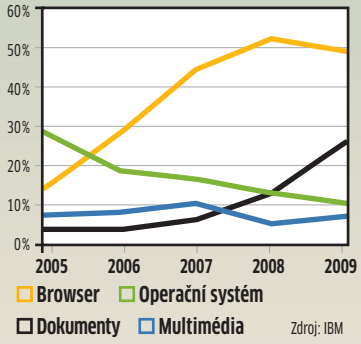
DATA A FAKTA

Barometr nebezpečí
v říjnu:

Autoři virů sázejí na zmanipulovaný mapový materiál pro navigační přístroje. Každý stažený podklad proto zkontrolujte virovým skenerem.

Hlavní cíle útoků



Zdroj: IBM

Útočníci pronikají do počítačů stále častěji mezerami v internetových prohlížečích a prostřednictvím zmanipulovaných dokumentů.

Kolik vydělávají hackeři

1. **Informace o kreditních kartách**
   0,04 € – 21 €
2. **Údaje o účtech**
   7 € – 690 €
3. **Proražené přístupy k e-mailu**
   0.06 € – 70 €
4. **Platné e-mailové adresy**
   0.23 € – 70 € pro MByte
5. **Webové proxy**
   0.11 € – 4 €

Zdroj: Symantec

Nejvíce vynáší prodej odcizených údajů o bankovních účtech.

Číslo měsíce

80 %

uživatelů Adobe Flash surfuje se zranitelnou verzí, tvrdí bezpečnostní firma Trusteer.

Hackeři falšují biometrická data

Modely notebooků s obličejovým skenerem byly považovány za bezpečné – až do teď. V současné době už si totiž hackeři do takového počítače dokážou vynutit přístup pomocí **ZMANIPULOVANÝCH FOTOGRAFIÍ**.

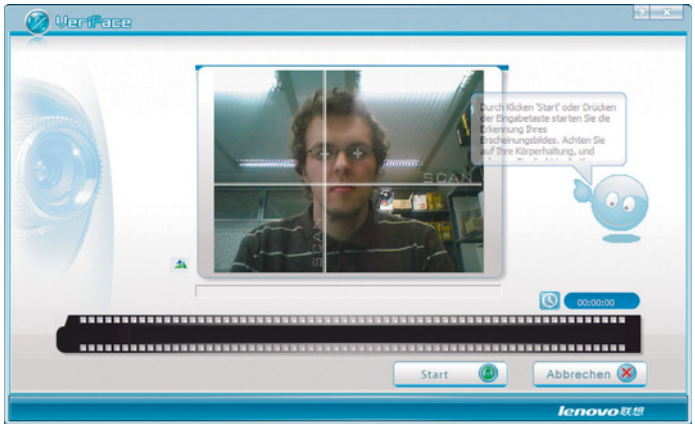
FABIAN VON KEUDELL

U novějších modelů notebooků už nemusíte zadávat žádná hesla – stačí váš obličej. Biometrický software jej porovná s uloženými charakteristickými rysy a PC pak pro vás uvolní. Díky tomu máte přístup k počítači jenom vy – a vynalézaví hackeři z Asie. Bezpečnostní experti vietnamské firmy Bkis Internet Security totiž vypátrali, jak lze obličejový skener ošálit. Výrobci jako Lenovo, Asus a Toshiba nabízejí u vybraných modelů možnost autentizace uživatele pomocí skenování obličeje. Vzdálí-li se pak daná osoba od počítače, software přístup zablokuje. V počátcích techniky rozpoznávání obličejů zaznamenával software jen několik ukazatelů, například vzdálenost očí nebo odstup koutku úst od špičky nosu. Podle světelných podmínek a kvality použité optiky pak byly výsledky natolik vágní, že software povolil přístup téměř každému. Nové verze softwaru ukládají zhruba deset fotografií uživatele a ty při autentizaci porovnávají s obrazem z webové kamery.
Útočníci však v algoritmu objevili chybu. Vytištěný snímek osoby, který pochází třeba ze stránky Facebooku, je schopen software přelstít. Aby se to podařilo, musí však útočníci pořídit kolem 30 různých variant obrázku, mezi nimi třeba černobílou fotografii nebo modifikaci s vysokým kontrastem. Takto vybaveni spustí „fake-face útok“ hrubou silou. Výsledkem bývá, že často už po dvacátém obrázku software přístup do chráněného počítače povolí.

