru, prostřednictvím otevřených portů na serveru. Tato chyba byla nalezena u verze 3.1, 3.1.1, 3.2, a 3.2.1. Řešením je update na opravenou verzi. Pro více informací navštivte stránky výrobce (**www.cisco.com**).
INFO: zpravy.actinet.cz

SAMSUNG FRAME MANAGER

Viry na nočním stolku

Kdo má doma digitální fotorámeček od Samsungu, má pravděpodobně také zavirovaný počítač. Neboť dodané cédéčko s ovladači obsahuje virus W32.Sality.AE. Postiženy jsou modely SPF-75H, SPF-85H, SPF-86H, SPF-85P, SPF-86P a SPF-105P. Škůdce se společně s originálním ovladačem nainstaluje na pevný disk – a bohužel jej dokážou odhalit zdaleka ne všechny antivirové programy. Jakmile se jednou ocitne v počítači, virus samostatně stáhne nový škodlivý kód z internetu a infikuje spustitelné soubory na disku. Fatální přitom je, že infekce zasáhne tolik souborů, že se škůdce dá jen velmi obtížně odstranit ručně. Pomoci mohou jen dobré antivirové nástroje, například Norton Antivirus firmy Symantec nebo McAfee Antivirus. Samsung už zareagoval a prodej postižených modelů zastavil. Kdo už fotorámeček vlastní, měl by si nainstalovat opravenou verzi ovladače 1.082 Frame Manageru.
INFO: www.samsung.com

ADOBE ACROBAT 9

Jednoduchá ochrana

Nové neznamená vždy lepší: PDF dokumenty chráněné heslem, které uživatelé vytvořili v Acrobatu 9, lze snáze prolomit než ty z Acrobatu 8. Stará verze sází na rozsáhlé zakódování souboru: Kvůli tomu generátor PDF zakládá pro heslo hned několik hašovacích hodnot MD5 – to znesnadňuje jeho zjištění hrubou silou, spotřebuje ovšem také více času procesoru. V nové verzi chtěli vývojáři vlastně jen zvýšit výkonnost a nasadili proto pouhý jeden MD5 hash. Výsledkem je sice výrazně rychlejší Acrobat – jenomže útočníci teď dokáží prolomit heslo stokrát rychleji než dříve. Domnělým řešením doporučovaným firmou Adobe je používat dlouhá hesla. V praxi se však ukázalo, že velmi rychle se dají prorazit dokonce i osmimístná hesla. Co opravdu pomůže, jsou zvláštní znaky a číslice.
INFO: www.adobe.com

SPOLEČNOST SYMANTEC PRO WEB 2.0

Nezávislost na hardwaru

Premiéra: Goeverywhere.com je prvním pokusem Symantecu na poli „cloud coumputingu".

Společnost Symantec ohlásila nejnovější inovaci Symantec GoEverywhere, což je zabezpečený on-line pracovní prostor, který uživatelům umožňuje přístup k webovým aplikacím kdykoli a kdekoli pomocí téměř libovolného zařízení vybaveného webovým prohlížečem. Pracovní prostor GoEverywhere je po dobu beta testů programu zdarma k dispozici prostřednictvím bezplatného účtu na adrese **www.goeverywhere.com**.

„Rostoucímu použití webových aplikací se musí přizpůsobit také naše pracovní počítačové prostředí, které se musí přesunout na web, což podle našeho mínění povede k posunu v používání stolních počítačů," řekl Don Kleinschnitz, general manager Symantec GoEverywhere. „Beta verze pracovního prostoru GoEverywhere novátorským způsobem využívá koncepty ‚shluků' a Web 2.0 nové generace. Zákazníkům tím rozšiřuje možnosti volby v tom, jak a kdy mohou přistupovat k informacím."

Beta verze pracovního prostoru GoEverywhere vychází z odborných znalostí společnosti Symantec v oblasti zabezpečení a úložišť. Základní služba umožňuje uživatelům přístup k jejich on-line webovým aplikacím a nabízí výběr webových aplikací pro zpracování textů, vytváření prezentací a práci s tabulkami i přístup k e-mailu prostřednictvím webového rozhraní. K dalším výhodám patří nezávislost na hardwaru a operačním systému (je požadován pouze prohlížeč internetu), nulová potřeba údržby (není nutná správa IT, zálohování nebo aktualizace) nebo bezpečné jednotné přihlašování k webovým aplikacím. Beta verze pracovního prostoru Symantec GoEverywhere je k dispozici pro vyzkoušení zdarma na adrese **www.goeverywhere.com**. Názory účastníků beta testů jsou vítány. Pomohou v dalším vývoji a rozvoji pracovního prostoru GoEverywhere.

