MALWAROVÁ EPIDEMIE „ITALIAN JOB"

Matka Tereza a Jon Bon Jovi zneužiti…

K pokusu o zcizení osobních informací došlo na konci června v Itálii. Několik útočníků se pokusilo napadnout tisíce oblíbených italských stránek, přičemž k útkou zneužili známou a běžnou zranitelnost IFRAME. Velké množství malwaru však útočilo i na nic netušící uživatele webu po celém světě.

Napadené webové stránky mají nejrůznější témata – automobily, automobilové závody, hotely, sport, hudbu, loterie a pornografii. Nedotčeny nezůstaly ani stránky o Jon Bon Jovim a Matce Tereze.

Rozsáhlý útok

„V posledních 48 hodinách bylo tímto způsobem „uneseno" více než 2000 italských webových stránek, přičemž každých šest až osm hodin docházelo ke zdvojnásobení počtu obětí," uvedl Ivan Macalintal, odborník na internetové hrozby z laboratoří TrendLabs společnosti Trend Micro. „Tyto webové útoky byly skryté a pro nechráněného spotřebitele neviditelné – tudíž nebezpečnější než běžné viry. Aby se útočníci vyhnuli identifikaci a zvýšili účinnost svého útoku, využívají více různých druhů malwaru, například keylogger pro získání osobních informací o bankovních účtech nebo heslech." „Nejnovější útok ukazuje, jak se trh s malwarem mění a jak účinnými se webové hrozby stávají," komentuje událost Anthony O'Mara, viceprezident Trend Micro pro oblast EMEA.

Autor nebo autoři tohoto posledního útoku strávili jeho plánováním pravděpodobně celé měsíce. Regionální záběr útoku a rychlost, s jakou k infekci webových stránek došlo, ukazuje na kriminální gang, jehož cílem byl zisk.

Jak to funguje?

Mechanismy šíření nákazy tvoří komplexní řetězec, závisí však na tom, že majitelé webových stránek si nejsou vědomi toho, že jejich stránky jsou narušeny, a na tom, že uživatelé surfující po těchto zdánlivě korektních stránkách se mohou stát součástí infekčního procesu:

1 URL „první úrovně" jsou narušené nebo hacknuté webové stránky. Zde jde především o italské weby nabízející místní turistické, hotelové, servisní, hudební či sázkařské služby.

2 Tyto webové stránky byly „upraveny" a do jejich HTML kódu byla zavedena škodlivá IP adresa (HTML_IFRAME.CU), takže uživatelé budou přesměrováni na jinou stránku s javascriptovým stahovačem (JS_DLOADER.NTI). To jsou URL adresy druhé a třetí úrovně.

3 Tato třetí úroveň URL adres stáhne do cílového systému dalšího trojského koně ze čtvrté úrovně URL – TROJ_SMALL.HCK.

4 Trojský kůň pak stáhne další dva trojské koně z různých URL adres páté úrovně. Jde o URL pro TROJ_AGENT.UHL a TROJ_PAKES.NC. Poté, co uživatel navštíví kteroukoli z uvedených webových stránek, je nakažený počítač přesměrován na jinou IP adresu, která obsahuje škodlivý JavaScript, který společnost Trend Micro detekovala jako JS_DLOADER.NTJ. Tento JavaScript poté stáhne novou součást infekční série detekovanou jako TROJ_SMALL.HCK. JS_DLOADER.NTJ se snaží způsobit přetečení bufferu uživatelského internetového prohlížeče a využít jeho zranitelnosti. Jejich prostřednictvím je schopen stáhnout TROJ_SMALL.HCK. Při prvních testech zjistili odborníci TrendLabs, že tento škodlivý JavaScript se snaží využít zranitelnost daného typu a verze prohlížeče.

TROJ_SMALL.HCK poté stáhne TROJ_AGENT.UHL a TROJ_PAKES.NC. TROJ_AGENT.UHL může sloužit jako proxy server, který umožní vzdálenému uživateli anonymní připojení k internetu přes nakažený počítač. Naproti tomu TROJ_PAKES.NC je uložen do dočasného adresáře a odesílá informace získané keyloggerem TSPY_SINOWAL.BJ.

