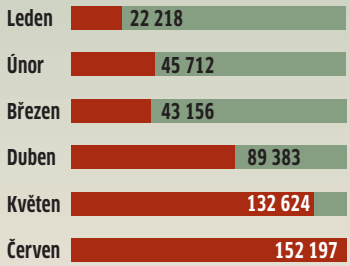
DATA A FAKTA

Barometr nebezpečí
v listopadu:

Hackeři využívají především mezery ve Windows 7, neboť mnozí uživatelé si dosud nenainstalovali antivirový program.

Falešný antispyware

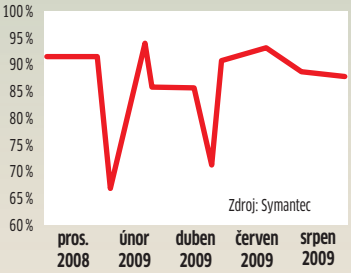


Zdroj: Antiphishing.org

Nárůst: Počet falešných antispywarových programů silně roste. Tyto nástroje stále častěji provádějí i špionáž v počítačích.

Trendy spamu

Podíl spamu v mailech



Zlomy: Po dopadení velkých spammerů kolabuje reklamní síť vždy jen dočasně. Normální stav představuje 90 % spamu v celém mailovém provozu.

Číslo měsíce

220

milionů eur je hodnota všech ukradených dat, která jsou v současné době k dispozici na internetovém černém trhu.

Velký útok na mailová hesla

Prostřednictvím zfalšovaných přihlašovacích stránek a certifikátů vniknou hackeři do vaší mailové schránky. Prozradíme vám, jak se proti novým **PHISHINGOVÝM TRIKŮM** bránit.

FABIAN VON KEUDELL

Používáte bezplatnou mailovou službu jako Yahoo, Hotmail nebo Google Mail? Pak by si hackeři mohli vaše maily rovnou přečíst. Při velkoryse koncipované akci pronikli internetoví zločinci do více než 30 000 účtů různých poštovních služeb a jejich přihlašovací údaje zpřístupnili on-line. Tato data si hackeři opatřili pomocí speciálních phishingových útoků: na různé mailové adresy rozeslali zprávu, která uživatele varovala, že s jejich poštovní schránkou je něco v nepořádku. Ti pak měli, jako třeba u Hotmailu, své přihlašovací údaje „verifikovat“ na stránce mailového serveru, k nerozeznání podobné originálu. Pokud tam uživatel svá data zadal, odeslal je hackerovi.

Doposud bylo možné rozpoznat falešné webové stránky podle chybějícího šifrování a nesprávného certifikátu, ale oba tyto příznaky už vychytralí hackeři dokážou zmanipulovat: vložením nulového znaku do Common Name certifikátu dosáhnou toho, že zranitelné browsery čtou znakový řetězec jen po dosažení tohoto znaku, ačkoliv je certifikát vlastně vystaven pro jinou doménu. Browser v takovém případě uvěří, že rozpoznal platný certifikát například pro **www.hotmail.com**. Mezera je známa už mnoho týdnů – u různých prohlížečů. Z těch nejznámějších dosud trik odhalily jen Firefox a Opera a uživatele varují dříve, než svá data domnělému hotmailovému serveru odešle. Microsoft chce Internet Explorer opravit záplatou, kterou právě vyvíjí.

Fatální je, že jakmile jednou hackeři získají přístup k mailovému účtu, mohou podle uložených zpráv poznat, ve kterých internetových obchodech oběť nakupuje. Přístupová data k těmto obchodům si útočníci nechají poslat na „kreknutý“ účet a pak mohou utrácet peníze jménem postiženého. Poté své stopy vymazáním mailového účtu zahladí – jeho obnovení pak už často není možné.

Kontrola a ochrana: Čtyři nejdůležitější okamžitá opatření

Zda byla vaše mailová schránka vyšpehována, můžete snadno zjistit na stránce **http://server-sniff.de**. Služba má přístup k databance s více než 40 000 položkami. Abyste se ale obětí takových útoků vůbec nestali, používejte bezpečná hesla a k procházení internetu Operu nebo Firefox. Maily, jejichž odesílatele neznáte, byste měli bez čtení rovnou vymazat. Zodpovídat bezpečnostní dotazy mailových služeb nemusí být právě snadné. Trik: Pište odpověď pozpátku nebo vkládejte zvláštní znaky.
INFO: www.hotmail.com

Hledání obětí: Na webové stránce ServerSniff můžete zkontrolovat, zda už je vaše e-mailová adresa včetně hesla veřejně přístupná na internetu.