Komentář redakce: *O využívání technologií Web 2.0 a cloud computingu píšeme na jiném místě našeho časopisu. Všechny zmiňované technologie však mají jednu společnou slabinu – bezpečnost. Je málo pravděpodobné, že by uživatelé, dennodenně bombardovaní zprávami o útocích hackerů, ztrátách dat nebo odcizení přístupových údajů, chtěli svou důležitou práci přesunout na internet. Možná bude novinka od firmy z oblasti bezpečnostních technologií tím správným impulzem k lepšímu vývoji v této oblasti.*

KASPERSKY ANTI-VIRUS

Nový antivir pro Windows 7

Společnost PCS, oficiální distributor Kaspersky Lab pro ČR a SR, oznámila vydání technického prototypu Kaspersky Anti-Virus pro systém Windows 7. Tento program je založen na novém antivirovém enginu, který poskytuje komplexní ochranu před všemi druhy internetových hrozeb.

Prototyp společnosti Kaspersky Lab je komplexním řešením, které zahrnuje nejen antivirovou komponentu rozpoznávající škodlivý software na základě známých vzorků malwaru, ale také heuristickou analýzu, jež umožňuje odhalit a zablokovat dosud neznámé nebezpečné programy na základě jejich podezřelého chování. Produkt obsahuje také firewall a antispamový filtr. Cílem prototypu je poskytnout efektivní ochranu

Bezpečněji: Jedním z prvních bezpečnostních nástrojů pro Windows 7 byl Kasperky Anti-Virus.

proti všem druhům internetových hrozeb – virům, červům, trojským koním, spywaru, útokům hackerů i spamu. Jádrem prototypu je nový antivirový engine, který oproti předešlé verzi účinněji detekuje škodlivé programy. Nový engine lépe pracuje s objekty a optimalizuje využití systémových zdrojů, a tím zrychluje kontrolu (skenování) systému. Nově uvedený prototyp je plně kompatibilní s 32 i 64bitovými verzemi operačního systému Windows 7.

„Očekáváme, že nová verze operačního systému Microsoft Windows bude ještě oblíbenější než ta předešlá a předpokládáme, že po jejím oficiálním vydání na ni přejde značné množství uživatelů. Již jsme obdrželi velké množství žádostí od firem, které plánují přechod na Windows 7 a už nyní testují jejich efektivitu a kompatibilitu operačního systému s dalším používaným softwarem. Proto jsme prototyp našeho řešení pro systém Windows 7 vyvinuli v rámci divize, která je odpovědná za vývoj produktů pro firemní zákazníky," uvedl Alexej Kalgin, ředitel produktového marketingu, divize Corporate Business, Kaspersky Lab. Kaspersky Anti-Virus pro operační systém Windows 7 lze stáhnout z webu **www.kaspersky.com/windows7**.

Společnost Kaspersky Lab navíc plánuje během testovací fáze nového operačního systému nabídnout také nástroje pro centrální správu. Ve chvíli oficiálního uvedení finální verze Windows 7 na trh nabídne společnost Kaspersky Lab plné portfolio svých produktů, které poskytnou komplexní ochranu firemním i domácím uživatelům nového operačního systému.

INFO: www.kaspersky.com

STATISTIKY ZRANITELNOSTÍ

INF/Autorun na prvním místě

Červ Win32/Conficker, který se v lednu začal masově šířit, napadl v Česku pouze několik tisíc počítačů a umístil se až na 9. místě lokálního žebříčku sestaveného ze statistických dat systému ESET ThreatSense.Net. V Česku nejvíce počítače v lednu napadal adware Win32/Toolbar.MyWebSearch, tedy infiltrace snažící se o zahlcení počítače nevyžádanou reklamou.

Celosvětově se nejvíce v lednu šířil INF/Autorun (9,71 % ze všech zachycených infiltrací), což je směs trojských koní zneužívajících funkci automatického spuštění přenosných médií (autorun.inf) v operačním systému Windows. Uživatelé, kteří mají funkci automatického spuštění povolenou, se vystavují velkému riziku, že po vložení CD / DVD či připojení USB klíče, paměťové karty nebo fotoaparátu, dojde k přenesení infiltrace na jejich počítač.

V lednu ESET ThreatSense.Net na druhém místě detekoval rodinu trojských koní Win32/PSW.OnLineGames, která dokáže způsobit velké škody hlavně hráčům online her. Infiltrace se na napadeném počítači snaží o získání citlivých údajů týkajících se přihlášení do online her, čímž zpřístupní útočníkovi cestu k vykradení konta postiženého hráče.

