DATA A FAKTA

Barometr nebezpečí
v dubnu:

S počátkem jara narůstá výskyt spamu. Přibývá také reklam na domněle užitečný ochranný software.

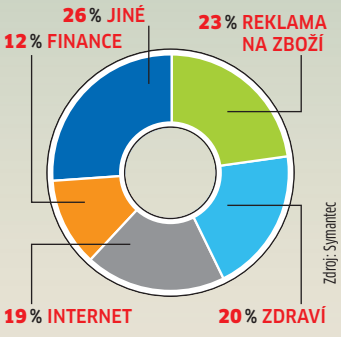
Nejdůležitější útoky roku 2008

1. **Využití mezery v DNS**
   Útočníci přesměrovávají URL
2. **Napadení LHC v CERN**
   Přístup k citlivým datům
3. **Infikování laptopů NASA**
   Na ISS dorazil první virus
4. **Únosy e-mailových účtů**
   Oběťmi jsou Sarah Palin & Co.
5. **Zmanipulování stránky o epilepsii**
   Hackeři ukazují blikající obraz

Zdroj: PC Tools

V loňském roce napadli hackeři důležité oblasti internetu.

Čeho se týká spam



Masová reklama: Obsahy spamu se zaměřují především na čtyři oblasti.

Číslo měsíce

316

eur – takový příspěvek požaduje pochybný antivirový klub v Dubaji za bezplatné demoverze antivirových nástrojů.

Mohutný útok nových virů

Armáda i firemní administrátoři jsou bezmocní. **VIRUS CONFICKER** se údajně nedá zastavit – a přitom je obrana docela jednoduchá.

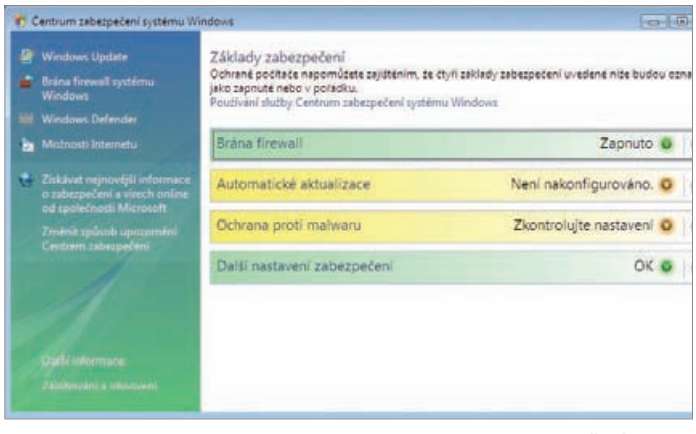
FABIAN VON KEUDELL

Nikdo jej nedokáže zastavit – bezmocná je dokonce i společná speciální jednotka složená z členů všech velkých výrobců antivirů, všech velkých softwarových firem a nadřízeného internetového úřadu ICANN (Internet Corporation for Assigned Names and Numbers). Úspěch nepřinesla ani odměna ve výši 194 000 eur. Samotné slůvko Conficker je dnes pro správce systémů po celém světě stále ještě noční můrou. Postiženy už jsou části německého bundeswehru, francouzských ozbrojených sil, americká letecká společnost Southwest Airlines a kolem milionu soukromých počítačů na celém světě (například v sousedním Německu více než 16 000)…

Co ale dělá virus tak nebezpečným, proč jej nikdo nedokáže zastavit? Prozradíme vám, proč se škůdce dokázal tak rychle rozšířit – a jak mu v tom lze bránit.

Všechno začíná 23. října 2008: Conficker využívá bezpečnostní mezeru ve Windows MS08-067, tedy „remote code execution vulnerability“. Pomocí zmanipulovaného přihlášení do sítě proniká virus do nechráněných počítačů po celé planetě. Už jen tím by mohl napáchat mnoho škod, kdyby totiž s oprávněním správce spouštěl vetřelecké programy. To však nedělá – místo toho se rozmnožuje tak, že uvnitř sítě záměrně vyhledává sdílené soubory a tím se šíří na jiné počítače. Vedle toho využívá i USB paměti a externí disky. Aby si nikdo nepovšiml, že v počítačích tropí své rejdy, blokuje funkci automatické aktualizace Windows, centrum zabezpečení Windows, antivirový nástroj Defender a systémový protokol Windows – aniž by o tom měl uživatel tušení.

Doposud virus napáchal jen poměrně málo škod. Experti antivirových firem se však obávají, že velký útok teprve přijde. Virus totiž dále zbrojí – nyní už se úspěšně brání dokonce i různým antivirovým nástrojům.



Domnělá ochrana: Virus Conficker zmanipuluje centrum zabezpečení Windows, které pak přestane varovat před infekcemi.

Časová tíseň: Je třeba jednat dřív, než dojde k masovému útoku

Greg Rattray, „Chief Internet Security Advisor“ v ICANN, vychází z toho, že se Conficker ještě více rozšíří – v důsledku četných nechráněných počítačů. Přitom pomoc by byla úplně jednoduchá: instalovat aktualizace Windows a počítače skenovat aktuálním antivirovým systémem. Například produkty firem Kaspersky a Symantec škůdce rozpoznají, i když už se usadil v počítači. Zbývá doufat, že autoři Confickeru nezatroubí k velkému útoku dříve, než bude většina počítačů chráněna. S obrovskou sítí botů osazených Confickerem se totiž dají obratem ruky ochromit i webové stránky renomovaných firem.