ITÁLIE: Už nejen anglicky mluvící uživatelé se musí na internetu bát…

Buďte ostražití

Tento útok přesně zapadá do výsledků analýz, které v Chipu pravidelně zveřejňujeme: internetový zločin už není záležitostí „bavících se studentů" nebo „zneuznaných géniů". V současné době jde už jen a pouze o jediné: o peníze. Italská kauza by měla být velkou výstrahou i pro uživatele v České republice, protože šlo o cílený útok na menší, neanglicky mluvící zemi. To naznačuje, že do budoucna nás proti podobným útokům nemusí „ochránit" ani náš libozvučný rodný jazyk…

DOPORUČENÍ PRO UŽIVATELE:

- Buďte opatrní na stránkách, které vyžadují instalaci nějakého softwaru. Nedovolte instalaci nového softwaru z prohlížeče kromě případů, kdy stoprocentně důvěřujete webové stránce nebo poskytovateli softwaru.
- Aktualizovaným antivirovým a antispywarovým programem prohlížejte jakýkoli program stažený z internetu. Platí to pro stahování ze sítí P2P, přes web i přes jakýkoli FTP server bez ohledu na zdroj.
- Dejte si pozor na neočekávané a podivně vypadající e-maily bez ohledu na to, kdo vám je poslal. Nikdy neotevírejte přílohy ani neklikejte na odkazy obsažené v takovém e-mailu.
- Vždy mějte spuštěný antivirový program pracující v reálném čase. Pravidelně sledujte jeho aktualizace a to, že je v provozu.
- Využívejte bezplatné bezpečnostní nástroje; najdete je například na adrese **www.trendmicro.com**.

DOPORUČENÍ PRO FIRMY:

- Užívejte metody pro skenování provozu HTTP. Vzhledem k tomu, že webové hrozby začínají převažovat nad ostatními, lze středním a velkým podnikům doporučit implementaci systémů pro skenování webu.
- Nedovolte, aby se do podnikové sítě dostaly nežádoucí protokoly. Nejnebezpečnější z nich jsou komunikační protokoly P2P a IRC (chat), které patří do arzenálů zbraní botů pro šíření malwaru a komunikaci se svým botmasterem.
- Zaveďte do sítě software pro sledování zranitelností. Tím, že budete udržovat své operační systémy stále aktuální, minimalizujete dopad síťové zranitelnosti a snižujete rizika nakažení těmito druhy červů. Také doporučujeme kontrolovat záplaty i u kancelářských aplikací.
- Omezte uživatelská privilegia všech uživatelů sítě. Rootkity běžící na úrovni kernelu jsou obvykle prezentovány jako ovladače zařízení, čehož lze využít. Pokud zakážete uživatelům „natažení a odstranění ovladačů zařízení", můžete snížit riziko této hrozby. Windows Vista tuto „situaci" díky svým bezpečnostním funkcím dokonce zcela znemožňují. Další malware zneužívá možnosti dané administrátorskému účtu. Doporučujeme omezit možnosti nebezpečných programů i tím, že mu omezíte jeho privilegia: uživatelům znemožněte přihlašovat se jako administrátoři.
- Používejte podnikové antispywarové programy. Vzhledem k tomu, že spyware patří mezi významné druhy podnikových hrozeb, doporučujeme nasadit specifický software, pro lepší rozpoznání a eliminaci.
- Provádějte školení zaměstnanců o potenciálních hrozbách. Většina dnešních útoků využívá malware, který se snaží uživatele obelstít. Většina malwaru zachyceného během roku 2006 nijak nepoškodila prostředí počítače, dokud na něj uživatel „neklikl". Doporučujeme naučit uživatele základním způsobům zabezpečení a reakci na typické scénáře útoků. Je důležité, aby uživatelé znali nové strategie útočníků a aby noví uživatelé stačili držet krok s bezpečnostní politikou a doporučeními společnosti.