Kromě INF/Autorun využívá USB disky a přenosná média ke svému šíření stále více počítačových hrozeb. Také mediálně známý červ Win32/Conficker se v lednu snažil kromě jiných metod šířit prostřednictvím funkce automatického spuštění po připojení vyměnitelného média. Potenciál ke vzniku virové epidemie se však nepotvrdil a Conficker se nakonec umístil až na třetím místě. Například v zemích západní Evropy nebylo šíření červa Conficker téměř zaznamenáno. Epicentrum naopak bylo na Ukrajině a v Rusku. Tento fakt může souviset s tím, že v zemích východní Evropy je stále instalováno velké množství nelegálních operačních systémů, a napadené počítače tak neměly staženu potřebnou bezpečnostní záplatu. V západní Evropě byla v lednu velmi rozšířená hrozba WMA/TrojanDownloader.GetCodec. Pokud se tento trojan dostane do počítače, najde všechny hudební nahrávky v populárních formátech a každou z nich mírně upraví. A to tak, že při následném spuštění se přehrávač pokusí stáhnout škodlivý obsah z internetové stránky tvůrců virových infiltrací.

INFO: zpravy.actinet.cz

OSOBNÍ ÚDAJE V OHROŽENÍ

Únik uživatelských dat u Monster Worldwide

Není to tak dávno, co česká média informovala o „hacknutí" serveru Libimseti.cz. Velkou mediální bublinu způsobil především únik tisíců lechtivých fotografií jednotlivých uživatelek. O tom, že nejde o nijak mimořádnou událost, nás ujistila i podobná aféra firmy z oblasti personální online inzerce. Společnost Monster Worldwide **(http://corporate.monster.com/)** potvrdila únik uživatelských dat z webu Monster.com a USAJOBS **(www.usajobs.gov/securityNotice.asp)**. Z databáze unikla data včetně loginů hesel a dalších informací o uživatelích. Společnost Monster Worldwide provozuje i českou verzi služby **(www.monster.cz)**, jejímž uživatelům doporučujeme okamžitou změnu přihlašovacích údajů a zvýšenou ostražitost ohledně výskytu dat ze svých životopisů v nepovolaných rukou.

INFO: zpravy.actinet.cz

BEZPEČNOST USA

Strategie informační bezpečnosti Spojených států

Barrack Obama, prezident Spojených států, deklaroval problematiku informační bezpečnosti jako strategickou prioritu **(www.whitehouse.gov/agenda/homeland_security/)**. Cílem je mimo jiné vytvořit bezpečnou infratstrukturu. Základem má být vývoj nových bezpečných systémů pro národní bezpečnost, ochrana infrastruktury zajišťující fungování ekonomiky, minimalizace možného zisku z nelegálních aktivit a povinnost společností zveřejňovat případné úniky osobních dat.

INFO: zpravy.actinet.cz

HROZBA PRO MOBILNÍ TELEFONY

Nový trojský kůň útočí na Symbian

Odborníci ze společnosti Kaspersky Lab odhalili nový škodlivý program pro Symbian. Tento populární operační systém využívají především mobilní telefony Nokia, ale i některé modely Samsung, Sony Ericsson, Motorola a další. Tento malware se poprvé objevil u uživatelů jednoho z indonéských mobilních operátorů. Trojský kůň napsaný ve skriptovacím jazyce Python zasílá zprávy SMS obsahující uživatelem neautorizovaný pokyn převést část peněz z účtu uživatele na jiný účet, který kontrolují podvodníci.

Jak je to možné? V síti příslušného indonéského operátora stačí k převodu peněz mezi účty uživatelů služby zaslat SMS na číslo 151. Kvůli softwarové zranitelnosti červ umožňuje tento převod provést bez toho, aby ho uživatel telefonu musel potvrdit či ho vůbec zaznamenal. Trojský kůň Trojan-SMS.Python.Flocker byl laboratořemi společnosti Kaspersky Lab zjištěn v pěti variantách, od . ab po .af. Převáděné částky se pohybují od 0,45 do 0,90 dolarů. Podvodníci doufají, že to, že jednotlivá převáděná částka je relativně nízká, jim umožní uniknout odhalení, protože uživatelé tuto aktivitu nezjistí nebo alespoň nebudou zpětně řešit. Pokud se takto ale útočníkům, podaří infikovat větší množství telefonů, částka, kterou výsledně získají, může být docela značná.

„Samozřejmě, že autoři trojského koně chtějí získat peníze," vysvětluje Denis Maslennikov, senior malware analyst ve společnosti Kaspersky Lab. „Až dosud se mnozí domnívali, že podvodné programy odesílající zprávy SMS bez uživatelova vědomí jsou pouze ruským fenoménem. Nyní je jasné, že se nejedná pouze o problém ruských uživatelů, ale s těmito podvody je třeba počítat i v jiných zemích."

