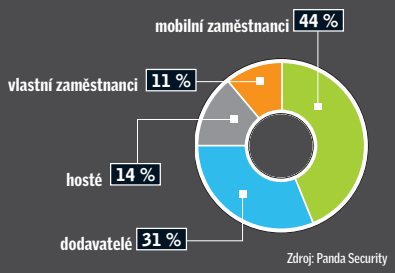
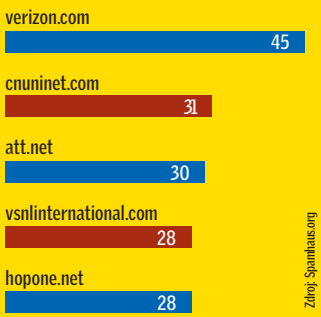
Barometr nebezpečí

Útoky na firmy



Viry nebo hacking: Za největší nebezpečí pro podnikové sítě považují firmy své zaměstnance.

Hlavní šiřitelé spamu



* počet hlášených případů na poskytovatele v milionech

Největší americký poskytovatel Verizon má ve své klientele mnoho spammerů, nic proti nim ale nepodniká.

BEZPEČNOSTNÍ WEB CHIPU

www.chip.cz

Na našich webových stránkách také naleznete aktuální bezpečnostní zpravodajství

Obrovská síť botů ohrožuje internet

Pozor na zdánlivě veselé e-maily! Provozovatelé celosvětově největší sítě robotů nyní přišli s novým a zvláště podlým spamovým útokem. Pomocí e-mailů, jejichž předmět přitahuje hláškami jako „I've never laughed so hard!", se snaží nalákat své oběti na webovou stránku „The Laughing Psycho Kitty Cat". Tam návštěvníka uvítá kočka, které autoři prostřednictvím grafického editoru propůjčili rozesmátý výraz. Stačí však kliknout na kterýkoli z odkazů na stránce, a hned se začne do počítače stahovat soubor „SuperLaugh.exe". Za ním se ovšem neskrývají žádné další „kočičiny", nýbrž bot Zhelatin. Ten pak svou oběť začlení do největšího uskupení botů na světě – sítě Storm-Worm.

Nezranitelná: Síť botů už nelze zastavit

Kolik počítačů už je postiženo, nelze přesně říci. Zatímco někteří bezpečnostní experti odhadují rozsah sítě botů na 50 milionů infikovaných PC, číslo mezi jedním a pěti miliony se zdá mnohem realističtější. I tak je tato síť stále ještě asi stokrát větší než většina jí podobných a disponuje větším výpočetním výkonem než nejsilnější superpočítač. Hlavní důvod, proč se obří síť zotročených počítačů dosud nepodařilo zničit, spočívá především ve skutečnosti, že jednotliví „nevolníci" už vzájemně nekomunikují přes centrální „velín", nýbrž prostřednictvím spojení typu peer to peer. Takto organizovaní členové pak, podobně jako filesharingová komunita eDonkey, pracují s protokolem Overnet: dojde-li k odstranění nějakého uzlu sítě, společenství se uzdraví samo – mezeru zaplní nový bot.

NEBEZPEČNÁ ZÁBAVA: **Za touto rozmarnou webovou stránkou se skrývá bot toho času největší sítě na světě.**

Průkopník: Storm-Worm inspiruje další zločince

Až dosud pochází většina obětí sítě Storm-Worm z anglofonní oblasti. Je to pochopitelně dáno způsobem, jakým provozovatelé této sítě lákají své oběti. Výhradně v angličtině psané e-maily jsou tematicky zaměřeny téměř vždy na občany USA. Předměty spamových zpráv se tak vztahují k americkým svátečním dnům nebo velkým sportovním událostem. Tento trik funguje tak dobře, že už se bezpečnostní experti obávají jeho brzkého napodobení, které by pak podobné útoky rozšířilo i do dalších jazykových prostorů. Anebo sám Storm-Worm dále zvětší svůj akční rádius a nakonec překoná i onen padesátimilionový odhad.

Info: www.cyber-ta.org

ESET PRO LINUX

Nové bezpečnostní produkty

Společnost Eset vydala v listopadu tři nová linuxová řešení pro firemní zákazníky. Eset Gateway Security, Eset File Security a Eset Mail Security jsou založeny na skenovacím jádru Eset NOD32 Antivirus. Všechny tyto nové produkty ochrany pro servery Linux/FreeBSD mají implementovánu technologii ThreatSense, a to se všemi funkcemi pro detekci virů, trojských koní, červů, rootkitů, spywaru, adwaru a dalších typů infiltrací. Nové produkty charakterizuje také centrální webová administrace a plně inkrementální a automatická aktualizace virové databáze za chodu, včetně aktualizace zdokonalené technologie ThreatSense.Net pro zasílání podezřelých souborů na analýzu.