INFO: www.icann.org

VYLEPŠENÍ OD ESETU

SysInspector v nové verzi

Byla uvolněna nová verze diagnostického nástroje Eset SysInspector. Ten je možné stáhnout zdarma na adrese **www.eset.cz/cz/eset-sysinspector**.

Nová verze produktu nabízí unikátní možnost odstranění problematických infiltrací pomocí funkce Servisní skript. Uživatel má možnost zaslat specialistovi technické podpory log přímo z grafického rozhraní diagnostického nástroje Eset SysInspector. „Tento log je následně analyzován a na základě informace o nalezené infiltraci je vytvořen textový skript, který je ihned zaslán zpět uživateli. Ten si textový skript importuje přímo do nástroje Eset SysInspector a zvolí konkrétní infikovaný soubor pro spuštění skriptu,“ říká Martin Jonáš, technický specialista, který lidem pomáhá v rámci projektu Antivirová ambulance bezplatně odstraňovat z počítačů škodlivý software.

Pomocí funkce Servisní skript je zaručeno spolehlivé vyléčení jednotlivých problematických infiltrací.

Eset SysInspector byl vyvinut pro účely důkladného prozkoumání operačního systému počítače v případech, kdy je chování počítače nestabilní a způsobuje uživateli problémy. Informace o nainstalovaných ovladačích, programech, síťových připojeních atd. mohou pomoci expertům, ale i laikům, zjistit příčiny podezřelého chování počítače. Eset SysInspector je určen běžným uživatelům, bezpečnostním technikům či pracovníkům technické zákaznické podpory a napomáhá odhalovat počítačové hrozby, především ty, které jsou pro běžného uživatele neviditelné (pracují na pozadí, zpomalují systém apod.).

INFO

Nová bezpečnostní rizika

TWITTER

Služba Twitter umožňuje účastníkům společenské komunity psát příspěvky i prostřednictvím SMS. Adresu odesílatele je však možné zfalšovat a příspěvky tak vytvářet na cizí účet. Od Twitteru zatím není řešení k dispozici, proto deaktivujte SMS funkci.
INFO: www.twitter.com

MICROSOFT EXCEL

Ve zmanipulovaném tabulkovém souboru mohou útočníci propašovat do počítače škodlivý kód. Uživatel pak ale musí program sám spustit. Záplata zatím není k dispozici. Neotvírejte proto žádné soubory, které neznáte.
INFO: www.microsoft.com

MOZILLA FIREFOX

Stačí jediná návštěva na webové stránce hackerů, aby jí browser vydal všanc uživatelova data a vpustil do vlastního počítače škodlivý kód. Nová verze bezpečnostní mezeru zaceluje. E-mailová „souprava“ Mozilly s názvem Thunderbird není touto chybou postižena.
INFO: www.mozilla-europe.org

GOOGLE CHROME

V prohlížeči Google Chrome byla nalezena zranitelnost způsobená chybou ve WebKitu při zpracování SVGlist objektů. Tato zranitelnost může být zneužita ke spuštění libovolného kódu. Chyba byla nalezena ve verzi 1.0.154.65. Problém se týká i uživatelů prohlížeče Safari, který používá tento WebKit také.
INFO: zprávy.actinet.cz

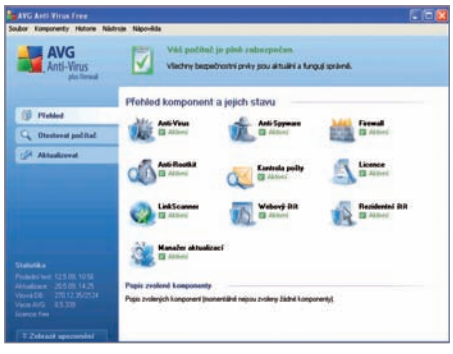
HP INSIGHT CONTROL SUITE FOR LINUX

Společnost HP odhalila ve svém produktu HP Insight Control Suite For Linux několik zranitelností. Chyby mohou být zneužity k překlenutí bezpečnostních pravidel nebo k vyvolání útoku CSFR (Cross-Site Request Forgery). Bližší informace včetně vydaných záplat naleznete na stránkách Hewlett-Packard.
INFO: zprávy.actinet.cz

AVG ANTI-VIRUS FREE EDITION

Antivirový software v českém jazyce

Společnost AVG Technologies uvolnila bezplatnou verzi svého antivirového systému AVG Anti-Virus Free Edition v českém jazyce. Produkt slouží k základní ochraně počítače před viry i spywarem a umožňuje bezpečné prohlížení webových stránek i práci s internetem. Volná edice AVG je určena výhradně pro domácí nekomerční použití na jednom počítači, je kompatibilní s operačními systémy Windows Vista i Windows XP, ale firma pro ni na rozdíl od svých placených produktů nezajišťuje nepřetržitou technickou podporu. AVG Anti-Virus Free Edition je uživatelům po celém světě nyní k dispozici již v jedenácti jazycích.