Proti prolomení ochrany: Bezpečná je pouze kombinace biometrických údajů

Skutečnou ochranu tedy obličejové skenery notebooků nezaručují. Vývojáři průmyslových biometrických skenerů se už ostatně od čistého rozpoznávání obličejů odklánějí. Opravdu bezpečné jsou jenom kombinace různých biometrických znaků, například otisk prstu a obraz oční sítnice. Příslušný skener přitom kontroluje nejen otisky prstů, nýbrž i rozměry ruky. K tomu oční skener sejme strukturu sítnice – to dnes představuje zatím neprolomitelný systém. Ale nezoufejte. Nechcete-li se u svého notebooku vzdát bezpečného rozpoznávání biometrických ukazatelů, nemusíte hned vydávat tisíce eur. Bohatě vám postačí jednoduchý skener otisků prstů. Mnozí výrobci už do svých modelů takovýto „swipe-scanner“ integrují. Jako dodatečné vybavení je vhodný Fingerprint Reader od Microsoftu **(www.microsoft.com, cca 45 eur)**. Přinejmenším jej lze ošidit daleko nesnadněji než obličejové skenery výrobců notebooků.

INFO: http://security.bkis.vn



Kontrola obličeje: Nové notebooky umožňují přístup do počítače na základě snímání obličeje – bohužel se tato ochrana dá snadno prolomit.

OPENOFFICE, MS OFFICE

Word s virem

Bezpečnostní mezera ve Wordu a v XML modulu bezplatné soupravy OpenOffice umožňuje hackerům dopravit do počítače škodlivý kód a spustit jej s oprávněním správce. Chyba se v textovém editoru projevuje při použití zmanipulovaných WMV souborů (Windows Media Video). Je-li takové video vloženo dovnitř textu, může při jeho otevření dojít k přeplnění paměti. Pak je možné dohnat počítač ke zhroucení nebo spustit hackerský program. Jiné slabé místo využívají útočníci prostřednictvím speciálního XML souboru. V OpenOffice používaný Open Document Format (ODF) obsahuje XML kód, který program spouští při otevírání souboru – tak si mohou hackeři přivlastnit kontrolu nad počítačem. Obě mezery jsou podle vyjádření výrobce Sun v aktuální verzi 3.1.1 odstraněny.

INFO: www.openoffice.org

HROZBA

Červ pro iPhone

Na serveru Slashdot **(http://apple.slashdot.org/story/09/11/08/1411259/First-i-Phone-Worm-Discovered-Rick-rolls-Jailbroken-Phones?-from=rss)** byla zveřejněna informace o prvním červu, který se šíří telefony iPhone zneužitím přednastaveného hesla pro SSH server, které si uživatelé nezměnili.

INFO: zprávy.actinet.cz

HACK V REÁLNÉM ČASE

Audio i video VoIP hovory kompromitovány

Na hackerské konferenci Toorcon byly předvedeny nové funkce Open-source aplikace UCSniff tool umožňující odposlech voice-over-internet-protocol hovorů prováděných například pomocí populárních aplikací pro iPhone. Už více než rok UCSniff tool poskytuje vše, co jen hacker k odposlechu takových hovorů potřebuje, ale dodnes se jednalo o sestavení těchto rozhovorů až po jejich ukončení. Stejným způsobem mohou být zachyceny i video hovory. S nástupem iPhonu a jiných smartphonů velké množství lidí přešlo na VoIP technologie umožňující spojení prakticky zdarma pomocí datového připojení telefonu. Problém je ten, že mnoho aplikací, které toto umožňují, nepodporuje jakékoli šifrování. Bez pochyb odposlech VoIP hovorů existuje stejně dlouho jako samotná technologie VoIP, UCSniff jen tuto práci značně ulehčuje. Podle vývojáře Jasona Ostroma se jedná o nástroj ulehčující testování zabezpečení sítí a pomáhající poskytovatelům bezpečnostních řešení držet krok s dobou. Více informací naleznete v článku na serveru The Register **(www.theregister.co.uk/2009/10/23/iphone_voip_sniffing_made_easy/)**. O rozruch v této oblasti se nedávno postaral Charlie Paglee, který na svém blogu **(http://voipwiki.com/)** tvrdil, že ho kontaktoval hacker z Číny, který prý cracknul protokol používaný komunikačním programem Skype. Zda šlo o podvod či skutečnost se doposud neprokázalo.

INFO: zprávy.actinet.cz

MICROSOFT

FTP hackeři

Využitím slabého místa v FTP serveru služeb Microsoft IIS 5 a 6 (Internet Information Services) si útočníci mohou na serveru zjednat oprávnění správce. Útok nedokáže odhalit ani vlastní ochrana Microsoftu „Stack Cookie Protection“. Hacker nejprve na FTP serveru založí speciální adresář a tuto složku vyvolá příkazem »NLST« (Name Listing). Podle vyjádření Microsoftu má být pro tento problém vydána záplata, dosud však není ve vývoji. „Mezera dosud nebyla aktivně využita,“ tolik tiskový mluvčí Thomas Baumgärtner. Těm, kteří přesto chtějí svůj server zabezpečit, momentálně pomůže jen tento trik: Pokud všem uživatelům FTP a hostujícím účtům odeberete oprávnění zakládat složky v kořenovém adresáři, nic pak nepořídí ani hacker.