Již loni byl například zaznamenán podobný útok v Číně, kdy podvodníci šířili malware, který ovládl mobilní telefon. Uživatelům se zobrazila výzva, že pokud chtějí získat nad svým zařízením opět kontrolu a používat ho, musí zaplatit 7 dolarů. A jak se bránit? Společnost Kaspersky Lab doporučuje uživatelům při prohlížení rizikových internetových stránek z mobilního telefonu mimořádnou opatrnost a především používání „mobilních antivirových řešení".

F-SECURE OD O2

Internet pod ochranou

Internet od O2 ochrání svým uživatelům data i počítač před napadením. Firma totiž pro své zákazníky připravila profesionální antivirový program F-Secure Profi Antivir. Služba je k dispozici od 1. února 2009 a je určena pro nové i stávající zákazníky všech variant vysokorychlostního internetu O2 Internet ADSL. Využívat ji mohou i zákazníci s mobilním připojením. Novou antivirovou ochranu dává Telefónica O2 svým klientům zdarma po celou dobu využívání služby.

„S nárůstem využívání počítačů je stále aktuálnější otázka bezpečnosti. Uvědomujeme si, že bez řádného zabezpečení je přístup na internet stále riskantnější. Podceňovat tato rizika se nevyplácí. Našim zákazníkům díky programu F-Secure odpadne obava o zavirování jejich počítače, krádež hesel internetového bankovnictví,"uvedl Matts Johansen, výkonný ředitel pro marketing spotřebitelského segmentu.

Profesionální program F-Secure Profi Antivir získá každý zákazník zdarma ke službám O2 Internet ADSL a O2 Internet Mobil. Nástroj obsahuje antivir, firewall a antispyware. Noví zákazníci obdrží program s omezenou platností na 60 dní na instalačním CD jako součást příslušenství pro provoz O2 Internet ADSL. Po uplynutí této doby zdarma obnoví platnost prostřednictvím internetových stránek a na základě automaticky zaslaného klíče. Stávajícím zákazníkům bude program ve stejné verzi k dispozici ke stažení na internetové stránce **www.internetbezpecne.cz**. Jeho platnost pak prodlouží stejným způsobem.

ANALÝZA TREND MICRO

Hrozby z kontinentů

Žádné překvapení – surfování po internetu bez nainstalovaného bezpečnostního softwaru může mít nebezpečné následky, zejména kvůli nárůstu webových hrozeb (ve srovnání s rokem 2005 o téměř 2 000 procent). Podle expertů Trend Micro zabývajících se počítačovými hrozbami pocházelo více než 50 procent z nejnebezpečnější stovky malwarových útoků z internetu. Zmiňovaný malware se do počítače uživatele dostává po návštěvě neznámých škodlivých webů.

Druhým největším zdrojem infekcí (43 procent) je malware, který se již nachází v počítačových systémech. Současné hrozby se obvykle skládají z více součástí, které se do počítače dostávají postupně – jedna nebo několik nejdříve stažených částí malwaru se ukryje v určitém souboru, odkud kontaktuje vzdálené místo na síti, z něhož natáhne do počítače další výkonný kód, jako je například malware pro odcizení dat. Přílohy e-mailů přicházejících z neznámých nebo škodlivých zdrojů tvoří třetí největší zdroj (12 procent) infekcí.

Dalšími obvyklými způsoby nákazy jsou tyto:

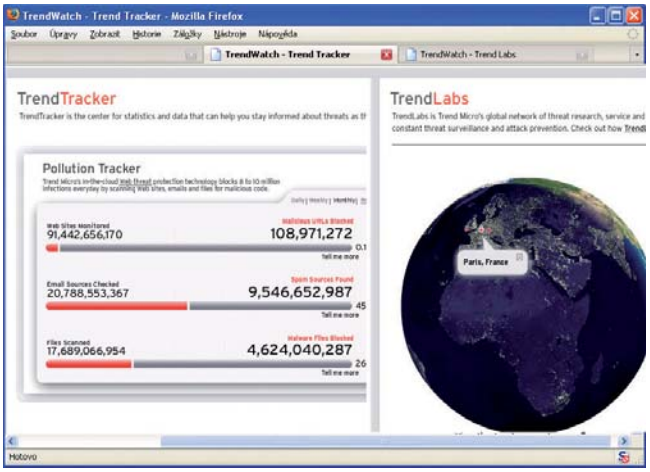
- přijímání souborů přes aplikace pro instantní messaging;
- stahování souborů nabízených v P2P sítích;
- používání přenosných záznamových médií (flash disky nebo přenosné či externí pevné disky);
- nedostatečné záplatování aplikací, u nichž byly zjištěny zranitelnosti.

