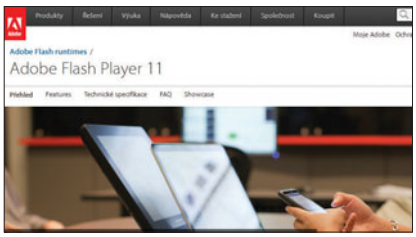
Mezery v Adobe Flash a přístup do systému

Sedm bezpečnostních zranitelností v přehrávači Flash Player společnosti Adobe může útočníkovi umožnit přístup do systému – a to na všech platformách.

V přehrávači Adobe Flash Player bylo nalezeno sedm zranitelností, které mohou hackerovi umožnit přístup do postižených systémů. Chybu lze označit za zvlášť závažnou i proto, že se vyskytuje ve všech verzích Flash Playeru – najdete ji nejen na počítačích se systémem Windows, ale i na počítačích s Mac OS či Linuxem a na smartphonech a tabletech s Androidem. Další nepříjemností je, že chyba byla nalezena i v multiplatformním prostředí Adobe AIR. Chybu objevili zaměstnanci společnosti Google a nahlásili ji Adobe.

Slabiny v softwaru mohou způsobit, že útočník získá úplnou kontrolu nad zařízením. Chyba také může zapříčinit zhroucení systému. Firma Adobe označila zranitelnost jako nebezpečnou, ale k možným způsobům zneužití se blíže nevyjádřila. Důvodem byla patrně i skutečnost, že výrobce reagoval rychle a nabídl na postižené systémy záplaty. Uživatelé systému Windows nebo Mac OS X mohou prostřednictvím webových stránek společnosti Adobe využít upgrade na verzi 11.5.502.110, pro uživatele Linuxu je k dispozici verze 11.2.202.251. Aktualizace Adobe Flash pro Android (2.x a 3.x) hledejte pod označením 11.1.111.24 a pro Android 4.x pod 11.1.115.27.



BUDOUCÍ FLASH SE AKTUALIZUJE JEDNOU ZA MĚSÍC

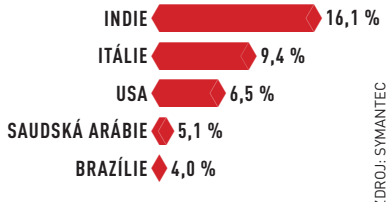
Potěšitelnou zprávou je, že v budoucnu by už Flash nemusel být jednou obrovskou bezpečnostní dírou do systému. Například ve Windows 8 už nebude chybět ani aktualizační rutina, protože přehrávač Flash je integrován přímo do aplikace Internet Explorer 10. V budoucnu se také počítá s tím, že Adobe bude opravovat Flash v rámci „Microsoft Patch Tuesday". Adobe tak pro Flash připraví aktualizace, které budou distribuovány v rámci záplat, které společnost Microsoft uvolňuje každé druhé úterý v měsíci.

Nebezpečné mezery

Chyba v přehrávači Flash Player umožňuje hackerům přístup k PC, tabletům a mobilním telefonům.

INDIE MEZI TOP SPAMMERY

Z Indie, Itálie a USA přišla ve třetím čtvrtletí roku 2012 třetina světového spamu.



ZDROJ: SYMANTEC

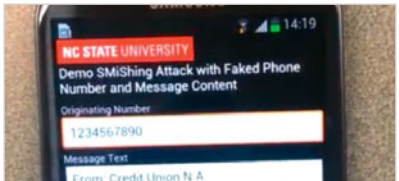
AVG 2013 Chip Edition

Na Chip DVD je opět připravena nejnovější verze komplexního antivirového řešení AVG Internet Security 2013 Chip Edition s celou řadou nových funkcí, které ochrání váš počítač nejen před malwarem.