Jen základ: Bezplatná verze antiviru nabízí pouze základní ochranu před hrozbami z internetu...

Kvůli stále intenzivnějším webovým útokům, kdy je každodenně infikováno kolem dvou milionů stránek, se společnost AVG Technologies rozhodla zařadit do bezplatné verze i funkci AVG Active Surf-Shield. Ta zabraňuje infikování počítače při nechtěném stahování nebezpečných souborů či skriptů a současně zajišťuje, že navštívené stránky nabízejí ve chvíli jejich otevření bezpečný obsah. Doplní tak ve free verzi již dříve obsaženou funkci AVG Search-Shield, která bezpečně vyhodnocuje v reálném čase všechny výsledky hledání na internetu a míru rizika nákazy signalizuje ikonou vedle jednotlivých odkazů. Pracuje přitom například s internetovými vyhledávači Google, Yahoo!, MSN nebo Baid. Obě funkce jsou součástí unikátní technologie LinkScanner, která chrání uživatele před skrytými i krátkodobými hrozbami na internetu. Software je k bezplatnému stažení připraven na adrese **http://free.avg.cz/download-den-avg-anti-virus-free-edition**. Doporučenými systémovými prostředky jsou procesor Intel Pentium, 300 MHz, pro instalaci 30 MB volného místa na disku a 256 MB paměti RAM.

NOVÁ SLUŽBA

OnlineFamily.Norton

Společnost Symantec Corp. oznámila spuštění nové služby, která zaujímá odlišný přístup k on-line ochraně dětí. Symantec nabízí OnlineFamily.Norton **(http://onlinefamily.norton.com/)**, což je služba s ročním „předplaceným odběrem" v hodnotě 60 USD, která bude do 1. ledna 2010 nabízena zdarma.

Služba OnlineFamily.Norton není jako tradiční produkty s funkcí rodičovského zámku, které se zaměřují pouze na blokování a sledování činností dětí on-line. Tato služba nabízí širší pomoc rodičům v získávání kontroly nad šedými oblastmi internetu. Rodiče sice potřebují nástroje pro on-line ochranu dětí, ale stejně důležité je i vzdělávání a komunikace s dětmi.

Podle průzkumu Norton Online Living Family Survey, provedeného v březnu 2009, se 56% rodičů obává, že se jejich děti mohou setkat s nebezpečími internetu (například s on-line útočníky a internetovou šikanou). To je víc, než kolik se jich obává nebezpečí souvisejících s drogami (44 %). Téměř polovina všech dotazovaných dětí (47%) také připouští, že vyhledávají „choulostivá" témata on-line nebo o nich na internetu čtou, ale daleko menší část (35%) z nich o těchto tématech s rodiči hovořila. Je zřejmé, že je zapotřebí řešení, které pomůže rozvíjet diskusi mezi rodiči a dětmi. Řešení OnlineFamily.Norton je postavené na filozofii dialogu, tudíž udržuje přehled rodičů nejen o činnosti dětí on-line, ale také o tom, co je na internetu i mimo internet zajímá.

Řešení OnlineFamily.Norton podporuje diskusi následujícími prostředky:

- Skutečná transparentnost: Při nastavování služby jsou rodiče a děti vedeni ke společnému vymýšlení a vytváření domácích pravidel pro „on-line činnosti". Děti vždy vědí o tom, že je služba OnlineFamily.Norton v počítači aktivní, a kdykoli také mohou zobrazit domácí pravidla, která se svými rodiči vytvořily.
- Pochopení záměrů dětí: Rodiče mohou zobrazovat slova a fráze, které dítě hledá na webech jako Google, YouTube a Wikipedia, a vidí, kam se pomocí nich dostane on-line. Tato funkce také dává rodičům představu o tématech, o která se jejich dítě zajímá.
- Přístup k informacím ze společenských sítí: Služba OnlineFamily.Norton sleduje činnost ve společenských sítích, jako jsou Facebook a MySpace, a nabízí možnost podívat se, jak děti popisují svoji osobu, když se přihlašují, a jak často se přihlašují.
- Zasílání zpráv v reálném čase: Děti mohou rodičům posílat v reálném čase prostřednictvím webu OnlineFamily.Norton nebo e-mailu informace o svých záměrech, když se pokoušejí navštívit blokovaný webový server.

Přizpůsobitelné nástroje pro zajištění bezpečnosti dětí

Účinné nástroje pro ochranu dětí před nebezpečími on-line jsou stále ještě nutností a ve spojení s komunikací poskytují dětem nejlepší ochranu a poučení o hrozbách, které s sebou přináší použití internetu. Služba OnlineFamily.Norton dává rodičům přístup k následujícím technologiím, které pomáhají zajistit bezpečnost dětí on-line:

- Sledování rychlých zpráv: Rodiče mohou sledovat na různých úrovních konverzaci pomocí rychlých zpráv se všemi kamarády.
- Pohodlná kontrola nad webovými servery: Možnost zakázat více než 40 kategorií témat dává kontrolu nad webovým obsahem vstupujícím do domácnosti. Starším dětem mohou rodiče povolit přístup ke všem webovým serverům, ale mohou označit nevhodné servery, aby se děti mohly samy rozhodnout, zda příslušný web navštíví.
- Zabezpečené osobní údaje: Sledování, vykazování a blokování osobních údajů, které se mohou děti záměrně nebo neúmyslně pokusit odeslat prostřednictvím rychlé zprávy, společenské sítě nebo webového serveru.
- Služba může také kopírovat vývoj každého dítěte, protože nastavení lze s věkem dítěte upravovat. Cena, dostupnost a kompatibilita Služba OnlineFamily.Norton, která byla dostupná v beta verzi jako Norton Online Family od února 2009, je nyní k dispozici zdarma,

OnlineFamily: jiný pokus o bezpečnější rodinný internet...

a to do 1. ledna 2010. Služba je v angličtině k dispozici na adrese **http://onlinefamily.norton.com** a prozatím poskytuje komplexní filtrování pro severoamerické a kanadské weby. Filtrování je podporováno také pro webové servery v angličtině ve Velké Británii, Irsku, Austrálii, na Novém Zélandu, v Indii a Jižní Africe, ale služba není pro tyto země plně optimalizována.

Komentář redakce: *V poslední době novinkám Symantecu obvykle tleskáme, tentokrát jde ale podle našeho názoru o trefu mimo cíl. Rodičovský filtr obohacený o sledovací modul a doplněný o rodinné posezení na téma „Pojďme si povídat o nebezpečích internetu" možná může mít úspěch v zemi, kde před každým domem visí vlajka s pruhy a kde házejí do moře ochočené kosatky. U nás ale normálním rodičům doporučíme použít balík Internet Security a rozumnou kontrolu dětských internetových aktivit...*

ADOBE READER A ACROBAT

Záškodníci přicházejí v PDF

Pomocí zmanipulovaného PDF souboru dokážou útočníci spouštět na napadených počítačích škodlivý kód s oprávněním správce. Příčinou je chyba při dekódování streamů JBIG2 – ty normálně odpovídají za vnořené grafiky v PDF. K prvním útokům hackeři potřebovali ještě JavaScript, nyní však už „exploit" dále zdokonalili. Teď už uživatel ani nemusí zmanipulovaný soubor spustit, stačí, aby byl soubor uložen na disku.

Na vině je vyhledávací funkce Windows. Ta pevný disk indexuje prostřednictvím služby Windows Indexing, a prohledává tedy i PDF soubory. Aby do nich služba mohla nahlédnout, spouští Adobe PDF-Parser, který pak vyvolá škodlivý kód uvnitř hackerského PDF. Poněvadž volání proběhne s dalekosáhlými systémovými právy indexovací služby, má útočník automaticky administrátorský přístup do PC – nezávisle na tom, jaká práva má aktuálně přihlášený uživatel Windows. Účinnou ochranu proti útokům nabízí sám výrobce – nainstalujte si nové verze 9.1 Readeru a Adobe Acrobatu.

INFO: www.adobe.com

NOVÁ VERZE

Kerio MailServer

Společnost Kerio Technologies vydala novou verzi Kerio MailServeru. Mezi novinky verze 6.7 patří globální adresář (Global Address List – GAL), vylepšené zabezpečení proti spamu a podpora linuxových distribucí Debian a Ubuntu.

Kerio Global Address List (GAL) nabízí způsob, jak přistupovat ke kontaktním informacím kolegů v rámci firmy prostřednictvím klientů, jako je například Microsoft Outlook. Větším společnostem Kerio GAL výrazně zefektivní každodenní práci. Kerio Global Address List je synchronizován s Microsoft Active Directory, Apple Open Directory a lokální databází uživatelů Kerio MailServeru. Antispamový modul je nyní optimalizován pro víceprocesorové systémy a využívá paralelního zpracování e-mailů pro zvýšení propustnosti filtrování. Vícenásobná ochrana proti nevyžádané poště nyní zahrnuje metodu automatického učení bayesiánského filtru, která zásadně zrychluje tvorbu bayesiánské heuristické databáze. Kerio také reaguje na preference uživatelů linuxových distribucí, a tak ke stávajícím Red Hat Enterprise Linux, SuSE Linux a CentOS přidalo podporu pro Debian 5.0 a Ubuntu 8.04 LTS.

INFO: www.kerio.eu

GOOGLE APPS

Každý si počte

V důsledku programátorské chyby ve webové službě Google Apps si interní dokumenty uživatelů může prohlédnout kdokoli. „Bug“ leží ve správě přístupu uvnitř App engine. Dokumenty sdílené uvnitř pracovní skupiny jsou chráněny. Pokud však nějaký uživatel povolí externímu účastníku přístup třeba jen k jedinému souboru, ten tak automaticky získá přístup ke všem ostatním dokumentům skupiny – aniž by se o tom kdokoli cokoli dozvěděl.

Google už stačil zareagovat a během dvou týdnů u všech postižených uživatelů v rámci servisu sdílení zrušil. To teď musí správci systémů pracně opět rekonstruovat ručně. Kdo chce mít absolutní jistotu, že dokumenty nikdo nepovolaný neuvidí, ať si je předem raději uloží na vlastním pevném disku, a ne v těžko kontrolovatelném prostoru „cloud computingu“.