I když údaje z jednotlivých regionů vykazují podobný celkový trend, přesto existují drobné odchylky: Severní Amerika stále vykazuje největší množství adwaru a výrazný nárůst malwaru pro odcizení dat, který se do počítačů dostává přes internet.

Malware pocházející z přenosných záznamových médií (flash disky, paměťové karty nebo přenosné či externí pevné disky) se nejvíce vyskytuje v Asii a Austrálii (29,31 procenta). Ve většině asijských zemí je mezi nejčastějšími zdroji nákazy (nejvíce ze všech regionů) malware šířící se prostřednictvím přenosných zařízení. Výjimku tvoří Čína – ta však kvůli velkému množství hráčů on-line her zase vykazuje vysoké procento spywaru pro tyto hry.

Hlavní příčinou nákazy v Evropě, na Středním východě a v Africe jsou trojské koně, které instalují do počítačových systémů další škodlivé soubory – a to buď stažením ze vzdáleného počítače, nebo jejich přímým umístěním do systému z kopie umístěné v jejich vlastním kódu. V tomto regionu jsou rozšířené i nákazy pomocí škodlivých IFrames (Inline Frames, oblíbený prvek webového designu, který umožňuje, aby jeden HTML dokument byl vložen do jiného HTML dokumentu).

Hlavní hrozby v Latinské Americe jsou rozmanité, region v současnosti vykazuje zejména nárůst vícekomponentových útoků. Některý „nový malware“ nalezený v počítačích do nich byl ve skutečnosti vložen jiným malwarem, který se v počítači nacházel již dříve.



Globální data: Na webu TrendWatch **(http://itw.trendmicro.com)** najdete i aktuální globální informace o jednotlivých typech hrozeb.

INFO

Nová bezpečnostní rizika

APPLE SAFARI

Ve webovém prohlížeči Apple Safari byla nalezena zranitelnost, zneužitelná nepovolanou osobou k získání citlivých informací. Zranitelnost je zavíněna nespecifikovanou chybou ve zpracování URL adres jednotlivých RSS kanálů. Zasaženi jsou všichni uživatelé Safari jak na Windows tak na Mac OS bez ohledu na to, zda RSS používají. Více informací naleznete na webu **http://brian.mastenbrook.net/display/27**. Společnost Apple byla s problémem seznámena.

INFO: zpravy.actinet.cz

SYMANTEC APPSTREAM CLIENT

Byla nalezena zranitelnost v Symantec AppStream Client, on-demand software delivery systému. Zranitelnost je zavíněna LaunchObj ActiveX ovladačem (launcher.dll). Této chyby může být zneužito ke stažení a spuštění libovolného souboru v kontextu přihlášeného uživatele. Zranitelnost zasahuje verze předcházející 5.2.2 SP3 MP1. V této verzi je již opravena. Bližší informace v původním oznámení **(na http://www.kb.cert.org/vuls/id/194505)**, případně přímo na stránkách výrobce **(www.symantec.com)**.

INFO: zpravy.actinet.cz

CISCO ROUTERY

The Register píše o zajímavém objevu výzkumníka z Recurity Labs v Berlíně **(http://www.theregister.co.uk/2009/01/05/cisco_router_hijacking/)**. V Cisco routerech běžících na procesorech PowerPC a MIPS lze s využitím kódu ROMmonu (podobný BIOSu v PC) kompromitovat IOS (software ve většině Cisco zařízeních).

INFO: zpravy.actinet.cz

SUN SOLARIS – OPENSSL – „EVP_VERIFYFINAL()“

Podle informačního serveru Secunia **(http://secunia.com/advisories/33765/)** potvrdila firma Sun zranitelnost v Sun Solaris, jejíž zneužití umožní potenciálním útočníkům útoky typu spoofing. Více podrobností o tomto problému, stejně jako možné řešení zranitelnosti najdete na webu výrobce **(http://sunsolve.sun.com/search/document.do?assetkey=1-66-250826-1)**.

INFO: zpravy.actinet.cz

NOVINKA NA POLI SOFTWARU

Norton 360

Na počátku února uvolnila společnost Symantec veřejnou beta verzi bezpečnostního balíku Norton 360. Verze 3.0 nabízí all-in-one bezpečnostní řešení pro osobní počítače. Nyní nově nabízí skenování pouze ohrožených souborů, což šetří čas a zlepšuje ochranu. Díky identifikaci nebezpečných stránek a podezřelých prodejců lze bezpečněji surfovat na internetu. Potěší také vylepšená ochrana identity při internetovém nakupování nebo bankovních transakcích.