Nová hrozba pro Android

Výzkumníci z univerzity v Severní Karolíně v USA objevili novou metodu SMS phishingu. Zranitelnost umožňuje spuštění nedůvěryhodné aplikace na telefonu, která vytvoří falešnou příchozí textovou zprávu SMS s libovolným obsahem – týká se to jak textu samotné zprávy, tak i odesílatele, kterým může být telefonní číslo ze seznamu kontaktů nebo jednoduše z vaší důvěryhodné banky.

Zvláště znepokojující je skutečnost, že zranitelnost nepotřebuje ke své činnost žádné zvýšené oprávnění, varuje profesor počítačových věd Xuxian Jiang. Google už na záplatě pro platformu Android pracuje.



DATOVÉ ÚNIKY MĚSÍCE

TWITTER: HACKNUTA CELÁ ŘADA ÚČTŮ

Služba Twitter oznámila, že velké množství jejích uživatelských účtů bylo napadeno hackery. Účty, včetně známých technologických blogů, byly zneužity pro zasílání podvodných zpráv. Firma proto hesla na hacknutých účtech resetovala a uživatele vyzvala, aby si vytvořili nová hesla. Také by si měli zkontrolovat, zda hackeři neprovedli změny v jejich profilu.

PODVODNÁ APLIKACE: HACKEŘI ZÍSKALI 500 000 EUR

Pouze dvacetiletému hackerovi z Francie se povedlo podvodem získat přibližně 500 000 eur. Jeho podvodná aplikace, která patřila na app storu k nejpopulárnějším, nalákala přibližně 17 000 obětí na bezplatné stahování. Jeho aplikace pak tajně posílala prémiové SMS zprávy a také na počítač hackera odesílala přihlašovací údaje k on-line účtům webů hazardních her.

COCA-COLA: DOHODA ZA MILIARDY ZRUŠENA

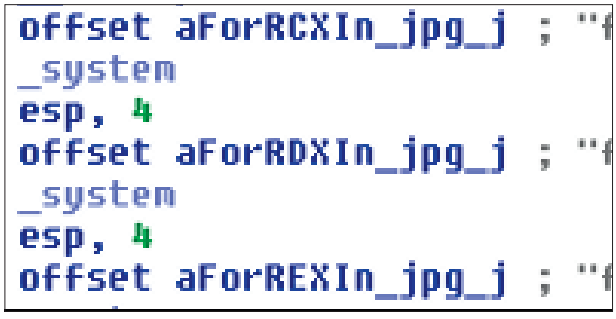
Nedávno se na internetu objevily interní dokumenty, vnášející světlo do tři roky starého případu. V roce 2009 se totiž Coca-Cola pokusila o akvizici čínského výrobce nápojů huiyuanJuice. Podle FBI se ale hackerům pomocí phishingového útoku podařilo infiltrovat počítače nejvyššího vedení firmy a získat celou řadu citlivých interních dokumentů. Čínská vláda poté prodej zablokovala.

42 %

ZTRACENÝCH MOBILNÍCH TELEFONŮ VE VELKÉ BRITÁNII NEMĚLO OCHRANU PŘED NEOPRÁVNĚNÝM PŘÍSTUPEM K DATŮM.

5 z deseti programů v žebříčku softwarových zranitelností patří podle společnosti Kaspersky firmě Adobe.

56 procent Britů se již stalo obětí počítačové trestné činnosti.



Trojský kůň krade fotografie

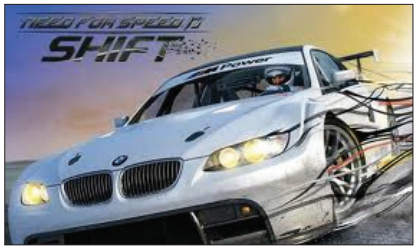
Bezpečnostní experti firmy Sophos objevili trojského koně, který je navržen tak, aby z pevného disku oběti ukradl všechny obrazové soubory. Program Troj/pixSteal-A na discích C, D a E hledá fotografie ve formátu JPEG a všechny nalezené soubory odesílá na FTP server v Iráku. Analytici také doporučují kontrolu zařízení na skenování dokumentů. Jedinou stoprocentní ochranou je prozatím zablokování FTP ve firewallu.