INFO: www.google.com

ZRANITELNOST

PowerPoint v ohrožení

V aplikaci Microsoft PowerPoint byla zjištěna zranitelnost, která kvůli blíže nespecifikované chybě umožňuje přístup k paměti při otevření upraveného souboru pro PowerPoint. Chyba může být zneužita ke spuštění libovolného kódu. Zasažen je Microsoft Office a PowerPoint verze 2000, 2003, 2004 for Mac, XP a Microsoft PowerPoint 2000, 2002 a 2003.

Zmiňovanou záplatu najdete v balíčku oprav, který Microsoft připravil pro květen 2009. Podrobnější informace o problému najdete na webu Microsoft Technet **(www.microsoft.com/technet/security/bulletin/ms09-may.mspx)**.

INFO: zprávy.actinet.cz

EBAY

Zfalšované aukce

Pomocí speciálního HTML kódu dokážou hackeři zmanipulovat aukce a změnit tak číslo nabídky a e mailovou adresu nabízejícího. Útočníci k tomu využívají kombinaci útoku Cross Site Scripting a XBL (XML Binding Language). Tímto způsobem lze navzájem propojit objekty z různých webových stránek.

Ačkoliv dosud není známo, kde přesně se chyba skrývá, eBay už údajně závadu odstranil. To ale ještě nestačí, říkají vývojáři Firefoxu. Šéf vývoje Cefn Hoile se domnívá, že problém je i v chování webových prohlížečů, podotýká však, že na vině není jen samotný browser. Faktem zůstává, že eBay musí přesně kontrolovat, která data přebírá z externích stránek, aby dokázal XSS mezery potlačit už v zárodku.

INFO: www.ebay.com

Nárůst spamu a napadených serverů

Společnost Symantec vydala svou dubnovou zprávu 2009 **MESSAGELABS INTELLIGENCE REPORT**. Analýza upozorňuje, že během jednoho měsíce došlo k nárůstu nevyžádané pošty o téměř 10 %.

Nevyžádaná pošta představuje již 85,3 % všech e-mailů, což je úroveň dosažená naposledy v září 2007. Dubnový ostře sledovaný summit G20 byl příčinou nárůstu cílených útoků škodlivého kódu. Dále se také podstatně zvyšoval počet každodenně zachycených nebezpečených webových serverů. Každý den bylo v průměru zachyceno již 3 561 serverů.

„Obrázková nevyžádaná pošta byla fenoménem, který dosáhl svého vrcholu v roce 2007. Nyní jsme svědky toho, jak tvůrci nevyžádané pošty oživují své techniky v naději, že se bude historie opakovat," řekl Paul Wood, MessageLabs Intelligence Senior Analyst společnosti Symantec. „Naneštěstí pro tvůrce nevyžádané pošty jsou lidé na druhé straně barikády na návrat obrázkové nevyžádané pošty připraveni, takže počítačoví zloději musí podstatně přepracovat své taktiky, pokud chtějí dosáhnout nějakých výsledků."

Mezi obrázkovou nevyžádanou poštu se dříve řadily e-maily obsahující přílohy, například soubory s příponou GIF nebo JPG, ve kterých byl vlastní nevyžádaný obsah. V současné době jsou však tyto obrázky umístěny na „neprůstřelných" hostingových serverech a využívají přesměrovací odkazy z renomovaných webů, pomocí kterých se zastírá jejich skutečné umístění. Tvůrci nevyžádané pošty obcházejí pomocí této techniky filtry nevyžádané pošty, které prověřují domény v odkazech obsažených v e-mailech, vyhodnocují charakter těchto domén a pravděpodobnost, že se jedná o nevyžádanou zprávu.

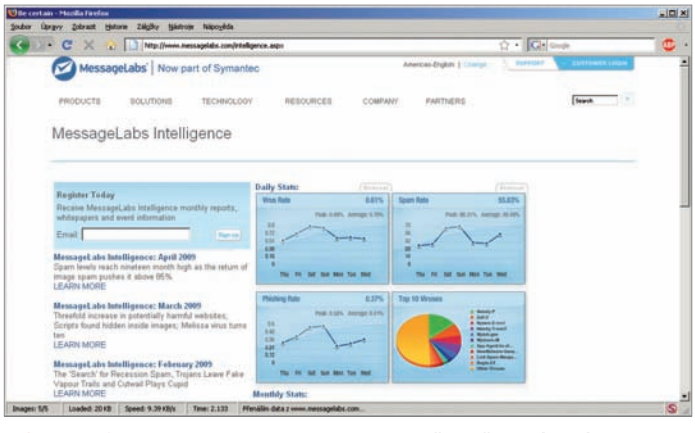
K dalším technikám používaným k zamezení zjištění patří vložení určitého standardního textu do obsahu zprávy, například informací o možnosti odmítnutí dalších zpráv, odkazů na zásady ochrany osobních údajů, jejichž cílem je vytvořit celkové zdání legitimní zprávy, která je v souladu se zákony, například se zákonem CAN-SPAM platným v USA. Dalšími často používanými taktikami jsou vložení náhodných slov do obsahu zprávy za účelem obejití technik zjištění pomocí otisků zpráv a použití značek jazyka HTML k ukrytí náhodného textu.