Zdroj: Trend Micro Incorporated

ANTIVIROVÝ SYSTÉM AVG

Antivir pro mobilní telefony

Grisoft ohlásil rozšíření nabídky bezpečnostních aplikací o produkt AVG Mobile Security. Ten slouží k ochraně mobilních telefonů na platformě Symbian UIQ 3.0. Systém pracuje na přístrojích Sony Ericsson P990i, M600i a W950i a obsahuje antivir s antispamem SMS zpráv, tedy ochranu proti nevyžádaným sdělením především reklamního typu.

„Produktem AVG Mobile Security vstupujeme do segmentu mobilních platforem," uvedl technický ředitel společnosti Karel Obluk. Aktualizaci softwaru zajišťuje systém distribuce s více než 10 000 servery ve světě a s velmi rychlou reakcí na případný výskyt nových hrozeb. Veřejná beta verze AVG Mobile Security je zájemcům k dispozici na webových stránkách společnosti po přihlášení do beta portálu. Zde mohou také získávat zkušenosti z testování či se o ně podělit s ostatními uživateli.

Podle zveřejněných výzkumů se počet virových útoků na mobilní telefony loni zpětinásobil a bezpečnostní incidenty zasáhly zákazníky více než 80 procent světových mobilních operátorů. Terčem úspěšného útoku se staly tisíce přístrojů. Viry mohou například vyřadit tyto přístroje z provozu nebo zvýšit telefonní účty pomocí nechtěných zpráv a hovorů. Podle odhadů existuje asi 350 virů, červů a dalšího škodlivého kódu pro mobilní telefony.

ZRANITELNÉ PROGRAMY

Nová bezpečnostní rizika

ZONEALARM

Chyba v programu

Mezera v jádru Spyware Removal 5.0.63.0 umožňuje uživatelům s omezenými právy přisvojit si práva správce. Postižen je nejen freeware ZoneAlarm, ale i komerční produkty. Řešení je poměrně snadné: výrobce už chybu odstranil a update je k dispozici.
Info: www.zonelabs.com

WLAN

Prolomený WEP

Díky dalšímu vylepšení algoritmu se darmstadtským vědcům podařilo prolomit 128bitový WEP klíč za méně než 60 sekund. Významně mohl být snížen i počet potřebných paketů. Odpovědí je rychlý a bezpodmínečný přechod na WPA nebo WPA2.
Info: www.tu-darmstadt.de

ANTIVIR

Nebezpečný mail

V domněle potvrzovacím mailu od Aviry se skrývá stahovač. Je-li spuštěna příloha maskovaná jako setup, downloader stáhne do počítače „Browser Helper Object" pro Internet Explorer. Plug-in však svou oběť špehuje. Zde lze jen doporučit zásadně ignorovat neznámé přílohy.
Info: www.avira.de

MPLAYER

Přetečení bufferu

V oblíbeném multimediálním přehrávači Mplayer (verze 1.0rc1 a starší) bylo nalezeno několik zranitelností typu buffer overflow. Tyto zranitelnosti se objeví při zpracování zákeřně upravených hudebních alb a názvů kategorií. Útočníkovi pak postačí, aby pomocí sociálního inženýrství dostal uživatele na svůj server; tam mu může podstrčit takto upravené mediální soubory a získá tím kompletní kontrolu nad jeho počítačem. Pro řešení situace existuje záplata, ale vydání nové opravené verze se zatím neplánuje. Více informací o chybě se dočtete na **www.mplayerhq.hu**.
Info: zpravy.actinet.cz

WINDOWS

Opět kurzory

Bezpečnostní mezera v souborech animovaných kurzorů ANI přidělala Microsoftu další starosti. Až druhá aktualizace má přinést definitivní nápravu. První update mj. způsoboval havárie softwaru jako Elster. Naštěstí je však již k dispozici záplata pod názvem KB935448.
Info: www.microsoft.com