Pozor na „sexting“ aplikaci

Web Yoursphere.com, zabývající se bezpečností dětí na webu, komentoval kriticky populární aplikaci Snapchat. Ta umožňuje odesílání obrázků (fotografií) a textových zpráv s možností nastavení časového limitu, po který se fotografie zobrazí na cílovém zařízení. Především mladší uživatelé ji proto využívají pro tzv. sexting – fotoverzi erotického rozhovoru. Podle Yoursphere.com je ale nebezpečné především to, že možnost nastavení krátkého časového úseku zobrazení může implikovat falešný pocit bezpečí. Ve skutečnosti však poskytovatel nezaručuje, že fotografie budou za nastavenou dobu skutečně odstraněny z jeho serverů.

FOTO: ISTOCKPHOTO/ALENGO; XUXIAN JIANG

Eset: SMS trojský kůň okrádal i obyvatele ČR



Trojský kůň SMS Boxer vyvinutý speciálně pro mobilní telefony s operačním systémem Android okrádal obyvatele České republiky a dalších 62 zemí. Potvrdil to nedávný výzkum antivirové společnosti Eset. Mezi nejvíce postižené země patří kromě Česka také Polsko, Německo, Rusko a Francie.

„Z Boxera se stal jeden z nejvýznamnějších SMS trojanů loňského roku a je zároveň prvním, který se snaží útočit v tak velkém počtu zemí,“ říká o hrozbě Petr Šnajdr, bezpečnostní expert společnosti Eset. Analýzu trojského koně zveřejnil Eset nedlouho poté, co SMS zpráva oslavila své 20. výročí. Přesně 3. prosince 1992 byla totiž ve Velké Británii odeslána první textová zpráva ve znění „Veselé Vánoce“.

Podstatou tohoto škodlivého kódu je skryté přihlášení mobilního telefonu do zpoplatněných SMS služeb, které provedl infikovaný mobil. Za normálních okolností vidí majitel smartphonu všechny přijaté zprávy, i ty zpoplatněné. V tomto případě však SMS Boxer tyto zprávy zablokoval, uživatel tedy nevěděl, že jeho mobil přijímal zpoplatněné esemesky. O infekci se pak dozvěděl až z vysokého účtu za telefon. SMS Boxer je schopen z mobilního telefonu získat informaci, ve které zemi se nachází a služby kterého operátora využívá. Na základě toho si z databáze vybere to správné telefonní číslo, na které se přihlásí a z nějž potom přijímá zpoplatněné zprávy.

Uživatelé se SMS Boxerem mohli nakazit například při instalaci falešných aplikací ze služby Google Play nebo po stažení těchto aplikací z různých stránek nebo úložišť. Lidé v domnění, že si do mobilu stahují nezpoplatněnou verzi neškodné aplikace, si nainstalovali i SMS Boxera. K nakažení tímto malwarem byly využívány oblíbené hry jako Sim City Deluxe Free, Need for Speed Shift Free, Assassin Creed a některé doplňky pro Angry Birds. V prosinci bylo v digitální službě Google Play nalezeno 22 aplikací infikovaných touto hrozbou, odkud však již byly odstraněny.

„Tvůrci této hrozby zneužili také fakt, že téměř nikdo nečte licenční ujednání při instalaci softwaru,“ vysvětluje Šnajdr. Uživatelé totiž při instalaci dali infikované aplikaci povolení k odesílání a přijímání textových zpráv.

Česko hostí malware, ale je bezpečné

Společnost Kaspersky Lab vydala každoroční bezpečnostní zprávu se statistikami za rok 2012. Analyzovaná data pocházejí z cloudové databáze Kaspersky Security Network (KSN), která slouží k telemetrii a k okamžité ochraně ve formě blacklistů a heuristických pravidel vytvořených na ochranu před nejnovějšími hrozbami.