SYMANTEC

DoS útoky pomocí e-mailu

Bezpečnostní souprava Internet Security Suite výrobce Symantec se stala obětí hackerského útoku. Prostřednictvím speciální e-mailové zprávy dokážou útočníci ochromit kontrolní mechanismus programu a znesnadnit tak rozpoznání škodlivého softwaru. Postiženy jsou produkty Symantecu Norton 360, Norton AntiVirus, Norton Confidential, Norton Internet Security a Endpoint Protection. Chybu neodhalil sám Symantec, nýbrž bezpečnostní experti firmy Next Generation Security Software. Ti poukazují na útok typu DoS (Denial of Service), který je zacílen speciálně na mailový skener produktů Symantecu. Jakmile skener na dotyčný mail narazí, nezkontroluje jej jen jednou, ale dostane se do nekonečné smyčky, v níž zprávu skenuje stále znovu a znovu. To má za následek timeout mailserveru, neboť PC přestane reagovat na požadavky připojení. Postižení uživatelé by měli skener deaktivovat, následně zprávu vymazat a poté virový štít opět zapnout.
INFO: www.symantec.com

ADOBE READER

Nová mezera

V programu Adobe PDF Reader byla objevena další bezpečnostní mezera, která útočníkům umožňuje propašovat do počítače škodlivý kód. Postiženy jsou verze 9.1.3 Adobe Reader i Adobe Acrobat. Pro tuto chybu dosud od výrobce bohužel neexistuje záplata. Chyba se projevuje v browserovém doplňku Readeru. Uživatelé by proto ve svých počítačích měli deaktivovat JavaScript, radí Adobe. Podle informací Chipu mohou útočníci využitím přetečení bufferu nahrát do postiženého počítače hackerské programy. Je proto vhodné nainstalovat si alternativní čtečku PDF, například bezplatný Foxit Reader, který si můžete stáhnout z adresy **www.foxitsoftware.com**. Ten je proti speciálně na produkty Adobe zaměřeným útokům imunní. Adobe chce tuto mezeru zacelit při příští aktualizaci.
INFO: www.adobe.com

HROZBA

SSL/TLS zranitelnost

V SSL byla nalezena kritická zranitelnost, která útočníkům umožňuje vložit se do zabezpečené SSL komunikace standardním „man-in-the-middle“ útokem. Webové stránky využívající SSL jsou zranitelné: jedná se např. o internetové bankovnictví, back-office systémy, které využívají webové služby, dále aplikace jako mailové a databázové servery, ale i webové stránky, které využívají certifikáty klientů. Marsh Roy a Steve Dispenda, zaměstnanci společnosti PhoneFactor, objevili bezpečnostní díru v SSL protokolu a na konci října informovali společnosti, jejichž produktů se týká. Zástupci PhoneFactor, IETF (Internet Engineering Task Force) a organizace ICASI (Industry Consortium for the Advancement of Security on the Internet) vytvořili pracovní skupinu, která sdružuje společnosti Microsoft, Intel, Nokia, IBM, Cisco, Juniper, Open SSL, Apache, NSS, Red Hat a Leviathan Security Group. Zranitelnost neměla být zveřejněna do začátku roku 2010, aby měli výrobci softwaru dost času na opravu, ale 4. listopadu byla nezávisle objevena při diskusi pracovní skupiny IETF TLS a zprávy o zranitelnosti se začaly rychle šířit IT security komunitou. Původní oznámení naleznete na **www.phonefactor.com/sslgap/**.
INFO: zpravy.actinet.cz

INFO

Nová bezpečnostní rizika

MICROSOFT LIVE MESSENGER

Využitím chyby v knihovně ATL mohou útočníci nahrát do počítače škodlivý kód. Postiženy jsou verze 8.1, 8.5 a 14.0. Kdo si nenahrál aktualizace, od konce října se už nemůže k Messengeru přihlásit. Aktualizace je již k dispozici.
INFO: www.microsoft.com