MYSQL

Obcházení nastavení

V databázi MySQL verze dřívější než 5.0.42 a 5.1.19 byly nalezeny dvě nové zranitelnosti, které mohou vést k obejití bezpečnostního nastavení a k nahrání libovolných knihoven (viz **http://bugs.mysql.com/**). První případ se týká nesprávně ošetřených uživatelských práv při použití příkazu VIEW a ve druhém případě jde o nesprávné ošetření cest ke knihovnám, což může útočník zneužít a nahrát libovolnou vlastní knihovnu. Opravené verze jsou již k dispozici na stránkách výrobce.
Info: zpravy.actinet.cz

SYMANTEC REPORTING SERVER

Navýšení přístupových práv

Symantec zveřejnil aktualizovanou verzi Reporting Serveru 1.0.224.0. Opraveny byly chyby, které umožňovaly vzdálenému útočníkovi odhalit heslo administrátora aplikace nebo získat vyšší přístupová práva.
Info: zpravy.actinet.cz

REALPLAYER A HELIXPLAYER

Vzdálené spuštění kódu

Na počátku července byla objevena zranitelnost v produktech RealPlayer (verze 10.x) a HelixPlayer (verze 1.x) společnosti RealNetworks. Zranitelnost dovoluje vzdálenému útočníkovi shodit aplikaci a/nebo spustit na cílovém stroji libovolný kód (**http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=547**). Jde o chybu typu „přetečení bufferu", která vznikne při zpracování souboru SMIL (Synchronized Multimedia Integration Language). Výrobce již na svých stránkách zveřejnil opravené verze.
Info: zprávy.actinet.cz

MICROSOFT

Záplaty na červenec

Microsoft zveřejnil na svých stránkách podpory bulletiny s informacemi o důležitých aktualizacích pro podporované verze svých aplikací. (**www.microsoft.com/technet/security/bulletin/ms07-jul.mspx**).

STUDIE SPOLEČNOSTI MCAFEE

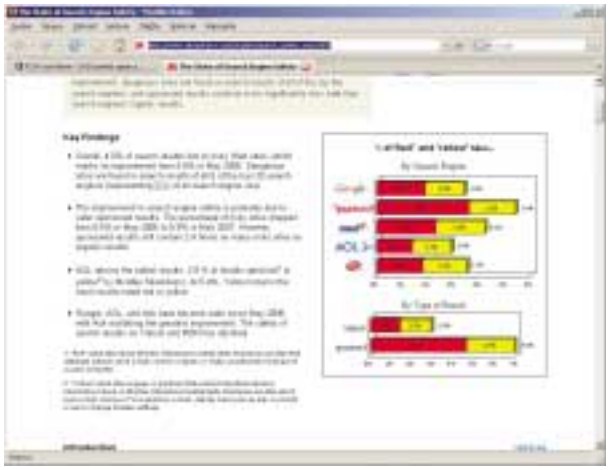
Bezpečnost vyhledávačů

Rok po vydání své první studie mapující bezpečnost vyhledávačů zveřejnila společnost McAfee aktualizovanou verzi analýzy The State of Search Engine Safety (Situace v oblasti zabezpečení vyhledávacích služeb). Aktuální výsledky ukazují, že ačkoliv celkový podíl potenciálně rizikových odkazů ve výsledcích vyhledávacích služeb poklesl na hodnotu okolo 1 procenta, sponzorované odkazy (tj. odkazy, jejichž zveřejnění je placeno inzerentem) jsou výrazně rizikovější než výsledky „regulérního" vyhledávání. Společnost McAfee celkově odhaduje, že jen americkým uživatelům internetu je každý měsíc předloženo 276 milionů výsledků vyhledávání, které odkazují na stránky ohrožující on-line zabezpečení.