Zpráva Kaspersky Security Bulletin zmiňuje na dvou místech také Českou republiku – a to ve dvou rozdílných rolích. Na jedné straně je Česko jedenáctou zemí v žebříčku Top 20 států, v nichž jsou umístěny servery, které se využívají k malwarovým útokům, na druhé straně je kybernetičtí zločinci nevyužívají k útokům na místní uživatele. Zpráva totiž jedním dechem dodává, že Česko je zároveň mezi těmi zeměmi, v nichž je nejbezpečnější se k internetu připojit. Kaspersky Lab v současnosti detekuje a blokuje více než 200 tisíc škodlivých programů denně. V prvním pololetí to přitom bylo v průměru „jen" 125 tisíc denně. Společnost Kaspersky Lab v roce 2012 úspěšně zablokovala více než 3 miliardy lokálních infekcí. Až 99 % veškerého mobilního malwaru bylo zacíleno na OS Android. Nicméně Apple také nezůstává ušetřen – nárůst útoků na Mac OS X je oproti loňsku téměř třetinový. Více informací naleznete v publikaci Kaspersky Security Bulletin.

Bezpečnostní testy: Laxní přístup správců webů

Bezpečnostní firma Sucuri zkontrolovala deset milionů náhodně vybraných webů, včetně internetových obchodů, on-line her a WWW stránek velkých korporací, jako je například Cisco. Při této kontrole nalezla více než 2 000 stránek, které kvůli špatně nakonfigurovanému serveru umožňují útočníkům získat přístup k citlivým stavovým zprávám. Všechny dotčené webové lokality jsou postaveny na často využívaných variantách serveru Apache, u kterých ale vlastník webu zapomněl na omezení přístupu k daným informacím. Podrobnější informace o průzkumu najdete na blogu firmy Sucuri (**blog.sucuri.net**).

Druhá kontrola 100 000 největších internetových stránek, kterou provedla bezpečnostní agentura Rapid7, ukázala, že některé servery dokonce ukládají hesla zákazníků ve formátu prostého textu.

Eurograbber: Odcizeno více než 36 milionů eur

Na první pohled bezpečné internetové bankovnictví se nedávno stalo cílem nebezpečného útoku, který hackerům vynesl obrovské sumy.

Check Point Software Technologies a soukromý nezávislý prodejce řešení prevence podvodů Versafe zveřejnili případovou studii „Eurograbber: Jak bylo ukradeno 36 milionů eur prostřednictvím malwaru". Ve studii je popsán vysoce sofistikovaný útok, při němž byly ze soukromých a firemních účtů po celé Evropě ukradeny miliony eur.

Eurograbber útočil na majitele bankovních účtů pomocí sofistikované kombinace malwaru zaměřeného na osobní počítače i mobilní zařízení. Útočníci propojili malware se svým řídicím serverem a nejprve napadli počítač obětí. Poté infikovali jejich mobilní zařízení, aby mohli zachytit SMS zprávy a obejít tak dvojí bankovní identifikační proces. Díky ukradeným informacím a jednorázovým autorizačním kódům (TAN – transaction authentication number) pak útočníci automaticky převáděli finance v hodnotě 500 až 250 000 eur z účtů obětí na podvodné účty po celé Evropě.