Novinku si mohou vyzkoušet i uživatelé operačního systému Windows 7 Beta (protože se ale tento systém stále vyvíjí, není možné zajistit plnou podporu). Plně kompatibilní verze Norton 360 bude k dispozici s oficiálním vydáním tohoto nového operačního systému. Chcete produkt otestovat, můžete si jej stáhnout z internetových stránek Symantec: **www.symantec.com/norton/beta/overview.jsp?pvid=n3603beta**.

INFO: www.symantec.com

TREND MICRO PRO LEPŠÍ BEZPEČNOST DĚTÍ

Den bezpečnějšího internetu

U příležitosti letošního Dne bezpečnějšího internetu („Safer Internet Day 2009“), kterým byl 10. únor, upozornila společnost Trend Micro na zvláštní aspekt IT bezpečnosti: bezrizikové užívání internetu dětmi a mladistvými. Tento mezinárodní den globálních aktivit se poprvé uskutečnil v Evropské unii v roce 2004 a od té doby se koná vždy druhý čtvrtek v únoru.

V rámci tohoto projektu zahájila společnost Trend Micro kampaň „Internetová bezpečnost dětí a rodin“, kterou chce přispět k větší bezpečnosti dětí a mladistvých na internetu. Program nabízí rodičům a učitelům náměty, jak upozornit mladé uživatele na internetové hrozby. Trend Micro navíc partnersky podporuje organizace, jako jsou Childnet International, ConnectSafly.org a Common Sense.

U příležitosti Dne bezpečnějšího internetu 2009 nabízí Trend Micro následující tipy pro bezpečnější internet pro děti a mladé uživatele.

- Sledujte a omezujte dobu využívání internetu: Domácí počítač by měl být umístěn tak, aby bylo možné sledovat chování dětí na internetu. Podle věku dětí je nezbytné regulovat dobu a čas, kdy mají děti k internetu přístup.
- Povídejte si s dětmi o využívání internetu: Zejména u malých dětí doporučuje Trend Micro rodičům sledovat oblíbené stránky svých dětí a rozhodnout, zda jsou vhodné pro děti daného věku.
- Kontrolujte obsah a chraňte data: Děti by měly být poučeny o tom, že by neměly na internetu zveřejňovat takové údaje, jako jsou adresy nebo telefonní čísla.
- Zjišťujte, s kým se děti na internetu baví: Rodiče by měli být pozorní zejména v případě, že jejich děti přicházejí na internetu do styku s cizími lidmi. Proto by měli s dětmi neustále hovořit o jejich aktivitách na internetu.
- Mějte nebezpečné webové stránky pod kontrolou: Programy pro zjišťování důvěryhodnosti webových stránek, jako je například TrendProtect, umožňují kontrolovat bezpečnost stránek a varují před nakaženými stránkami nebo stránkami, z nichž se šíří malware.
- Využívejte URL filtry: Většina internetových bezpečnostních balíků nabízí URL filtry, které zamezují v přístupu na webové stránky s nevhodným obsahem.
- Aktualizujte svůj bezpečnostní software: Ve svém počítači vždy mějte aktualizovanou verzi bezpečnostního softwaru, abyste ho mohli chránit před viry, spamem, spywarem a dalším malwarem.

PODVODNÉ WEBOVÉ STRÁNKY

Rezignace Baracka Obamy

Laboratoře PandaLabs společnosti Panda Security detekovaly 40 webových stránek, které zneužívají zvolení prezidenta Spojených států Baracka Obamy k šíření malwaru. Stránky obsahují nadpis „Barack Obama rezignoval“. Po kliknutí na článek a potvrzení stažení souboru se počítač infikuje zákeřným malwarem, který změní počítač na „zombie“ (podvodníci pak mohou počítač ovládat na dálku). Tyto zombie bývají obvykle spojovány do sítí botů, které podvodníci pronajímají třetím stranám. Ve finále jsou pak napadené počítače zneužívány k rozesílání spamu nebo k útokům typu „denial of service“. Podle PandaLabs se zdroj útoku nachází v Číně, protože všechny domény zakoupila čínská společnost s dlouhou historií útoků pomocí škodlivých kódů.

Není to poprvé, co bylo jméno Baracka Obamy internetovými podvodníky zneužito k šíření malwaru: falešné zprávy (s dárkem v podobě malwaru) se objevovaly už během kampaně a krátce po volbách.

Více informací o tomto útoku najdete na blogu Pandalabs: **http://pandalabs.pandasecurity.com.**

INFO: www.pandasecurity.com

NÁSTROJE TRUSTPORT

Řešení problému Conficker

Několikrát zmiňovaný internetový červ Conficker se sice na první místa virových hitparád nedostal, přesto ztěžuje život milionům uživatelů. Jak se ho lze zbavit?