Studie společnosti McAfee zahrnula pět hlavních vyhledávacích nástrojů používaných v USA – Google, Yahoo!, MSN, AOL a Ask. Základem studie byla analýza prvních 50 odkazů, které vyhledávač vracel jako odpověď. V rámci studie bylo zadáno 2300 běžných klíčových slov a frází, které byly vybrány ze seznamů typu Google Zeitgeist (žebříček nejvyhledávanějších slov na vyhledávači Google), Yahoo! Buzz a dalších oborových zdrojů. Každý výsledek byl porovnán s databází nástroje McAfee SiteAdvisor, který obsahuje hodnocení více než 8,2 milionu serverů z hlediska jejich bezpečnosti pro uživatele. V rámci tohoto hodnocení je červená barva přiřazena rizikovým serverům, které obsahují adware, spyware či viry, provádějí pokusy o zneužití zranitelností, jsou spojeny se zasíláním nevyžádané pošty, zobrazují nepřiměřeně agresivní okna typu pop-up nebo jsou silně provázány s dalšími servery spadajícími do této kategorie. Žlutá barva je přiřazena serverům, při jejichž používání je doporučována jistá obezřetnost. Spoluautorem studie je Ben Edelman, odborník na spyware, který spolupracuje na službě McAfee SiteAdvisor jako poradce.

Mezi klíčová zjištění studie patří:

- Až 4 procenta výsledků vyhledávání obsahovalo odkaz na nějaký rizikový web.
- Služba America Online vrací nejbezpečnější výsledky vyhledávání. Pouze 2,9 procenta odkazů vede na servery označené aplikací McAfee SiteAdvisor červeně nebo žlutě. Ještě před rokem přitom u AOL činilo zastoupení rizikových odkazů ve výsledcích vyhledávání 5,3 procenta. Naopak nejvíce rizikových („červených" nebo „žlutých") odkazů vrací Yahoo – 5,4 procenta.
- Sponzorované odkazy směřují na rizikové servery až 2,4krát častěji než výsledky „regulérního" vyhledávání. Celých 6,9 procenta veškerých sponzorovaných odkazů označuje aplikace McAfee →



PODROBNOSTI: Komplexních analýzu najdete na webu McAfee.

IBM INTERNET SECURITY SYSTEMS

Útoky prostřednictvím dokumentů

V posledním roce sleduje divize IBM Internet Security Systems nový trend v oblasti vytváření malwaru. Tvůrci škodlivých kódů přišli na to, jak vložit nebezpečný kód do neškodně vypadajícího dokumentu. Ohroženy jsou například dokumenty Microsoft Office a dokumenty pdf. Pokud si vzpomínáte, tak asi před 10 lety bylo běžné, že viry byly připojeny k dokumentům Office pomocí maker. Když se pak ale antivirové programy naučily identifikovat makra, tento druh ohrožení byl silně potlačen.

Nová technika je ale jiná. Současní tvůrci škodlivého kódu vsadí do dokumentu takzvaný „shell code", který je pro většinu dnešních antivirových programů neviditelný. Tyto kódy jsou typicky programované tak, aby poskytly kriminálníkům vzdálený přístup do počítačů obětí a umožnily tak například krádeže identit, e-špionáž či přeměnu PC uživatele na tzv. zombie.

PHISHING: Nebezpečí i pro Ministerstvo obrany Spojených států amerických.

Problém spočívá mimo jiné v tom, že běžní uživatelé jsou ostražití vůči souborům s neznámými koncovkami, ale klasickým souborům typu .doc, .xls, .pdf a .ppt důvěřují. Proto má tato taktika tak vysokou úroveň „infekčnosti". Stejná technika byla použita při phishingovém útoku, který se objevil na Ministerstvu obrany Spojených států amerických (www.fcw.com/article97186-12-26-06-Web). Proto je dnes, stejně jako před 10 lety, nutno upozorňovat uživatele na nebezpečí běžných souborů. V minulosti to byla makra, dnes jsou to „shell code".

→ SiteAdvisor červeně nebo žlutě. I toto číslo však představuje zlepšení oproti situaci před rokem, kdy rizikových sponzorovaných odkazů bylo 8,5 procenta. Hlavní zásluhu na tomto zlepšení mají inovace Googlu (seznamy sponzorovaných odkazů Googlu se navíc zčásti zobrazují i na stránkách AOL a Ask).