Hlavní charakteristiky útoku:

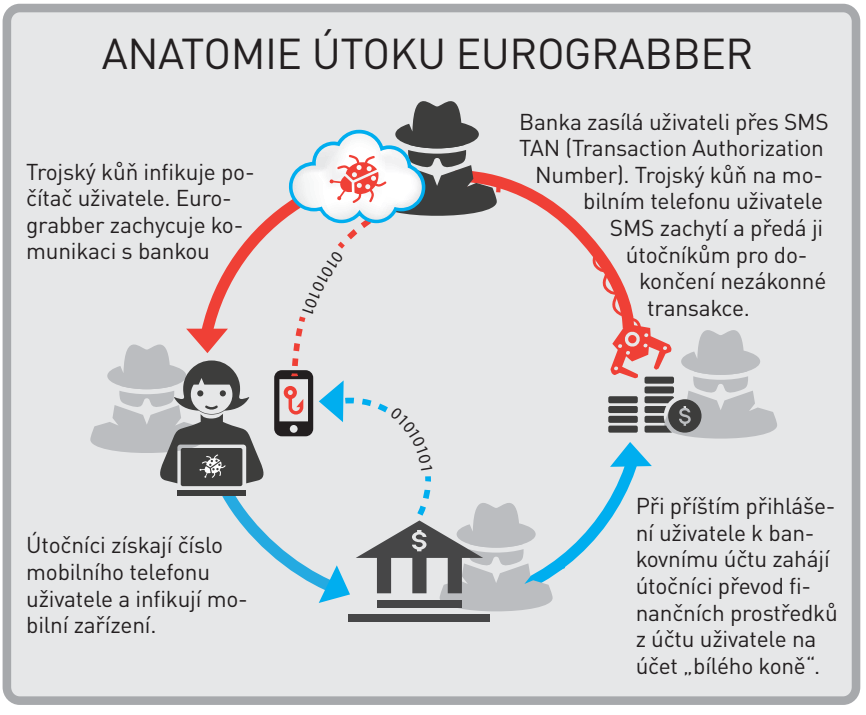
► Dle odhadů bylo z více než 30 000 firemních a soukromých bankovních účtů ukradeno přes 36 milionů eur.

► První útoky byly provedeny v Itálii, rychle se rozšířily do Německa, Holandska a Španělska.

► Krádeže byly provedeny pomocí sofistikovaného malwaru, který byl namířen na počítač a mobilní zařízení bankovních zákazníků.

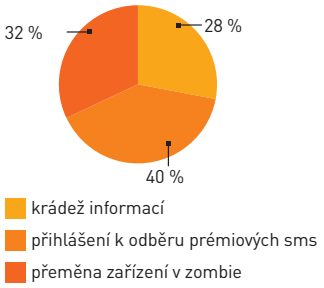
► Útoky byly speciálně zaměřeny na mobilní zařízení Android a BlackBerry, což jen potvrzuje rostoucí trend útoků na zařízení s OS Android.

„Kyberútoky jsou stále sofistikovanější, kreativnější a cílenější, než byly kdy předtím," komentoval Eran Kalige, vedoucí centra bezpečnostních operací ve společnosti Versafe. „Jak jsme mohli vidět u Eurograbberu, kyberzločinci útočili na nejslabší článek, což byli lidé používající daná zařízení. Útočníci použili sofistikované technologie, aby zahájili a automatizovali své útoky a nemohli být sledováni." Případová studie obsahuje popis, jak byl Eurograbber, útočící na tisíce bankovních účtů po celé Evropě, proveden. Celou studii naleznete na **www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf**.