Info: www.eset.cz

ZPRÁVA IBM X-FORCE

Heslo za tabulku čokolády?

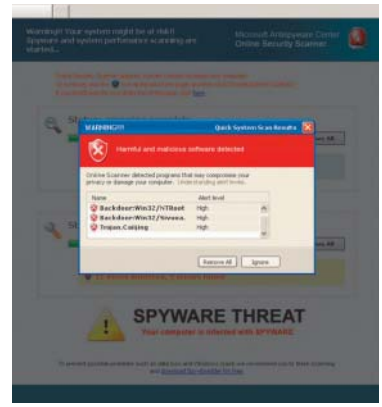
Téměř každý dnes používá několik různých přihlašovacích a přístupových hesel. Hesla potřebujeme pro přístup ke svému firemnímu počítači, pro přístup ke svému účtu v bance nebo pro přístup na oblíbené webové stránky. Jakou hodnotu má však takové heslo? Na to neexistuje jednoznačná odpověď. V roce 2004 odhalil výzkum na jednom z nejrušnějších vlakových nádraží ve Velké Británii, že 70 procent lidí by prozradilo své heslo do počítače za tabulku čokolády. A co když vám teď řeknu, že dnes má vaše přístupové heslo k počítači hodnotu méně než 4 centy? Většina lidí má určitou představu o tom, jakou hodnotu mají údaje o kreditních či platebních kartách (číslo karty, údaje na magnetickém pásku, PIN), a dokážou také odhadnout cenu informací potřebných pro přístup k účtu prostřednictvím online bankovnictví. Málokdo však už dokáže ocenit hodnotu hesel, se kterými pracuje každý den.

Pro ilustraci, balík 7000 přihlašovacích jmen, hesel a e-mailových účtů se dá najít a zakoupit přes internet za 250 USD. Popis tohoto balíku říká, že pocházejí ze známé pornostránky. Jenže proč by si někdo kupoval 7000 loginů na pornostránku, když dokáže získat přístup za 20 USD měsíčně? Proto, že nejde o přístup k této pornostránce, ale o možnost proniknout do jiných webových stránek uživatelů, jejichž údaje jsou obsaženy v balíku. Podobných balíků se v temných zákoutích internetu dá nalézt neskutečně mnoho. Liší se jen obsahem a typem dat, která obsahují, a samozřejmě cenou. Více informací najdete v nejnovějším blogu Guntera Ollmanna, ředitele bezpečnostních strategií v IBM ISS, na adrese **http://blogs.iss.net/archive/PasswordValue.html.**

ROGUE ANTISPYWARE

Falešná stránka Microsoftu

Bezpečnostní iniciativy Microsoftu mají i své stinné stránky: jméno softwarového gigantu nyní zneužívá trojský kůň k nalezení nových obětí. Aby podvod vypadal pokud možno věrohodně, hackeři dokonce na internetu zřídili falešný „Microsoft Antispyware Center". Návštěvníkům stránky je tam předstíráno provedení okamžité bezpečnostní kontroly – která samozřejmě zjistí vysoce riziková ohrožení. Nic netušící uživatelé, kteří pak kliknou na „Remove All", tím spustí download souboru „setup.exe". To ovšem není žádný instalační soubor bezpečnostního nástroje Microsoftu, ale speciální stahovač. Jakmile je spuštěn, změní tento diverzant různé položky systémového registru, mezi nimi i bezpečnostní nastavení Internet Exploreru. Poté stahovač zavede vlastního trojského koně, který se nainstaluje do složky



C:\Windows\System32. Program pak funguje jako odchytávač hesel a navíc bombarduje plochu uživatele vyskakovacími reklamními okny. Nebezpečná stránka je sice stále ještě na internetu, ale téměř všechny virové skenery s aktuálními signaturami už trojského koně poznají a jeho instalaci zabrání.

Info: www.f-secure.com

IBM X-FORCE

Hrozby pro rok 2008

Vždy na konci roku zveřejňuje společnost McAfee předpověď nejvážnějších bezpečnostních hrozeb pro následující rok. Ani letos tomu není jinak.

Oči hackerů se upírají na aplikace Web 2.0

Na webech Salesforce.com, Monster.com a MySpace a na dalších serverech spadajících mezi aplikace typu Web 2.0 se jako nový trend objevuje škodlivý kód a dochází ke kompromitaci uživatelských dat. Útočníci se stále častěji zaměřují na tzv. sociální sítě. Narušitelé sledují informace, které zde uživatelé sdílejí, aby tak jejich následné útoky mohly působit věrohodněji. Odborníci z laboratoří McAfee Avert Labs předpokládají, že tyto aktivity útočníků v příštím roce dále vzrostou.