▶ Největší rizika i nadále představuje vyhledávání slov spadajících do oblasti digitální hudby a technologií. Fráze „digital music" vedla k vrácení výsledků, mezi nimiž bylo až 19,1 procenta odkazů na rizikové servery. Následovaly fráze „tech toys" (technické hračky) a populární klíčová slova jako „chat" a „wallpaper".

▶ Mezi nejrizikovější klíčová slova také patří programy pro sdílení souborů. Nebezpečné jsou výsledky vyhledávání systémů pro sdílení souborů Bearshare (45,9 procenta rizikových výsledků), Limewire (37,1 procenta), Kazaa (34,9 procenta) a Winmix (32 procenta).

▶ V seznamech sponzorovaných odkazů je celých 3,2 procenta odkazů směřujících na podvodné servery. Typický podvodný server nabízí v tomto případě prodej softwaru, který je jinak distribuován zdarma, může se také jednat o stránky obsahující zavádějící informace o účtování volání na určitá telefonní čísla nebo o neprofesionálně vytvořený server obsahující klamavé informace.

▶ Ve výsledcích vyhledávání, které se týká „obsahu pro dospělé" (erotický obsah), se podíl rizikových serverů od konce loňského roku zvýšil o 17,5 procenta. Rizikové odkazy nyní představují 9,4 procenta veškerých výsledků vyhledávání v této kategorii. Ve sponzorovaných odkazech, které se zobrazí při vyhledávání „obsahu pro dospělé", přitom procento rizikových odkazů vzrostlo o celých 72 procent.

Zpráva The State of Search Engine Safety obsahuje další podrobné informace včetně komplexních analýz výsledků „regulérního" vyhledávání a sponzorovaných odkazů. Celá studie společnosti McAfee mapující bezpečnost vyhledávačů je k dispozici na webu **www.siteadvisor.com/studies/search_safety_may2007**.

ZAJÍMAVÉ WWW STRÁNKY

Neztraťte svá data

Společnost McAfee spustila spolu se svým distributorem, společností DNS, na počátku července nové webové stránky věnované úniku informací (Data Loss Prevention). Na stránkách **www.ochranadat.com** najdou především firmy informace, jak zabránit nepříjemným situacím zapříčiněným ztrátou informací či důvěrných údajů.

DNS a firma McAfee připravují i šňůru odborných bezplatných seminářů, na které se mohou zájemci na těchto stránkách zaregistrovat. Stránky také nabízejí konzultační služby: pomocí formuláře uvedeného na stránkách můžete zaslat odborníkům z DNS a McAfee svůj dotaz a ti vám ho během krátké doby zodpoví.

Stránky **www.ochranadat.com** se věnují popisu situace, která může nastat a ohrozit chod firmy, ale také nabízí návod, jak takové situaci zabránit. Spuštění stránek předcházel průzkum na toto téma, který před nedávnou dobou firma McAfee zveřejnila. Ten ukazuje, že v globálu je únik dat pomocí e-mailu, dokumentů či přenosných zařízení problém, kterému firmy ve většině případů ještě neumí zabránit.

STUDIE TREND MICRO

Hrozby včera a dnes

Společnost Trend Micro Incorporated zveřejnila výsledky studie týkající se rozdílů mezi tím, jak koncoví uživatelé v podnicích vnímali bezpečnostní hrozby v roce 2005 a letos. Studie vyhodnotila odpovědi 1200 koncových podnikových uživatelů v USA, Spojeném království, Německu a Japonsku a porovnala je s analýzou provedenou globální výzkumnou sítí Trend Micro TrendLabs v roce 2005.