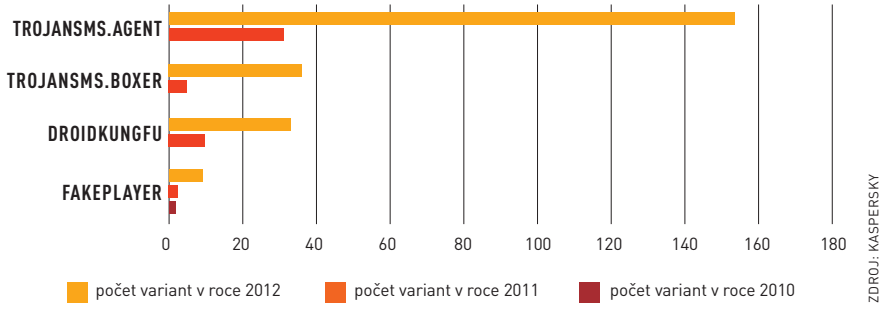


Předpověď firmy Eset: Bezpečnostní hrozby pro rok 2013

DRUHY MOBILNÍHO MALWARU – 2010, 2011 A 2012



POČET VARIANT MALWARU PRO ANDROID – 2010, 2011 A 2012



ZDROJ: KASPERSKY

Na konci každého roku hodnotí antivirová společnost Eset na základě svých výzkumů o bezpečnosti z celého světa uplynulý rok a sestavuje trendy hrozeb pro následující sezonu. Jaké tedy budou největší hrozby? Dočkáme se výrazného nárůstu mobilního malwaru a jeho variant, vzroste šíření škodlivých kódů prostřednictvím webových stránek, zvýší se počet botnetů a útoků na cloudy, které zapříčiní úniky informací.

ZÁSADNÍ NÁRŮST POČTU MOBILNÍHO MALWARU

V roce 2012 jsme mohli pozorovat, jak škodlivé programy vytvořené pro operační systém Android upevňovaly svou pozici jednoho z důležitých nástrojů kyberzločinců. Rychle rostoucí trh s mobilními zařízeními láká útočníky, kteří proto vyvíjejí se zvýšeným úsilím malware zaměřený na chytré telefony a tablety.

Během prvního čtvrtletí roku 2012 zaznamenal podle výzkumné společnosti IDC operační systém Android meziročně růst o 145 % v tržním podílu i prodejích. Agentura Juniper Research navíc odhaduje, že v roce 2013 vzroste počet uživatelů používajících mobilní internetové bankovnictví na svých smartphonech až na 530 milionů. Přitom podle stejné studie jich bylo v roce 2011 jen 300. V kontextu rostoucích prodejů a nových způsobů využití mobilních zařízení a vzhledem k rozmachu škodlivých programů pro mobilní telefony v průběhu roku 2012 se jako hlavní trend pro rok 2013 jeví právě exponenciální nárůst mobilního malwaru. Jednotlivé škodlivé programy pro Android jsou dost odlišné na to, aby měly samostatnou klasifikaci. V roce 2011 (do listopadu) bylo zaznamenáno 52 druhů škodlivých programů pro Android, v porovnání s loňskými 56. Ačkoli se tedy toto číslo v průběhu roku 2012 dramaticky nezměnilo, vše nasvědčuje tomu, že počet zaznamenaných druhů hrozeb se ještě zvýší. Lze ale očekávat, že počet hrozeb pro Android poroste, aniž by se dramaticky zvyšovala jejich pestrost. Bude spíše přibývat množství takřka totožných škodlivých kódů, stejně jako třeba v případě systému Windows. Vezmeme-li v úvahu výše uvedené informace a škodlivé aktivity prováděné na zařízeních na bázi Androidu, je možné klasifikovat následující hlavní typy hrozeb: krádež informací (spyware), distribuce SMS zpráv na prémiová čísla a transformace zařízení v „zombie" (připojení k botnetu). To znamená, že přístup k zařízení spadne do rukou zločincům, kteří ho mohou ovládat na dálku, instalovat do něj další škodlivé kódy, krást data, měnit konfigurační parametry atd.

V roce 2012 se zvýšil také počet upravených variant malwaru pro Android. Jedná se o modifikované verze známých škodlivých programů. Graf zobrazuje čtyři hlavní typy malwaru pro Android a počet jejich variant, které se objevily v letech 2011 a 2012.