Botnety ve stopách červů

V roce 2007 došlo k nárůstu policejního a soudního stíhání tvůrců a šiřitelů programů typu bot. Útočníci se proto budou zaměřovat na jiné metody. Varovným precedentem byl případ červa Storm Worm, známého také pod názvem Nuwar. Červ Storm Worm zatím ze všech kódů, které byly v historii zaznamenány, prokázal největší variabilitu. Tvůrce vypustil červa v tisících variantách, měnil programovací techniky, metody infekce i postupy sociálního inženýrství. Červ Storm tak dokázal vytvořit dosud největší síť navzájem přímo propojených počítačů. Laboratoře McAfee Avert Labs předpovídají, že úspěch tohoto červa přiměje další útočníky, aby se pokusili vytvořit podobné sítě typu botnet.

Instant Messaging

Obavy z červů šířících se prostřednictvím aplikací instant messagingu existují již několik let. Taková hrozba by během několika sekund dokázala jako blesk zasáhnout miliony uživatelů po celém světě. Škodlivý kód šířící se přes nástroje IM se již objevil, zatím jsme se ale nesetkali s hrozbami, které by se dokázaly samy spustit. Takový okamžik však může být blíže, než si myslíme. Známé zranitelnosti v oblíbených IM aplikacích vzrostly v roce 2007 ve srovnání s předcházejícím rokem více než dvojnásobně. Co je však ještě důležitější, v roce 2007 se objevilo deset bezpečnostních hrozeb, které byly klasifikovány jako velmi závažné – loni do této kategorie přitom nespadala ani jedna. V letech 2005 a 2006 se prostřednictvím aplikací IM šířily nejpoužívanější viry, tato situace se ale mění – v roce 2007 se v aplikaci Skype již rozšířili první červi. Předpokládá se, že tento trend bude pokračovat.

Zacíleno na on-line hry

Hrozby „virtuálním ekonomikám" rostou podobně jako hrozby ekonomikám reálným. Se zvyšující se hodnotou virtuálních objektů vyjádřenou v reálných penězích se stále více útočníků snaží těchto statků zmocnit a zpeněžit je. Doklady o tomto trendu se objevily již letos. Například počet trojských koní (programy zaměřující se na krádeže hesel), které se snažily zmocnit přihlašovacích údajů k on-line hrám, rostl v roce 2007 rychleji než počet trojských koní zaměřených na bankovní účty.

Rodina operačních systémů se rozšířila o Windows Vista

V roce 2008 bude systém Windows Vista nasazen na velkém množství počítačů a jeho podíl na trhu překoná 10 %. Přijetí nejnovějšího systému společnosti Microsoft bude mj. urychleno vydáním balíčku Service Pack 1 pro Windows Vista. Spolu s rozšířením tohoto systému mu zvýšenou pozornost začnou věnovat i hackeři a tvůrci škodlivého kódu, kteří se zaměří na způsoby, jimiž půjde ochranu Windows Vista obejít. Od vydání systému bylo zatím letos ohlášeno 19 zranitelností. Předpokládáme, že v roce 2008 tento počet výrazně stoupne.

Pokles adwaru pokračuje

V některých státech byly proti šíření softwaru, který uživateli masivně doručoval reklamu, podniknuty právní kroky. Pokles adwaru začal v roce 2006 jednak v důsledku nové legislativy, jednak vzhledem k lepší obraně i negativním reakcím, které tato forma reklamy vyvolávala. Největší hráči na tomto poli v roce 2007 od tohoto způsobu reklamy upustili a trend poklesu adwaru bude pokračovat i v následujícím roce.

Phishing rozšíří svůj záběr

Kybernetičtí podvodníci se stále častěji zaměřují na menší, méně známé servery. Nejznámější servery a firmy s celosvětově známými značkami dokáží na snahy o krádeže a zneužití údajů obvykle rychle reagovat a zvýšit zabezpečení. Pro podvodníky jsou podobné útoky stále obtížnější a riskantnější. Zaměření zlodějů informací na méně známé servery je usnadněno i tím, že řada lidí používá pro účty v různých službách stejné uživatelské jméno i heslo.