Jak výsledky průzkumu ukazují, mezi lety 2005 a 2007 došlo k nárůstu spamu, letos však překvapivě méně koncových podnikových uživatelů ve Spojených státech uvádělo, že dostali spam. Respondenti ze Spojeného království v roce 2007 všeobecně považovali bezpečnostní hrozby za méně závažné než v roce 2005. Naproti tomu němečtí respondenti považují v roce 2007 všechny hrozby za závažnější než v roce 2005.

Podle průzkumu hrozeb provedeného TrendLabs vzrostl počet digitálních hrozeb mezi prosincem 2005 a listopadem 2006 o 163 procent. U webových hrozeb došlo mezi lednem 2005 a lednem 2007 k nárůstu o 540 procent. Koncoví uživatelé si však závažnost hrozeb příliš nepřipouštějí, pravděpodobně kvůli tomu, že mnoho nových infekcí probíhá nepozorovaně.

Zajímavé výsledky ukazuje i průzkum týkající se spywaru. Procento respondentů, kteří se setkali se spywarem, poklesl ve Spojených státech (z 41 procent v roce 2005 na 35 procent v roce 2007), v Německu (z 23 procent v roce 2005 na 19 procent v roce 2007), ale zejména ve Spojeném království (ze 42 procent v roce 2005 na 26 procent v roce 2007). Příčinou poklesu spywaru je podobně jako u spamu zvýšená komplexita a propracovanost útoků a to, že uživatelé obtížněji detekují nový škodlivý kód, který se instaluje nepozorovaně.

Vzhledem k rostoucímu počtu a náročnosti spamových a phishingových útoků doporučuje Trend Micro pokračovat v nepřetržitém vzdělávání podnikových koncových uživatelů. Kromě toho, že spamové a phishingové útoky uživatele obtěžují, často obsahují odkazy na stránky obsahující škodlivý zdrojový kód, například spyware. Infekce touto cestou znamenají vážnou hrozbu pro osobní i podnikové informace.

I když si koncoví uživatelé v některých zemích uvědomují vážnost hrozeb, jsou také mnohem ochotnější podstupovat riziko a na podnikových počítačích otevírají podezřelé dokumenty nebo klikají na podezřelé odkazy. Pravděpodobně spoléhají na dostupnost a odpovědnost týmů technické podpory a cítí se méně osobně odpovědní za bezpečnostní pravidla a praktiky v práci.

EVROPA: Nechybí ani podrobné údaje z většiny zemí...

Další informace týkající se bezpečnostních hrozeb, všeobecné bezpečnosti internetu, dat dostupných v reálném čase a malwarového blogu Trend Micro naleznete v Trend Micro Threat Resource Center na adrese **http://itw.trendmicro.com**. Tento nový centrální informační zdroj využívá výsledky zpravodajství o hrozbách v reálném čase, které shromažďuje TrendLabs, globální organizace Trend Micro pro výzkum a podporu. Trend Micro Threat Resource Center nabízí širokou škálu dynamicky se měnících informací o hrozbách a pomáhá návštěvníkům držet krok s výskytem nejnovějších hrozeb, mít přehled o vývoji hrozeb a souvisejících technologií a o doporučených postupech k ochraně před nimi.

BUĎTE V OBRAZE: Threat Resource Center nabízí komplexní informace o hrozbách z internetu.

PERLIČKY Z PRŮZKUMU:

- Uživatelé ze Spojených států mají všeobecně mnohem větší důvěru v ochranu poskytovanou firemními počítači. Okolo 40 procent jich totiž uvedlo, že jejich pracovní počítače jsou lépe chráněny před spamem, spywarem a phishingem než jejich počítače domácí. Výsledkem je, že na svých pracovních počítačích ve větší míře klikají na podezřelé odkazy (17 procent), zejména ve srovnání se svými německými protějšky (8 procent).
- 48 procent všech respondentů, kteří se stali obětí spywaru nebo phisingu, věří, že jejich IT oddělení mohlo incidentu zabránit.
- Mezi největší obavy týkající se ohrožení počítače patří odcizení identity, ztráta osobních informací a porušení soukromí. O něco méně se uživatelé obávají spamu; virů a trojských koní se týkají ztráty výkonnosti počítače nebo zhoršení produktivity.
- Japonští koncoví uživatelé se nejvíce ze všech spoléhají na jejich IT oddělení. V posledních třech měsících před průzkumem se jich celých 44 procent obrátilo na své IT oddělení. Nejméně na tento útvar spoléhají američtí koncoví uživatelé, kteří u něj v témže období hledali radu a podporu pouze ve 24 procentech.
- Američtí uživatelé jsou zejména ve srovnání s britskými uživateli mnohem více ochotni brát bezpečnostní hrozby vážně. Příkladem může být studie, která udává, že 60 procent amerických respondentů považuje spyware za vážnou hrozbu, zatímco u britských respondentů je tomu tak pouze ve 48 procentech. Podobně 48 procent amerických koncových uživatelů rozpoznává nebezpečí spamu, zatímco pouze 27 procent britských uživatelů jej vnímá jako nebezpečnou hrozbu.

STATISTIKA ÚTOKŮ

Potřetí vítězem

Již třetí měsíc po sobě se na vrcholu statistiky ESET ThreatSense.NET drží exploit Win32/TrojanDownloader.Ani.Gen, který v červnu zaznamenal podíl 3,95 %. Jak již bylo několikrát zmíněno, exploit napadá počítače s operačním systémem Windows, a to od verze Microsoft Windows 2000 SP4 až po nová Windows Vista, a zneužívá soubory s příponou ANI. Nepřestává se šířit, přestože Microsoft vydal bezpečnostní záplatu již na konci března. Na vině jsou neaktualizované počítače hlavně domácích uživatelů, kteří si bezpečnostní záplatu nestáhli nebo kteří používají nelegálně získaný operační systém a stahování záplat mají z toho důvodu raději neaktivní. ESET ThreatSense.NET získává data od 10 milionů dobrovolných uživatelů z celého světa a je tak nejpřesnější statistikou svého druhu.

Na druhém místě v žebříčku najdete infiltraci Win32/BHO.G, která dosáhla 2,41 % z celkových červnových detekcí. Tato infiltrace se na napadeném počítači nainstaluje jako Browser Helper Object v prohlížeči Internet Explorer a monitoruje vše, co uživatel přes tento prohlížeč udělá. Získává tak seznam navštívených webových stránek a hesla zadávaná při přihlašování k e-mailu nebo internetovému bankovnictví.

Na třetí místo se za měsíc „propracoval" červ Win32/Rjump.A. Tato infiltrace se šíří hlavně prostřednictvím externích zařízení, jako jsou USB flash disky, externí pevné disky nebo paměťové karty, a po napadení počítače umožňuje útočníkům vzdáleně přistupovat do systému uživatele. Od minulého měsíce se Win32/Rjump.A posunul o dvě místa dopředu a zaznamenal podíl 2,26 %. V první pětce je ještě Win32/Spy.VBStat.J (1,99 %), který monitoruje aktivity napadeného počítače a zobrazuje nevyžádaná reklamní pop-up (vyskakovací) okna, a INF/Autorun (1,83 %), což jsou různé rodiny červů, které vždy podobným způsobem infikují soubory typu autorun.ini (typicky se šíří prostřednictvím USB klíčů), aby zajistily své spuštění a následné napadení počítače.

TOP 10 infiltrací – červen 2007

	Virová hrozba	Podíl na celkovém počtu infiltrací
1.	Win32/TrojanDownloader.Ani.Gen	3,95 %
2.	Win32/BHO.G	2,41 %
3.	Win32/Rjump.A	2,26 %
4.	Win32/Spy.VBStat.J	1,99 %
5.	INF/Autorun	1,83 %
6.	Win32/Pacex.Gen	1,56 %
7.	Win32/Adware.Virtumonde	1,47 %
8.	Win32/Netsky.Q	1,22 %
9.	Win32/PSW.QQRob	1,00 %
10.	Win32/Rootkit.Vanti.EE	0,88 %