INFO: www.microsoft.com

INFO

Nová bezpečnostní rizika

MICROSOFT

Softwarový gigant zacelil hned pět kritických bezpečnostních mezer, jimiž mohou hackeři propašovat do počítače škodlivý kód. Postižena jsou Windows XP a Windows Vista. Aktualizace přijdou do počítače automaticky prostřednictvím služby Windows Update.

INFO: www.microsoft.com

GOOGLE CHROME

Jediná zmanipulovaná webová stránka stačí, aby se browser Chrome zhroutil a v PC se spustil záškodnický program. Proto si nainstalujte aktuální verzi 2.0.172.43 Google Chrome. Ta odstraní tuto a ještě dvě další slabiny.

INFO: www.google.com/chrome

ORACLE CRITICAL PATCH UPDATE ŘÍJEN 2009

Společnost Oracle vydala balík bezpečnostních záplat pro celkem 21 produktů. Kromě databáze se záplatují aplikační server, WebLogic, JRockit, E-Business Suite, AutoVue, Agile EDM, produkty PeopleSoft/JDE a Oracle Communications Order and Service Management.

INFO: zpravy.actinet.cz

DDOS VE ŠVÉDSKU

Několik významných švédských webů se stalo nedávno obětí distribuovaného DoS útoku. Mimo jiné byly vyřazeny z provozu i www stránky policie. O síle útoku vypovídá příklad společnosti Adeprimo, jejíž web v době útoku zahltilo 400 tisíc požadavků za sekundu oproti obvyklým osmi stům požadavkům. Další informace nabízí například server The Register **(www.theregister.co.uk/2009/10/30/swedish_ddos_attacks/)**.

INFO: zpravy.actinet.cz

UPGRADE PRO MOZILLU FIREFOX

Mozilla Foundation vydala 27.10.2009 celkem jedenáct bezpečnostních oznámení **(www.mozilla.org/security/announce/)** týkajících se webového prohlížeče Firefox. Šest zranitelností je kritických. Řešením je povýšení na Firefox 3.0.15, nebo 3.5.4. Některé zranitelnosti se týkají i balíku aplikací SeaMonkey. V tomto případě je doporučen upgrade na verzi 2.0

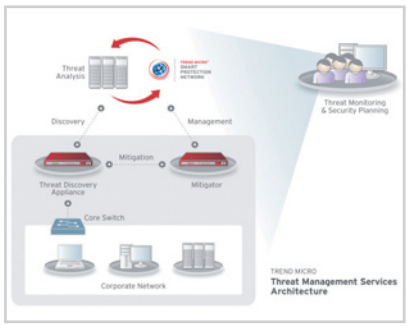
INFO: zpravy.actinet.cz

ZABEZPEČENÍ TREND MICRO

Threat Management Services

Společnost Trend Micro představila novou nabídku Threat Management Services, která podnikům zajišťuje „dohled nad bezpečností sítí“ – vrstvu zabezpečení posilující současnou bezpečnostní infrastrukturu organizace v boji proti aktivnímu malwaru určenému ke krádeži dat, který stávající bezpečnostní řešení nedokáží odhalit. Trend Micro™ Threat Management Services tyto hrozby odhalí a zajistí včasné varování, zabrání jejich dalšímu šíření a umožní nápravu situace; firmy získají lepší ochranu, větší přehled a jednodušší správu. Služby Threat Management Services jsou tvořeny třemi balíky, které nabízejí celou řadu poradenských služeb pro detekci hrozeb a plánování zabezpečení. Patří sem:

► Trend Micro Threat Discovery Services: Tento balík obsahuje technologii Threat Discovery, která umožňuje IT oddělení identifikovat, analyzovat a zmírnit dopady problémů celopodnikového zabezpečení proti hrozbám, včetně dosud nezjištěných napadení, rizikového chování a postupů, potenciálních bodů průniku malwaru a dalších situací zvyšujících zranitelnost sítě. Díky nonstop zpravodajství Trend Micro o hrozbách z celého světa, které je součástí infrastruktury Trend Micro Smart Protection Network, získají zákazníci přehled o nejrůznějších rizikových faktorech zabezpečení informací v celé své síti z na míru připravených denních a týdenních sestav.



► Trend Micro Threat Remediation Services: Tento balík obsahuje funkce Threat Discovery Services a nepřetržité monitorování, aktivní výstrahy včasného varování a poradenské služby pro nápravu škod způsobených skrytým malwarem pro krádež dat. Tyto služby poskytují odborní poradci Trend Micro Threat Management Advisor, kteří 24 hodin denně, 7 dní v týdnu aktivně pracují na monitorování nákaz v sítích zákazníka.

► Trend Micro Threat Lifecycle Management Services: Tento balík obsahuje veškeré funkce z předchozího balíku a dále je rozšiřuje o automatické odstraňování hrozeb a technologii analýzy příčin spolu se službami aktivního plánování zabezpečení, které poskytuje specializovaný poradce Trend Micro Threat Management Advisor.