Červ pro své šíření zneužívá zejména kritickou chybu v systémové službě, která se stará o síťové sdílení složek. Na infikovaném počítači pak dochází ke vzdálenému spouštění škodlivých kódů. Aby zabránil své detekci a likvidaci, Conficker okamžitě znemožní automatické aktualizace systému a bezpečnostního softwaru některých antivirových výrobců. Následně přes místní síť či internet napadá další počítače.

Zajímavé alternativy pro vyřešení tohoto problému nabízí bezpečnostní řešení firmy TrustPort. Jednou z cest je vygenerování mobilního antiviru na nezavirovaném počítači. Ten lze uložit na flash disk a poté použít pro vyčištění infikovaného systému. Dalším řešením je vytvořit pomocí produktu TrustPort Antivirus nebo TrustPort PC Security záchranný disk, který obsahuje nezavirovaný operační systém a antivirový software. Tak lze spolehlivě zlikvidovat škodlivé kódy i po fatálním selhání operačního systému instalovaného na pevném disku.

INFO: www.trustport.cz

KONEC ANALOGU

Vypnutí Žižkova

Konec analogového vysílání v Praze se blíží. 30. dubna 2009 bude vypnut analogový televizní vysílač na pražském Žižkově. Neznamená to však definitivní konec analogového vysílání v Praze. Analogový televizní signál bude možné přijímat i nadále pomocí ostatních vysílačů a vykrývačů. Ne všude však bude signál ve stejné kvalitě a například Primu nebude možné naladit na poměrně velkém území Prahy. Celá Praha je však již pokryta digitálním televizním vysíláním, proto doporučujeme analogové vysílání opustit. Alternativ je celá řada – od digitálního vysílání DVB-T přes satelitní či kabelovou televizi až po IPTV, kterou ve velkém prosazuje O2.

Na Chip DVD v rubrice Chip Plus najdete speciální Diginoviny, ve kterých se dočtete podrobnosti a také alternativy k analogovému televiznímu vysílání.

INFO: www.digitalne.tv

BRITANNICA 2.0

Konkurence pro Wikipedii?

Ve snaze konkurovat Wikipedii přichází Encyclopaedia Britannica Online s novými možnostmi a rozšířeními, s jejichž přispěním se pokusí dohnat velký náskok svého konkurenta.

Encyklopedie hodlá rozšířit řady svých redaktorů, kteří budou pracovat na správě aktuálních témat. Pro návštěvníky stránek je nyní u každého článku k dispozici tlačítko „Navrhni úpravu“, které umožňuje navrhnout případné změny. Nefunguje to však stejně jako v případě Wikipedie. Navrhnuté změny na Encyclopaedia Britannica budou před publikováním povinně zhodnoceny a schváleny redaktory. Uživatelé, kteří navrhnou změny, budou v článku zveřejněni a návštěvníkům bude poskytnut seznam všech, kteří přispěli, spolu s historií posledních úprav.

INFO: www.smh.com.au

ACER ASPIRE ONE

Tentokrát s 10palcovým displejem

Firma Acer představila nový netbook Aspire One, který je tentokrát vybaven větším, 10“ displejem. Netbook váží 1,18 kg a je optimalizován pro prohlížení webových stránek a využívání internetu. Displej je podsvícen LED diodami a disponuje rozlišením 1 024 × 600 bodů.

V horní části displeje se nachází webová kamera Acer Crystal Eye. Netbook je standardně dodáván s připojením Wi-Fi (802.11b/g) a Bluetooth a může být doplněn i volitelnými bezdrátovými technologiemi WiMAX nebo 3G. Na baterie by měl vydržet až sedm hodin. Počítač v lesklém provedení se bude prodávat ve čtyřech barevných odstínech (bílém, modrém, červeném a černém). Může být dodán až s 2GB pamětí a přes své malé rozměry se může pochlubit 160GB pevným diskem a dále multiformátovou čtečkou paměťových karet.

INFO: www.acer.cz

NOKIA N79

Trénink s mobilním telefonem

Nokia představila mobilní telefon Nokia N79 Active, k jehož příslušenství patří bezdrátový pás na měření tepové frekvence Polar Bluetooth WearLink. Tento doplněk řady Nokia Nseries tvoří dokonalého společníka při běhání. Systém A-GPS a nová verze populární aplikace Nokia Sports Tracker vás pobízejí, abyste zaznamenávali a publikovali na webu své oblíbené trasy a údaje o své kondici. Můžete také sdílet hudbu, kterou jste při tréninku poslouchali, stejně jako uploadovat a geotagovat fotografie své trasy pořízené pětimegapixelovým fotoaparátem vestavěným v telefonu Nokia N79 Active.