Summit G20 byl předmětem intenzivní pozornosti médií na celém světě a v posledních dvou měsících také důvodem nárůstu cílených útoků škodlivého kódu – ty dosáhly nejvyšší intenzity počátkem dubna. V roce 2008 docházelo v průměru přibližně k 53 útokům denně a v prvním čtvrtletí roku 2009 vzrostl počet těchto útoků asi na 60 denně. V období těsně před summitem G20, který se konal 2. dubna v Londýně, a v následujících dnech se počet cílených útoků zvýšil až na přibližně 100 denně.

Cílem těchto útoků byly finanční organizace včetně jednotlivců z některých centrálních bank zemí náležejících do skupiny G20. E-mail obsahoval přílohu PDF, která by po otevření způsobila nainstalování a spuštění trojského stahovacího programu. Ten by do cílového počítače následně stáhl další spywarové součásti. Bylo pozorováno, že některé útoky byly reakcí na neškodné e-maily, z čehož plyne, že nejméně jeden z příjemců byl již infikován.

Neustále se také zvyšuje počet nebezpečných webových serverů. V dubnových statistikách je dobře patrný nárůst o 27,3 %, což znamená, že každý den je v průměru zablokováno 3 561 nových nebezpečných webových serverů. Původcem je řada hrozeb, mezi jinými automatické stahování trojských koní z webu, trojské koně skryté v souborech PDF, škodlivý kód vydávaný za soubory GIF, které jsou ve skutečnosti spustitelnými soubory, a nebezpečné značky HTML IFRAME. Poslední uvedená hrozba je většinou důsledkem narušení webového serveru útokem využívajícím techniku SQL injection, která je s oblibou používána k útokům na jinak legitimní „slušné" domény. Dalším virníkem je software maskovaný do podoby legitimně vyhlížejících aplikací, k nimž se řadí podvodný software pro ochranu před škodlivým kódem.

INFO: www.messagelabs.com/intelligence.aspx.



Zajímavosti: Na webu MessageLabs najde kromě zmiňované zprávy i celou řadu zajímavých informací...

STATISTIKA ESET THREATSENSE.NET

Napadené počítače rozesílají spam

Podle pravidelných měsíčních statistik globálně nejrozšířenějších počítačových hrozeb systému Eset ThreatSense.Net byl i v dubnu největší hrozbou červ Win32/Conficker, který nakazil téměř desetinu počítačů.

Kromě útoků vedených za účelem získání citlivých dat se tvůrci infiltrací stále častěji zaměřují na šíření škodlivých kódů, pomocí kterých po napadení počítače vytvoří na dálku ovládanou velkou síť infikovaných počítačů (tzv. botnetů). Tyto sítě jsou následně využívány k rozesílání nevyžádané pošty (spamu). Na druhém místě za Confickerem se v dubnu umístil INF/Autorun – tak Eset označuje směs hrozeb (nejčastěji trojských koní) šířících se přes vyměnitelná média. Vysoký podíl mezi počítačovými infiltracemi měl v dubnu také Win32/PSW.OnLineGames (7,01 %), snažící se odcizit hlavně přístupové údaje k účtům hráčů populárních on-line počítačových her. První pětku infiltrací uzavírá Win32/Agent a rodina trojských koní Win32/TrojanDownloader, která často slouží útočníkům k rozesílání spamu. Do této rodiny patří široká paleta infiltrací s převahou Win32/TrojanDownloader.Wigon a Win32/TrojanDownloader.Swizzor. Všeobecně jsou tyto hrozby spojené se stahováním a instalováním infikovaných komponent na počítač uživatele.

Nejčastější hrozby v Evropě

Střední Evropa byla v dubnu pod palbou jednoho z členů rodiny Win32/TrojanDownloader. Varianta trojského koně Win32/TrojanDownloader.Wigon byla top hrozbou na Slovensku (5,58 %), v České republice (8,51 %) a v Maďarsku (6,14 %). Dlouhodobě se v ČR šíří velké množství nevyžádané pošty (adware), která zahlcuje a zpomaluje počítače uživatelů.

Ve východní Evropě dosáhl největšího podílu červ Conficker. Zatímco ve Finsku představoval podíl nebezpečného červa 8,80 %, v Rumunsku to bylo 10,24 %, v Rusku 18,47 %, a na Ukrajině dokonce 24,63 %.

SMART SURFING FOR MAC

Volný a bezpečný pohyb pro Mac OS X

Společnost Trend Micro ohlásila nový produkt, který pomůže uživatelům na platformě Mac s libovolným prohlížečem bezpečně surfovat po webu a bez obav používat odkazy v e-mailu i systémech rychlého zasílání zpráv a být neustále chráněni před internetovými útoky. Trend Smart Surfing for Mac nabízí antimalware a ochranu před webovými hrozbami

Ať už spotřebitelé používají jakýkoli operační systém, potřebují ochranu před internetovými útoky a krádežemi identity. Technologie společnosti Trend Micro pro obranu před malwarem a ochranu před webovými hrozbami chrání identitu a osobní data uživatelů při nákupech, práci s internetovým bankovnictvím i při surfování on-line. Tyto technologie blokují odkazy na nebezpečné webové servery, jak v e-mailu, tak v systémech rychlého zasílání zpráv.