OPENOFFICE

Slabé místo v bezplatném kancelářském balíku firmy Sun může vést k „heap overflows“ a umožnit tak hackerům přístup do počítače. Řešením je aktualizace. Ve verzi 3.1.1 je mezera uzavřena a bylo odstraněno i několik menších chyb.
INFO: http://www.openoffice.org

APPLE QUICKTIME

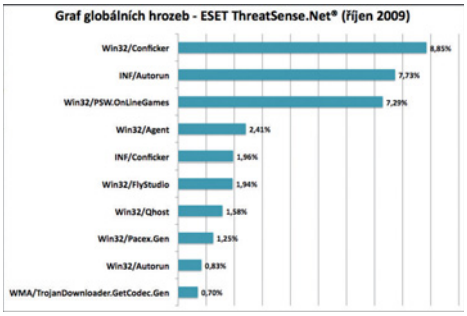
Ve verzi Quicktime pro Windows byly zjištěny čtyři kritické chyby, jejichž využitím mohou hackeři infikovat počítač. Stačí k tomu zmanipulovaný videosoubor ve formátu H.264. I zde je řešením aktualizace, protože verze 10.5.8. zmiňované chyby odstraňuje; najdete ji na webové stránce výrobce.
INFO: www.apple.com

INTERNET EXPLORER 6 A 7

Browsery obsahují chybu, kvůli které je lze donutit přistupovat k CSS objektům i poté, co byly odstraněny. Na základě toho mohou útočníci vytvořit stránky, které shodí prohlížeč a dovolí spuštění libovolného kódu. Podle Microsoftu není zranitelnost zneužívána, ale kód, který chybu využívá, je znám a dosud neexistuje patch, který by chybu opravil. Podle dalšího vývoje bude patch k dispozici v rámci pravidelných měsíčních záplat. Není znám ani žádný postup, který by zamezil zneužívání zranitelnosti při používání Internet Exploreru. Microsoft doporučuje aktualizovat veškerý software, nainstalovat antivirový a antispywarový software a používat firewall.
INFO: zpravy.actinet.cz

STATISTIKA FIRMY ESET

Na Čechy útočí falešné antiviry



Mezi uživateli v Česku byla v říjnu nejrozšířenější virová hrozba Win32/Kryptik, což je označení pro infiltraci zahrnující skupinu podvodných aplikací včetně falešných antivirů, (16 % ze všech zachycených hrozeb v ČR). Vyplývá to ze statistiky Eset ThreatSense.Net, která obsahuje informace o typu a počtech škodlivých kódů zachycených na počítačích uživatelů.

Falešné antiviry jsou oblíbeným nástrojem kyberzločinců. Nelegální skupiny, které se pohybují v šedé zóně internetu, stále lépe graficky napodobují antiviry předních výrobců, matou uživatele podobnými názvy a inkasují tisíce dolarů od nachytaných nešťastníků. Kryptik zaznamenal vysoký podíl také v Rakousku (26,46 %), Německu (17,39 %), Švédsku (13,55 %) a Velké Británii (12,92 %). Z globálního hlediska je nerozšířenější stále Conficker.

Jak funguje proces oklamání uživatele: Po infikování počítače škodlivým kódem je uživatel obtěžován vyskakovacími okny a smyšlenými informacemi o napadení počítače. Jako řešení problému je nabízen antivirový program, který odstraní všechny nalezené hrozby. Tyto hrozby však na počítači nejsou. Pokud uživatel zaplatí požadovanou částku (až 2 000 Kč), získá bezcenný program, který počítač ve skutečnosti vůbec nechrání. Falešný antivirus například nalezne stovky hrozeb i na zcela novém počítači, který nemá připojena žádná vyměnitelná média, není v síti a ani není připojen k internetu.

Celosvětově však stále virové oblasti vládne Conficker, který dosáhl podílu 8,85 % ze všech zachycených počítačových hrozeb. Ani situace na dalších místech v první pětce se od předchozího měsíce nezměnila. INF/Autorun, jak Eset označuje směs hlavně trojských koní zneužívajících funkci autorun.inf v OS Windows, byl na druhém místě s podílem 7,73 %, třetí místo patří trojským koním útočícím na data a majetek hráčů online her – Win32/PSW.OnLineGames (7,29 %). Pětku nejrozšířenějších světových hrozeb uzavírá rodina Win32/Agent, vykrádající data z počítačů uživatelů, a INF/Conficker, jak Eset označuje varianty Confickeru zneužívající autorun.inf.