Všechny tři balíky služeb jsou určeny k posílení a rozšíření stávající infrastruktury zabezpečení, která má nevyhnutelně mezery, jichž zneužívají utajené nové hrozby. Bezplatná čtrnáctidenní ukázka služeb Security Threat Assessment (Hodnocení bezpečnostních hrozeb), poskytovaná společností Trend Micro, klade důraz na skutečnost, že prostředí většiny firem není tak bezpečné, jak si tyto firmy myslí: ze 130 hodnocení bezpečnostních hrozeb Security Threat Assessment provedených společností Trend Micro od října 2008 do srpna 2009 bylo 100% všech zúčastněných podniků nakaženo aktivním malwarem.

Nejenže se v počítačích skrývají neznámé hrozby, nový výzkum Trend Micro navíc naznačuje, že malware zůstává v počítačích mnohem déle, než se dříve předpokládalo. Při analýze více než 100 milionů napadených IP adres zjistila společnost Trend Micro, že většina napadených IP adres zůstává nakažena (nebo je opakovaně napadána) po dobu delší než dva roky a v zemích s nejvyššími hodnotami trvá nákaza nejčastěji 300 dní. Osmdesát procent všech napadených počítačů zůstává nakaženo déle než měsíc. Služby Trend Micro Threat Management Services jsou součástí řešení Trend Micro Enterprise Security – úzce integrované nabídky produktů, služeb a řešení pro zabezpečení obsahu, založené na infrastruktuře Trend Micro Smart Protection Network. Trend Micro Enterprise Security zajišťuje bezprostřední ochranu před novými hrozbami a zároveň podstatně zjednodušuje správu zabezpečení a snižuje náklady s ní spojené.

ODHALENÍ KASPERSKY LAB

Zneužití YouTube pro videospam

Společnost Kaspersky Lab oznamuje, že její odborníci zaznamenali velké množství spamů odkazujících na reklamu na serveru YouTube. Nevyžádané e-maily byly rozesílány v mnoha variacích, všechny však obsahovaly stejný odkaz.

YouTube je velmi atraktivním zdrojem pro distribuci spamu díky své celosvětové popularitě. Již v roce 2007 předpovídali specialisté ze společnosti Kaspersky Lab možnost zneužití serveru YouTube jako prostředku k rozesílání nebezpečných e-mailů. Toto je však první případ, kdy jsou uživatelé přímo přesměrováni ke sledování reklamního videa. „Je přirozené, že tento typ reklamy je zajímavější a zasáhne mnohem více uživatelů,“ říká Daria Gudková, ředitelka obsahové analýzy a výzkumu v Kaspersky Lab. „Před dvěma lety zneužili spammeři jméno YouTube a místo zajímavého videa byli uživatelé přesměrováni na reklamní sdělení. Nyní vede odkaz přímo na populární server YouTube, kde je umístěna nevyžádaná reklama.“

Není to letos poprvé, co byli tvůrci spamů kreativní. V dubnu byly zaznamenány zprávy obsahující nestandardní obrazový materiál, které inzerovaly služby spammerů. Tyto grafické soubory byly také upraveny pomocí metod využívajících obrazový šum, které způsobily spamovým filtrům značné problémy. Společnost Kaspersky Lab proto znovu upozorňuje na důležitost zapnutého spamového filtru, který blokuje nevyžádanou a potenciálně nebezpečnou korespondenci. Spamové filtry v produktech společnosti by také měly mít nastaven mod „učení“, díky němuž se neustále zlepšuje ochrana proti všem typům nevyžádané pošty.

INFO: www.kaspersky.com

HROZBY PRO IE, CHROME A SAFARI

Podvrh PayPal SSL klíče

Hackeři zveřejnili padělek SSL certifikátu pro PayPal, který využívá chyby v programovací aplikaci CryptoAPI. Ta je využívána prohlížeči Internet Explorer, Google Chrome a Apple Safari pro Windows. Při použití falešného certifikátu všechny tři prohlížeče hlásí, že certifikát pro on-line platby je v pořádku. V případě, kdy hackeři zkombinují zranitelnost v CryptoAPI s již déle dostupnou aplikací SSLSniff, je relativně snadné donutit prohlížeč zobrazit falešnou stránku bez jakýchkoliv varování, dokonce i když adresa začíná https. Mluvčí společnosti PayPal řekl, že bezpečnostní tým společnosti si je plně vědom zranitelnosti a v současnosti se snaží zajistit další zabezpečení, které by mohl nasadit. Zranitelnost byla zveřejněna v červenci na konferenci BlackHat, ale Microsoft ji zatím ani nepotvrdil, ani neopravil. Mluvčí softwarového gigantu oznámil, že jeho bezpečnostní tým ověřuje možné zranitelnosti Windows, prezentované na BlackHatu, a že společnost přijme potřebná bezpečnostní opatření, aby ochránila své zákazníky. Více informací naleznete na webu TheRegister.co.uk **(www.theregister.co.uk/2009/10/05/fraudulent_paypay_certificate_published/)**.