ŠÍŘENÍ MALWARU PROSTŘEDNICTVÍM WEBU

V roce 2013 se dočkáme ustálení způsobů, kterými kyberzločinci rozšiřují svůj škodlivý kód. Šíření malwaru prostřednictvím přenosných zařízení jako USB disků se bude snižovat a malware se bude více šířit s využitím mezičlánku, jehož úkolem je přilákání dalších obětí. Mezičlánek je například webový server, který je napaden třetí stranou, a obsahuje počítačové hrozby. Poté, co ovládnou server, vysílají kyberzločinci odkazy lákající uživatele ke stažení malwaru. Zároveň jsou veškeré odcizené informace uloženy právě na těchto napadených serverech, aby se zabránilo zapojení osobních počítačů, které mohou být lépe chráněny a kde může detekce a ochrana před malwarem vyústit ve ztrátu ukradených dat.

BOTNETY NA VZESTUPU

Od roku 2010 si škodlivé programy, navržené tak, aby kradly informace a generovaly příjmy, značně upevnily svoji pozici. V průběhu roku 2011 došlo k výraznému nárůstu botnetů, které se i loni významně rozrůstaly po celém světě. Například červ Dorkbot je jednou z hrozeb, které jsou schopny proměnit váš počítač v zombie.

CLOUD A PŘÍPADY ÚNIKU DAT

Skladování dat v cloudu je další z trendů roku 2012. Podle analytické firmy Gartner má na zvyšující se popularitu tohoto typu skladování dat přímý vliv obliba zařízení vybavených fotoaparátem, jako jsou tablety a smartphony. I když tato technologie umožňuje lidem ukládat data prakticky z jakéhokoli zařízení s přístupem k internetu, jsou tyto služby zároveň oblíbeným terčem počítačových útoků, které mohou ohrozit bezpečnost dat a způsobit únik informací. To se potvrdilo například poté, co útočníci získali přístup k některým účtům služby Dropbox, k nimž byly odjinud ukradeny přihlašovací údaje. I když se nejednalo o selhání samotné služby Dropbox, donutily tyto události jejího provozovatele k vylepšení bezpečnosti. Dalšími službami, které v průběhu roku 2012 rovněž potkaly incidenty ústící v únik informací, byly LinkedIn, Yahoo! nebo Formspring. Letos také musely společnosti vydávající kreditní karty, jako Visa a MasterCard, zveřejnit varování, když jejich systém zaznamenal únik informací. Tento incident ovlivnil celkem 56 455 účtů obou společností, z nichž 876 bylo použito při spáchání nějakého typu podvodu.

Kompletní obsah zprávy připravené výzkumným týmem Eset si můžete přečíst přímo na adrese **go.eset.com/us/resources/white-papers/Trends_for_2013_preview.pdf**.

Více internetového vydírání

„Tento operační systém byl z bezpečnostních důvodů uzamčen“ – s podobnou zprávou se již mnoho on-line uživatelů určitě setkalo.

Jde o typ škodlivého kódu, který označujeme jako ransomware. Ten číhá převážně na podezřelých webových stránkách a počítač nakazí automatickým stažením souboru ihned po navštívení webové stránky nebo například po kliknutí na infikovanou reklamu. Bylo však zaznamenáno i šíření prostřednictvím e-mailu. Hrozba zablokuje počítač oběti a obnoví jeho funkci až po zaplacení výkupného. Počítačoví zločinci k dosažení svého cíle často využívají sociální inženýrství, například zobrazení falešné zprávy, která se vydává za zprávu od místní policie a snaží se oběť přesvědčit k zaplacení pokuty. Zprávy často obsahují varování, jako například: „Prohlíželi jste nedovolené materiály a musíte zaplatit pokutu.“ S ransomwarem se už setkali i čeští uživatelé, kteří obdrželi podvodnou lokalizovanou zprávu s logem Policie ČR. Zajímavé je, že ransomware obvykle účtuje za odemknutí počítače pouze 60 až 200 dolarů. Vzhledem k tomu, že požadované výkupné zaplatí přibližně 3 procenta majitelů nakažených počítačů, si však mohou kyberzločinci měsíčně vydělat až téměř 400 000 dolarů.