WINDOWS

Hromadná záplata

Celkem 34 bezpečnostních mezer, postiženy všechny produkty – přichází možná největší „patch-day“ v historii Microsoftu. Softwarový gigant z Redmondu zaceluje od Windows 2000 přes Windows 7 až po Internet Explorer a Office kritické mezery, jimiž mohly do počítačů pronikat záškodnické programy. Většinu slabin hodnotí Microsoft jako kritické mezery. Poprvé od poloviny října je do aktualizace zahrnut i zbrusu nový systém Windows 7: tím je uzavřena mezera v implementaci SMB2 síťového protokolu Windows. V případě Internet Exploreru jde o tři vstupní brány, například zranitelný ATL-ActiveX, jimiž mohou útočníci nahrávat škodlivé programy. Uživatelé Windows, Office & Co. dostávají záplaty do počítače automaticky prostřednictvím služby Windows Update.

INFO: www.microsoft.com

CHECK POINT

Řešení DoS zranitelnosti Microsoft Windows 7

V protokolu SMB (Microsoft Server Message Block) bylo objeveno zranitelné místo, které umožňuje útočníkovi DoS útok (Denial of Service), při kterém dochází k zahlcení serveru požadavky a jeho pádu nebo minimálně k jeho nefunkčnosti a nedostupnosti. Tato chyba v zabezpečení se týká systému Windows Server 2008 a je také první chybou oznámenou pro Windows 7. SMB je protokol pro sdílení souborů v síti, který je implementován v systému Microsoft Windows. Tato zranitelnost je důsledkem chyby v jeho implementaci. K selhání dojde při parsingu datových polí speciálně vytvořených SMB paketů. Vzdálený útočník může zneužít této chyby pomocí speciálně vytvořené síťové zprávy. Úspěšné zneužití může způsobit odmítnutí služby na cílovém systému a způsobit tím, že přestane reagovat do jeho ručního restartování. Popis útočného kódu je již veřejně dostupný. Check Point nyní nabízí ochranu této chyby prostřednictvím IPS produktů – IPS Software Blade, SmartDefense a IPS-1. Tato produkty jsou schopny poškozené pakety SMB detekovat a úspěšně blokovat. Více informací můžete nalézt na oficiálních stránkách společnosti Microsoft a Check Point.

VAROVÁNÍ TREND MICRO

Koobface zneužívá Google Reader

Trend Micro TrendLabs zaznamenaly další rozšíření botnetu Koobface, který začal zneužívat službu společnosti Google nazvanou Google Reader. Výzkum hrozeb prováděný společností Trend Micro průběžně monitoruje nezákonné aktivity Koobface, včetně zaplavení webů pro social networking, ať už jde o Facebook, MySpace, nebo Twitter, adresami URL, které Koobface nakazil. Pracovníci Trend Labs zjistili, že Koobface zaplavil weby sociálních sítí adresami URL služby Google Reader. Podstatou tohoto útoku je účet Google kontrolovaný gangem Koobface, který hostuje stránku s falešným videem YouTube. Když oběť na falešné video YouTube klepne, je přesměrována na napadený web, který hostuje další falešné video YouTube. Tento napadený web nakazí počítač uživatele a následně se oběť stane součástí botnetu Koobface. V době vzniku tohoto článku bylo známo přibližně 1 300 jedinečných účtů služby Google Reader vytvořených gangem Koobface na webech sociálních sítí. Společnost Trend Micro o tomto incidentu informovala Google.

„Jde o další útok, kde počítačoví piráti zneužívají k vlastnímu obohacení nástroje pro social networking, jež byly původně určeny pro zábavu,“ konstatuje šéf technologického oddělení Trend Micro Raimund Genes. Google Reader je bezplatná služba nabízená společností Google, která uživatelům umožňuje sledovat a sdílet nový obsah na webových serverech. A právě funkci, která uživatelům umožňuje sdílet nový obsah, zneužívají počítačoví piráti k rozesílání záplavy nebezpečných odkazů.

INFO: www.trendmicro.com