Díky nástroji Trend Smart Surfing for Mac jsou uživatelé na platformě Mac chráněni před internetovými podvody, které se z nich snaží vymámit důvěrné informace, i před nechtěným nainstalováním nebezpečného softwaru.

„Rodičovská kontrola“ pomáhá chránit děti na internetu. Funkce rodičovské kontroly umožňuje rodičům vybrat webové servery, které chtějí zablokovat, a tak chránit děti před nevhodným obsahem, aniž by jim bránili ve využívání všeho, co jim internet může nabídnout.

INFO

Nová bezpečnostní rizika

MOZILA THUNDERBIRD

Sun oznámil chyby v softwaru Mozila Thunderbird verze 2.0.0.19 a dřívějších, dodávaných se systémem Solaris 10. Zranitelnosti mohou být zneužity k obcházení bezpečnostních opatření, mohou zapříčinit únik citlivých informací, dovolují provedení cross-site scripting útoků a kompromitaci zranitelného systému. Řešením je použití záplaty 125541-04, kterou spolu s bližšími informacemi naleznete na stránkách společnosti Sun **(http://sunsolve.sun.com/search/document.do?assetkey=1-66-258748-1)**

INFO: zprávy.actinet.cz

JAVASCRIPT ZRANITELNOSTI ADOBE READER A ACROBAT

Společnost Adobe informovala o dvou zranitelnostech, které mohou být zneužity k útokům přes JavaScript z upraveného PDF souboru a které umožňují spuštění libovolného kódu. Napadnutelné jsou pravděpodobně všechny verze. 12. května by měly být uvolněny updaty na verze 9.X, 8.X a 7.X pro Windows, 9.X a 8.X pro Unix i Macintosh. Mezitím Adobe doporučuje zakázat spouštění JavaScriptu. Zranitelnost zatím pravděpodobně není zneužívána. Podle analýzy provedené společnosti Qualys po odhalení poslední podobné zranitelnosti v únoru potrvá dlouhou dobu, než uživatelé nainstalují opravné patche. Dají se očekávat pokusy o zneužití zranitelnosti. Více informací naleznete v oznámení výrobce na **www.adobe.com/support/security/advisories/apsa09-02.html**.

INFO: zprávy.actinet.cz

ESET SMART SECURITY

Nenáročný strážce

Slovenská firma Eset patří v oblasti počítačové bezpečnosti mezi stálice, a tak nás nepřekvapilo, že neuplynul ani rok a my jsme mohli opět otestovat její bezpečnostní balík Smart Security, tentokrát již označený číslem 4.

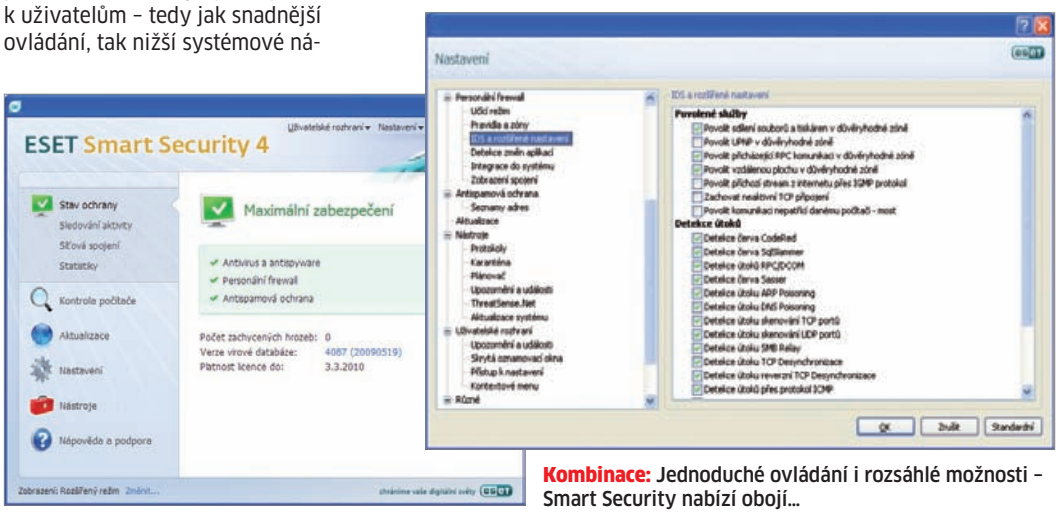
Novinka by měla nabídnout především vstřícnější přístup k uživatelům – tedy jak snadnější ovládání, tak nižší systémové nároky. My můžeme potvrdit, že těchto cílů bylo jednoznačně dosaženo. Ovládání celého balíku je skutečně jednoduché a zvládne ho i naprostý začátečník. Lehce rozporuplné dojmy však máme ze systémových nároků – program zabere v paměti více než 50 MB, což je ve srovnání s konkurencí minimálně dvojnásobek. Pravda ovšem je, že ani na nejpomalejším počítači v redakci nebyla instalace ESS4 téměř znát a práci brzdil tento nástroj pouze zanedbatelně. Jen v superlativech lze mluvit o rychlosti skenování – na testovacím počítači byl program minimálně o třetinu rychlejší než u srovnatelné konkurence.