INFO: zpravy.actinet.cz

NOVÉ VERZE ANTIVIROVÝCH ŘEŠENÍ

TrustPort pro rok 2010

Do prodeje byly uvolněny bezpečnostní produkty TrustPort Antivirus 2010 a TrustPort PC Security 2010. Nové verze přinášejí zdokonalení jak v oblasti funkcí, tak v oblasti ovládání. TrustPort Antivirus 2010 a TrustPort PC Security 2010 směřují především do oblasti domácností a malých kanceláří. Zatímco první produkt se soustředí na ochranu počítače proti malwaru všeho druhu, na všech vstupních bodech počítače, druhý produkt k tomu přidává personální firewall a zabezpečení soukromých dat prostřednictvím šifrování a skartace.

Mezi firemní zákazníky míří TrustPort Antivirus Business 2010 a TrustPort PC Security Business 2010. Jejich vzhled i funkcionalita vycházejí z verzí pro domácnosti, nabízejí ovšem možnost centrální správy a hromadné instalace softwaru v podnikové síti. Kromě toho je lze zakoupit nejen ve verzi se dvěma, ale také se čtyřmi skenovacími motory, což přibližuje virovou detekci magické hranici sta procent. Ve všech zmíněných produktech byly nově použity jako výchozí kombinace skenovací motory AVG a BitDefender. Došlo tak ke zvýšení virové detekce při současném snížení počtu falešných poplachů. Oproti předchozím verzím přibyla automatizovaná instalace softwarových aktualizací, bez nutnosti manuálního zásahu uživatele. Jedná se o funkční aktualizace, nikoli o automatické aktualizace virových vzorků, které jsou samozřejmostí již dávno. Zdokonalení se dočkala také poštovní ochrana. Software nově obsahuje zásuvné moduly pro všechny běžně používané klienty, tedy Microsoft Outlook, Outlook Express, Windows Mail a Mozilla Thunderbird, a umožňuje tak efektivnější likvidaci nevyžádané a infikované pošty. Proti pokusům malwaru vyřadit antivirus z normálního provozu byla zavedena ochrana systémových souborů antiviru. TrustPort Antivirus 2010 a TrustPort PC Security 2010 jsou kompatibilní se všemi aktuálními platformami Windows, a to v 32bitové i v 64bitové verzi. Lze je provozovat na Windows 7, Windows 2008, Windows Vista, Windows 2003, Windows XP a Windows 2000. Software je k dispozici v pěti jazykových verzích - anglické, české, italské, německé a španělské. Jazyk rozhraní si uživatel volí při instalaci, ale lze ho změnit kdykoli za běhu programu.

NEBEZPEČNÁ HROZBA

SSL/TLS zranitelnost

V SSL byla nalezena kritická zranitelnost, která utočníkům umožňuje vložit se do zabezpečené SSL komunikace standardním „man-in-the-middle“ útokem. Díky tomu jsou zranitelné webové stránky využívající SSL: například internetové bankovnictví, back-office systémy, které využívají webové služby, dále aplikace jako e-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. Byla ustanovena pracovní skupina ze zástupců PhoneFactor, IETF (Internet Engineering Task Force) a organizace ICASI (Industry Consortium for the Advancement of Security on the Internet), 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 výrobci sotftwaru měli dost času na opravu, ale 4. listopadu byla zranitelnost nezávisle objevena na diskuzi pracovní spiny IETF TLS a zprávy o zranitelnosti se začaly rychle šířit IT security komunitou.

INFO: www.phonefactor.com/sslgap/

ŘEŠENÍ: AVG LINKSCANNER

Kritická slabina sociálních sítí

Zkracování internetových odkazů, zejména pro komunikaci na sociálních sítích, umožňuje zamaskovat nebezpečné stránky se škodlivým kódem. Jejich přítomnost dokáže odhalit bezpečnostní nástroj AVG LinkScanner **(www.linkscanner.avg.com)**. Cíl každého linku testuje v reálném čase a nespoléhá na databáze, mnohdy zastaralé již ve chvíli publikování. Dnešní hrozby se totiž většinou přesunují z místa na místo v čase kratším než 24 hodin. Služby zkracující linky umožňují vtěsnat odkazy do 140 znaků jedné zprávy na Twitteru či zkrátit těžko zapamatovatelnou adresu. Stávají se tak stále populárnějšími. Obdobných služeb existuje celá řada a některé jsou přímo součástí klientských twitterových aplikací nebo jiných sociálních sítí.

„Problémem zkrácených URL je, že většinou ani vzdáleně nepřipomínají původní adresu. Uživatel proto nikdy neví, kam jej nasměrují. Lidé se sice chtějí dostat na konkrétní stránku, ale zneužít takový link k odkazu na skrytý škodlivý kód je velmi jednoduché," vysvětluje ředitel výzkumu společnosti AVG Technologies Roger Thompson.