Parazitický kód zapouští kořeny

Parazitický kriminální kód (crimeware) směřující k obohacení svých tvůrců postupně vytlačoval ostatní malware a počítačové viry. V loňském roce několik útočníků použilo k doručení crimewaru do počítačů opět klasických virů, které měnily soubory na disku a vkládaly do nich příslušný kód. Jako nové hrozby se loni objevily viry Grum, Virut a Almanahe. Množství variant starší hrozby Philis vzrostlo

KOMPLETNÍ ZABEZPEČENÍ

Trend Micro Mobile Security

Společnost Trend Micro Incorporated představila nejnovější verzi svého řešení pro zabezpečení mobilních zařízení, která se na trh dostane v prosinci. Řešení Trend Micro Mobile Security (TMMS) 5.0 je vybaveno funkcemi pro šifrování dat a autentizaci: pokud se mobilní zařízení ztratí nebo je odcizeno, uložená data důležitá pro chod podniku jsou zašifrována a dá se k nim přistupovat pouze přes heslo. Data v zařízeních, která neodpovídají bezpečnostním zásadám, mohou být administrátory vymazána. Antimalwarový software blokuje viry, červy, trojské koně a spam zasílaný přes SMS. Vestavěný firewall a systém pro zjišťování průniků IDS (Intrusion Detection System) chrání před průniky hackerů nebo útoky DOS (denial-of-service) – což jsou všechno potenciální hrozby pro mobilní zařízení.

Trend Micro Mobile Security 5.0 Standard zahrnuje antivirus, firewall, Intrusion Detection System a centralizovanou správu. Trend Micro Mobile Security 5.0 Advanced má navíc funkce pro šifrování dat a autentizaci. Ceny TMMS 5.0 začínají na 35 USD. Info: **www.trendmicro.cz**

o 400 procent, zcela nová hrozba jménem Fujacks byla zaznamenána v celkem 400 verzích. Celkové množství parazitického malwaru vzroste v příštím roce odhadem o 20 %.

Virtualizace mění informační bezpečnost

Dodavatelé řešení zabezpečení jsou pomocí virtualizace schopni vytvořit pružnější ochranu proti hrozbám. Současné hrozby lze ve virtualizovaném prostředí snadněji zastavit, ale profesionální hackeři a autoři škodlivých kódů samozřejmě nespí na vavřínech. Budou hledat cesty, jak novou technologii zabezpečení obejít, a souboj s nimi bude i nadále pokračovat.

Útoky proti VoIP vzrostou o 50 procent

V letošním roce byl oproti roku 2006 zaznamenán více než dvojnásobek bezpečnostních zranitelností, které se týkaly aplikací přenosu hlasu přes internet (VoIP). Zaznamenáno bylo rovněž několik útoků spadajících do kategorie vishing (podvodné vyzvídání citlivých údajů) a phreaking (útoky proti telekomunikačním systémům). Neexistuje žádná známka toho, že by se růst hrozeb proti VoIP měl zpomalit. Technologie VoIP je stále relativně nová a vývoj bezpečnostních řešení má za jejím nástupem zpoždění. Laboratoře McAfee Avert Labs proto předpokládají 50 % nárůst těchto bezpečnostních hrozeb v příštím roce.

Další informace o jednotlivých hrozbách, jejich hodnocení a nezkreslené výsledky výzkumů v oblasti bezpečnosti IT naleznete na blogu McAfee Avert Labs Security na adrese **www.avertlabs.com/research/blog/.**

Nová bezpečnostní rizika

WINAMP

Kopie oblíbeného softwaru pro přehrávání médií s číslem verze nižším než 5.5 lze podle vyjádření bezpečnostní firmy iDefense „kreknout" prostřednictvím speciálně upraveného odkazu. Znamená to, že útočník může v napadeném počítači spouštět škodlivý kód. Řešením je aktualizace na nejnovější verzi přehrávače.
Info: **www.winamp.com**

KASPERSKY SCANNER

Slabé místo ActiveX modulu v on-line skeneru od firmy Kaspersky umožňuje hackerům propašovat do počítače libovolný program. Příčinou problému je zranitelnost formátovacích řetězců v mnoha funkcích. Bezpečnostní aktualizace je k dispozici na webové stránce firmy Kaspersky.
Info: **www.kaspersky.com**

OFFICE

Aktualizace s číslem MS07-060 uzavírá podle tvrzení Microsoftu kritickou bezpečnostní mezeru ve Wordu. Tato slabina umožňuje útočníkům prostřednictvím preparovaného dokumentu dostat do počítače záškodnický kód a získat tak kontrolu nad PC. Doporučujeme nahrát aktuální aktualizaci a zříci se oprávnění správce.
Info: **www.microsoft.com**

INTERNET EXPLORER

Další aktualizací uzavírá Microsoft ve svém internetovém prohlížeči hned čtyři mezery. Blíže nepopsané chyby umožňují pomocí speciálně vytvořené webové stránky získat kontrolu nad browserem i nad Windows. Opět doporučujeme bezpodmínečně nahrát aktuální update!
Info: **www.microsoft.com**