Z hlediska ovládání lze také ocenit, že Eset skryl pokročilé funkce za volbu „Rozšířený režim“. Začátečníci nejsou stresováni velkým množství voleb a zkušenější uživatelé ocení rozsáhlé možnosti konfigurace. Snad nejvíce je to znát u firewallu, který nyní dokáže také kontrolovat šifrovanou komunikaci (SSL, HTTPS, POP3S) i komprimované soubory.

Za příjemnou novinku lze označit nástroj SysRescue, pomocí něhož lze vytvářet záchranná DVD a USB disky.

Antispamový modul podporuje čtyři nejrozšířenější programy (Microsoft Outlook, Mozilla Thunderbird, Windows Mail a Windows Live Mail) a nabízí také rychlejší antispamový filtr. Další novinkou je ochrana před vypnutím (což je oblíbená taktika celé řady škůdců).

A co se nám nelíbilo? Ve srovnání s konkurencí chybí bezpečnostnímu balíku několik „modulů“. Absenci antiphishingového nástroje lze omluvit (obvykle stačí ten, který je integrován v browseru), mrzela nás ale chybějící rodičovská kontrola a upozorňování na nebezpečné weby. Pokud pro vás nejsou zmiňované výtky důležité, lze program jen doporučit – nízké systémové nároky a snadné ovládání z něj dělají jasného favorita především pro méně zkušené uživatele.



Kombinace: Jednoduché ovládání i rozsáhlé možnosti – Smart Security nabízí obojí…

LOGICA

Platforma pro auto nové generace

Firma Logica představila internetovou platformu pro spojení dopravních specialistů, návrhářů a dalších odborníků, kteří pracují na návrhu zeleného vozu budoucnosti. Účastníci se zapojují do virtuálních diskusí na platformě Online Collaboration Platform (OCP), vyvinuté společností Logica.

Tato platforma spojuje velké množství specialistů z různých disciplín ve strukturované diskusi o produktech a službách souvisejících s vozem c,mm,n a pomáhá prezentovat jednotlivé nápady a náměty ve snadno pochopitelné podobě. To přispěje k obohacení a urychlení celého procesu navrhování.

Prototyp vozu c,mm,n byl prezentován na automobilovém veletrhu v Amsterdamu. Projekt byl iniciován holandskou ekologickou organizací Stichting Natuur en Milieu a sponzorován společnostmi Logica, Athlon Car Lease a Rabobank. Vývoje vozu se účastní technické univerzity Delft, Eindhoven a Twente a poradenská firma DHV.

INFO: www.logica.com

VERBATIM SSD EXPRESSCARD

Rychlejší než USB, kapacita až 64 GB

Firma Verbatim Europe u nás začala prodávat ExpressCard SSD kartu pro uživatele notebooků. SSD (Solid State Drive) karta nabízí uživatelům PC s XP/Vista i uživatelům Mac OS X přídavnou paměť, která je až pětinásobně rychlejší než USB flash disky nebo externí disky (klasické nebo SSD) připojené přes pomalejší rozhraní USB. Verbatim ExpressCard SSD je založena na 34mm ExpressCard modulu (75 mm × 34 mm × 5 mm) a v obchodech je k dostání v kapacitách 16, 32 a 64 GB, a to za 2 149 Kč, 3 799 Kč a 6 999 Kč. Rychlost čtení je až 120 MB/s (800×), rychlost zápisu až 30 MB/s (200×). Karta ExpressCard SSD podporuje funkci Windows ReadyBoost ve Windows Vista. Karta se ve slotu také snadno přenáší. Disky se dodávají společně se zálohovací aplikací Nero BackitUp 4 Essentials. Recenzi karty přineseme v příštím čísle.

INFO: www.verbatim-europe.cz

NOVINKA NA AUKRO.CZ

Vlastní e-shop na aukčním portálu

On-line aukční portál Aukro.cz zavádí pro své uživatele zcela novou službu – Aukro Shopy. Prodávající si mohou jednoduše vytvořit vlastní „virtuální obchod“ s jedinečnou subdoménou, prodávat předměty pod svou unikátní značkou, za pevné ceny a ve více kategoriích najednou. Kromě zásadního zefektivnění správy prodeje předmětů umožňuje tato novinka také podstatné prodloužení doby vystavení předmětů na 30 dnů a výhodné snížení poplatků za jejich vystavení. Službu mohou také využít maloobchodníci, kteří nemají vlastní e-shop nebo kteří hledají další prodejní kanál na internetu. Založení a aktivace služby je snadná. Stačí mít alespoň deset pozitivních komentářů v transakční historii, v rámci Aukra si otevřít vlastní jedinečnou subdoménu, která se bude vztahovat pouze k jednomu „virtuálnímu obchodu“, zvolit si jméno a případně i logo Shopu, a pak už jen začít vystavovat. Aukro Shopy jsou měsíčně zpoplatněny 70 korunami. Za první měsíc provozování vlastního Shopu zaplatí uživatelé Aukru pouhých 15 korun. Dalším poplatkem je pak provize z úspěšného prodeje. Po prvním týdnu od spuštění této nové služby si uživatelé aukčního portálu „otevřeli“ bezmála pětistovku e-shopů.