„Nakažené" internetové stránky jsou nejnovějším způsobem přenosu malwaru do počítačů. Cílem útoků je nejčastěji krádež citlivých osobních informací nebo dat, případně zapojení pracovní stanice do sítě ovládané z vnějšího prostředí (botnet). Počítač mohou uživatelé nakazit pouhým kliknutím na odkaz, prohlédnutím obrázku, a někdy dokonce stačí pouze přejet myší přes banner. Útočníci hrozby obvykle nechávají na webové stránce méně než jeden den a poté je přesunují jinam. Snaží se tím co nejvíce snížit pravděpodobnost odhalení.

„LinkScanner je jediný bezpečnostní nástroj schopný detekovat ukrytou hrozbu za zkrácenou URL," pokračuje Thompson. „Pouze LinkScanner zastaví nebezpečný pokus o otevření webové stránky dříve, než je pozdě." AVG LinkScanner je k dispozici zdarma na adrese **www.linkscanner.avg.com**.

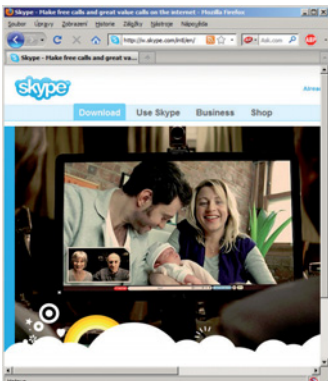
SKYPE

Odposlech VoIP

Pomocí speciálního trojského koně se jistému švýcarskému softwarovému vývojáři podařilo odposlouchávat zašifrované rozhovory na Skypu. VoIP program je považován za bezpečný, neboť spojení mezi oběma partnery při rozhovoru jsou šifrovaná. Bezpečnostní expert nyní na internetu vystavil zdrojový text nástroje, který se „zaháčkuje" do běžícího procesu Skypu v počítači. Odtamtud trojský kůň slyší každý rozhovor nezašifrovaně, jeho obsah zaznamená do MP3 souboru a ten poté odešle do předem určeného serveru na webu.

Už v roce 2008 se proslýchalo, že takovéto nástroje aktivně nasazuje bavorská justice. Tyto zprávy nebyly ani dementovány, ani potvrzeny. Autor nyní zveřejněného nástroje v minulosti pracoval pro bezpečnostní IT firmy, například pro ERA IT, které údajně vyvíjejí odposlechové programy pro orgány činné v trestním řízení. Před takovýmito útoky může ochránit jenom aktualizace softwaru. Skype už na řešení pracuje.

INFO: www.skype.com



INFO

Nová bezpečnostní rizika

ADOBE READER/ACROBAT

V aplikaci Adobe Reader i jeho placené verzi Adobe Acrobat byla nalezena kritická zranitelnost, zneužitelná ke kompromitaci systému. Zranitelnost je zavíněna blíže nespecifikovanou chybou a v tuto chvíli je aktivně zneužívána. Adobe doporučuje blokovat používání JavaScriptu při prohlížení webu a udržovat databáze svého antivirového softwaru aktuální, ačkoli i tak je možné chybu zneužít. Proti zneužití jsou také chráněni uživatelé Windows Vista používající DEP (Data Execution Protection), což je systém ochrany proti spouštění kódu z paměti RAM. Adobe by mělo podle svého vyjádření chybu opravit při příležitosti vydání pravidelných záplat 13. října. Více na serveru Adobe.com.

INFO: zpravy.actinet.cz

SAFARI, IE, CHROME

Devět týdnů poté, co hacker předvedl, jak kompromitovat autentizační certifikát pro libovolnou webovou stránku, uživatelé Internet Exploreru a dalších aplikací zůstávají v ohrožení, protože Microsoft neopravil zranitelnost v rozhraní pro programování aplikací CryptoAPI **(viz http://msdn.microsoft.com/en-us/library/ms867086.aspx)**. To způsobuje, že IE a další aplikace jsou závislé na kódu, který je možné obelstít falešnými SSL certifikáty. Chyba může způsobit to, že Google Chrome, Apple Safari pro Windows a Internet Explorer zobrazí podvodnou stránku bez jakéhokoliv varování. Naopak v prohlížeči Firefox byla chyba odstraněna **(www.theregister.co.uk/2009/08/04/firefox_critical_update/)** několik dní po zveřejnění zranitelnosti na konferenci BlackHat **(viz www.theregister.co.uk/2009/07/30/universal_ssl_certificate/)**. V současnosti není jisté, kdy bude zranitelnost opravena; Microsoft tvrdí, že prošetřuje zranitelnosti prezentované na BlackHatu, a jakmile skončí, přijme opatření nezbytná k ochraně svých zákazníků

INFO: zpravy.actinet.cz

PHP

V PHP bylo nalezeno větší množství zranitelností s dosud nespecifikovaným dopadem. Jedná se o chybu v ověřování certifikátů SSL, chybu ověření vstupu při práci s EXIF daty a jiné. Zranitelnosti byly ohlášeny ve verzích předcházejících 5.2.11. Více informací naleznete na PHP.net **(www.php.net/releases/5_2_11.php)**.