Verze Active je dodávána se sportovními sluchátky a páskou na ruku, abyste mohli během tréninku zůstat připojeni. Můžete si také bezdrátově naladit rádio pomocí vysílače FM v telefonu. Předpokládaná cena je kolem 12 500 Kč.

INFO: www.nokia.cz

CENY ZA VOLÁNÍ

Levnější volání do mobilních sítí

Od 1. února platí nový výměr ČTÚ (Český telekomunikační úřad), stanovující nové propojovací poplatky za hovory termínované v mobilních sítích. Zjednodušeně řečeno se jedná o velkoobchodní cenu za volání do mobilní sítě. Jako první zareagoval na tuto skutečnost U:fon, který zlevnil hovorné u svých tarifů. Později následovali také někteří VoIP operátoři. Podrobnosti najdete v Top listu na straně 104.

E-BOOK

Amazon uvádí čtečku Kindle 2

Čtečka elektronických knih Kindle od společnosti Amazon, využívající technologii elektronického papíru, je již na trhu delší dobu, konkrétně od listopadu 2007. Není proto divu, že se dočkala svého nástupce, který má odstranit některé z nedostatků starého modelu.

Již jsou také k dispozici první skutečné fotografie Kindle 2 – je z nich patrné, že změn se dočkal celkový design a čtečka je více zaoblená, stejně tak klávesy jsou kulaté a více odpovídají rozložení na běžné klávesnici. Scrollovací kolečko pak nahradil malý joystick. Displej je prakticky stejný jako u Kindle 1 (je tedy černobílý) a podle všeho pravděpodobně nebude disponovat ani podsvícením, jako například konkurenční Reader Digital Book PRS-700BC od Sony.

Nemilým překvapením je však to, že čtečce Kindle 2 opět chybí slot pro paměťové karty, takže se uživatel bude muset spolehnout na zabudovanou paměť, jejíž kapacita se odhaduje na 2 GB.

INFO: www.itnews.sk

SOFTWARE602

Představení Gerbery

Česká firma Software602, známá výrobou kancelářských nástrojů, představila nový produkt. Kompletní řešení pro nahrazení oběhu papírových dokumentů vývojáři nazvali Gerbera.

Jak charakterizovat tento nástroj? Produkt obsahuje inteligentní formuláře a nástroje pro jejich oběh, schvalování a archivaci. Podle obchodního ředitele firmy Pavla Nemravy jde o předpřipravené řešení, které lze velmi rychle uzpůsobit potřebám zákazníka a napojit jej na jakýkoli informační systém. Technologickým základem jsou přitom inteligentní formuláře 602XML.

Společnost Software602 také oznámila předběžné výsledky za minulý rok. Dosáhla obratu 81,7 milionu korun, což představuje meziroční nárůst 22 %. Více než 80 % obratu Software602 nyní pochází z projektů dodávek na míru jednotlivým zákazníkům, jen 8 % tvoří prodej softwarových licencí.

INFO: www.602.cz

DOPLNĚK PRO FIREFOX

Live Search i ve Firefoxu

Microsoft v takzvané „válce prohlížečů“ rozhodně nezahálí a uvolňuje nový doplněk určený pro konkurenční prohlížeč Firefox. Tato aktualizace umožňuje optimalizované využití služby Microsoft Live Search přímo v prohlížeči Firefox.

Nový add-on, který do pravého horního rohu prohlížeče Firefox přidá malé vyhledávací okno, se může pochlubit i automatickou nápovědou určenou pro začínající uživatele vyhledávače Live Search.

Vydání doplňku Live Search je součástí strategie společnosti Microsoft, jež má vést k posílení pozice prohlížeče Internet Explorer. Se svými 67,6 % sice trhu stále dominuje, na paty mu však šlape právě Mozilla Firefox, jejíž podíl 21,5% je pro open-source novým rekordem.

INFO: http://blogs.msdn.com/livesearch/

KONICA MINOLTA MAGICOLOR

Superlevná barevná tiskárna

V podobě modelu Magicolor 1600W představila firma Konica Minolta levnou barevnou tiskárnu pro domácí použití. Kvůli nízkým pořizovacím nákladům je však třeba vzít v úvahu spíše nižší rychlost tisku: přístroj zvládne pouze pět barevných nebo dvacet černobílých stran za minutu. Tiskové rozlišení se nachází na přijatelných 600 × 600 dpi při barevném a 1 200 × 600 dpi při černobílém tisku. Díky kompaktní velikosti 28 × 40 × 38 cm se již nyní dostupná tiskárna vejde i na malou plochu.

INFO: www.konicaminolta.cz