INFO: zpravy.actinet.cz

CUTEFTP / CORE FTP

V programech CuteFTP a Core FTP byla nalezena zranitelnost. Tito FTP klienti totiž nedokáží zpracovat příliš dlouhé popisky u jednotlivých FTP serverů. Uživatel tak může například importovat seznam takových serverů, případně tento seznam obnovit ze zálohy a při pokusu připojit se na nějaký z nich zavinit přetečení paměti a umožnit tak spuštění libovolného kódu. Zranitelnost je potvrzena v CuteFTP ve verzi Home a Professional 8.3.3.0054 a Core FTP 2.1.1612. Více informací o zranitelnosti v CuteFTP a Core FTP najdete na serverech Secunie **(http://secunia.com/advisories/36874/)**.

INFO: zpravy.actinet.cz

ZPRÁVA SPOLEČNOSTI SYMANTEC

Sváteční spamy

Společnost Symantec oznámila vydání své říjnové zprávy 2009 MessageLabs Intelligence Report.

Analýza odhaluje nárůst nevyžádané pošty tématicky zaměřené na svátky, včetně Halloweenu, Dne díkůvzdání, Vánoc a dne svatého Valentýna, a také vlnu phishingových útoků souvisejících s posledními termíny pro podání daňových přiznání.

V polovině října začal tým MessageLabs Intelligence pozorovat, že nevyžádaná pošta na téma Halloween tvoří 0,5 % veškeré nevyžádané pošty, soustavně narůstá a s blížícím se svátkem dosahuje špičkových hodnot 500 milionů e-mailů kolujících každý den po celém světě. V říjnu se také vzedmula vlna phishingových e-mailů, které předstíraly, že pocházejí z finančního úřadu.

Jak uvádí tým MessageLabs Intelligence, zatímco tématem e-mailů zaměřených na Halloween, které pocházely z robotických sítí Rustock a Donbot, byly léky nebo software, nevyžádaná pošta zaměřená na Vánoce a Den díkůvzdání odeslaná robotickou sítí Cutwail se týkala replik hodinek. Nevyžádané zprávy týkající se replik hodinek tvořily v říjnu přibližně 2 % nevyžádané pošty. Odhaduje se, že v následujících měsících budou po celém světě každý den kolovat dvě miliardy těchto zpráv. Nejvíce phishingových e-mailů s předstíraným původem v IRS bylo zachyceno 10. října, kdy ve 24hodinovém období tvořily 67 % všech phishingových e-mailů, zatímco phishingové e-maily s předstíraným původem v HMRC dosáhly vrcholu 13. října, kdy tvořily 81 % všech phishingových e-mailů zachycených v tento den, což je historicky jedna z největších phishingových vln zaměřených na HMRC.

„Jak je v této části roku pro tvůrce nevyžádané pošty typické, snaží se vydělat na svátcích," řekl vedoucí analytik MessageLabs Intelligence Paul Wood. „Nejspíš jsou až příliš horliví, ale rozesílání nevyžádané pošty je hra velkých čísel a velké objemy dosud nepochybně autorům nevyžádané pošty přinášely úspěch. Možná začínají tak brzy proto, aby se v konkurenčním boji s jinými robotickými sítěmi pokusili maximalizovat svoji šanci na úspěch."

V říjnu se sice objevily vlny phishingu souvisejícího s daňovými přiznáními, ale obecně jsou phishingové útoky na ústupu ve srovnání s nejvyššími úrovněmi aktivity počátkem tohoto roku. Tým MessageLabs Intelligence se domnívá, že je to částečně důsledkem toho, že je k dispozici méně sad phishingových nástrojů. Zdá se ale, že narůstají vlny phishingu v jiných jazycích než angličtina, například ve francouzštině a italštině.

„Co se týče vln phishingu," řekl Wood, „zaznamenali jsme v přístupu útočníků podstatný posun. Nejen, že experimentují s různými jazyky, ale kromě finančního sektoru se cílem jejich pozornosti stávají také služby online, jako je webový e-mail. Důvodem je pravděpodobně to, že e-mailové adresy se v hojné míře používají k ověřování na jiných webech, například ve společenských sítích, na maloobchodních a aukčních webech."

V říjnu tým MessageLabs Intelligence zachytil také další řadu nevyžádaných zpráv ve stylu podvodu se záložní platbou v souvislosti s nějakou událostí. Tou je tentokrát mistrovství světa v kopané v Jižní Africe v roce 2010. Zprávy požadují od adresáta finanční obnos, po jehož zaplacení obdrží inzerovanou výhru.

Tým MessageLabs Intelligence informoval počátkem měsíce také o nárůstu objemu nevyžádané pošty související s trojskými koni Bredolab rozesílané z robotické sítě Cutwail (Pandex). Cílem trojského koně Bredolab šířeného ve formě komprimované přílohy e-mailu je dát odesílateli úplnou kontrolu nad cílovým počítačem. Nejnovější e-maily měly v předmětu sledovací číslo zásilky. Nevyžádaná pošta související s trojským koněm Bredolab dosáhla nejvyšší úrovně v říjnu a každý den v měsíci tvořila 3,5 % nevyžádané pošty a 5,6 % škodlivého kódu. Tým MessageLabs Intelligence odhaduje, že každý den je distribuováno 3,6 mld. e-mailů se škodlivým kódem Bredolab.

Další nejdůležitější informace ve zprávě:

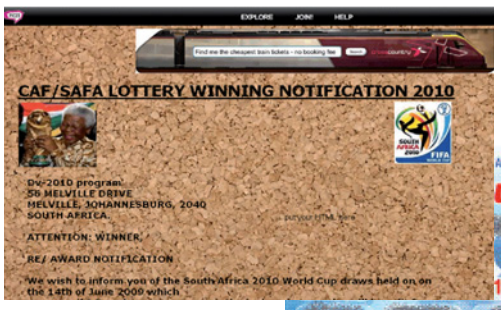
Nevyžádaná pošta: V říjnu 2009 byl globální podíl nevyžádané pošty v e-mailovém provozu z nových a dříve neznámých závadných zdrojů 88,1 % (1 z 1,1 e-mailů), což je od září zvýšení o 1,7 %.

Viry: Globální podíl e-mailů napadených virem v e-mailovém provozu z nových a dříve neznámých závadných zdrojů byl v říjnu jeden z 230,8 e-mailů (0,43 %), což je od září zvýšení o 0,18 %. 19,2 % škodlivého kódu šířeného e-mailem obsahovalo v říjnu odkazy na nebezpečné webové servery, což je od září pokles o 20,6 %.

Phishing: V říjnu byla aktivita phishingu 1 z 293,7 e-mailů (0,35 %), to je zvýšení o 0,11 %.

Zabezpečení webu: Analýza činností zaměřených na zabezpečení webu ukazuje, že 37,6 % veškerého webového škodlivého kódu zachyceného v říjnu. Tým MessageLabs Intelligence identifikoval také každý den v průměru 3 086 webových serverů, které se nově staly hostiteli škodlivého kódu a jiných potenciálně nežádoucích programů, jako je spyware a Avare.

Říjnová zpráva 2009 MessageLabs Intelligence Report obsahuje podrobnější údaje o všech výše uvedených trendech a hodnotách a podrobnější rozbor trendů v zeměpisných oblastech a ve vertikálních oborech. Úplná zpráva je k dispozici na adrese **http://www.messagelabs.com/intelligence.aspx**.



Loterie: Vyhráli jste miliony v Nigérii nebo jen vstupenky na mistrovství světa ve fotbalu?

Spam: Mezi nejčastější cíle útoků patří oblast zdravotnictví.

INFO

Trendy hrozeb podle zeměpisných oblastí

► Úroveň nevyžádané pošty se v říjnu zvýšila v Dánsku o 0,6 %, čímž si tato země zajistila pozici země s největším podílem nevyžádané pošty, který dosahuje 96,2 % ze všech e-mailů.

► V USA se podíl nevyžádané pošty zvýšil na 94,0% a v Kanadě na 93,0%. Podíl nevyžádané pošty vzrostl ve Velké Británii na 93,3%.

► Největší nárůst nevyžádané pošty byl v Mexiku, kde podíl nevyžádané pošty vzrostl o 4,8 % na 92,7 %. V Nizozemsku dosáhl podíl nevyžádané pošty 93,5 %, v Austrálii vzrostl na 92,9 %.

► V Hongkongu dosáhl podíl nevyžádané pošty 94,5 %, v Japonsku byl na úrovni 91,7%.

► Aktivita virů vzrostla v Číně o 0,77 % na 1 v 80,7 e-mailů, čímž se Čína dostala na první místo tabulky.

► Největší zvýšení ze všech zemí bylo pozorováno v Lucembursku, kde se aktivita virů zvýšila o 97 %.

► Úroveň virů v USA byla 1 v 291,2 (1 vir v jednom z 291,2 e-mailů) a v Kanadě 1 v 274,0. V Německu byla úroveň virů 1 v 192,1, v Nizozemsku 1 v 367,8, v Austrálii 1 v 277,5, v Hongkongu 1ve 174,6 a v Japonsku 1 v 248,7.

► Lucembursko byla nejaktivnější země v oblasti phishingových útoků s podílem 1 v 110,0 e-mailů, za ním následovala Čína s podílem 1 v 138,2.