NÁRŮST RANSOMWARU

Tým Norton společnosti Symantec zaregistroval v posledních dvou letech dramatický nárůst ransomwaru, který využívají profesionální počítačové gangy. Hrozba zablokuje počítač a požaduje zaplacení výkupného. Další zajímavosti:

► Ransomware se objevil již v roce 2009 v Rusku a východní Evropě. Nyní se výrazně rozšířil i do západní Evropy, USA a mnoha dalších zemí.

► Profesionální kybergangy používají tento inteligentní malware, který v počítači uživatele identifikuje, ve které zemi žije (prostřednictvím IP adresy), a v počítači zobrazí po zablokování zprávu v místním jazyce s logem lokální policie.

► Ransomware kompletně uzamkne zařízení a uživatele informuje, že jediný způsob, jak obnovit funkčnost, je zaplatit pokutu. To zvyšuje šanci, že uživatelé podvodu uvěří a výkupné nakonec zaplatí.

► Vznikají stále nové varianty ransomwaru a kyberzločinci se tak snaží dostat přes zabezpečení počítače. Jedna z nejnebezpečnějších variant dokonce nakazila 500 000 počítačů za pouhých 18 dnů.

► Zprávy se postupně vyvíjejí. Počítačoví zločinci používají různé způsoby, jak donutit uživatele k platbě (například různými metodami sociálního inženýrství). Dřívější varianty používaly na uzamčené obrazovce pornografické obrázky, aby zahanbily uživatele a přiměly jej k zaplacení pokuty. Nyní používají například logo FBI nebo v našem případě logo Policie ČR.

► I když uživatel nakonec výkupné zaplatí, zločinci často funkčnost počítače neobnoví. Jediným spolehlivým způsobem, jak obnovit funkčnost, je odstranit malware.

Podrobnější informace o ransomwaru si můžete přečíst na webu Symantecu. Tým Norton připravil pro uživatele také speciální video, které ukazuje, jak hrozbu jednoduše odstranit: **www.youtube.com/watch?v=_dKBXeoLIFo&feature=youtu.be**.

Hry zdrojem mobilního malwaru

Symantec ve svých bezpečnostních předpovědích pro rok 2013 varoval před madwarem neboli mobilním adwarem, který může ohrozit bezpečnost citlivých údajů, kontaktních informací a informací o zařízení a vše zpřístupnit kyberzločincům. Madware se může do telefonu dostat zcela nenápadně při stahování aplikací a nejčastěji má podobu automaticky otevíraných oken, případně může přidávat ikonky, měnit nastavení prohlížeče nebo shromažďovat osobní údaje.

Je zřejmé, že se předpověď Symantec naplní. Jen za posledních devět měsíců se počet takových aplikací, včetně těch nejagresivnějších forem madwaru, zvýšil o 210 procent. Jelikož informace o zařízení a jeho poloze lze legálně shromažďovat pro reklamní účely, což umožňuje lepší cílení reklamy, očekává Symantec stále větší a větší využití madwaru ve snaze maximalizovat příjmy z mobilní reklamy. To zahrnuje i více agresivní a potenciálně nebezpečné získávání peněz z „bezplatných“ mobilních aplikací.

Kyberzločinci v novém roce nezahálí a snaží se zneužít novoroční období, kdy se tradičně rozesílá velké množství SMS. Symantec detekoval SMS spam botnet, který se zaměřuje na mobilní zařízení se systémem Android a rozesílá nevyžádané SMS zprávy. Zatímco klasické botnety, zaměřené na rozesílání spamu, nepřinášejí nic nového, mobilní technologie otevírají kyberzločincům nové možnosti. Trojský kůň s názvem Android.Pikspam se šíří prostřednictvím SMS zpráv, které propagují bezplatné verze populárních her, případně uživatele informují o nějaké výhře. Pokud nic netušící uživatel klikne na odkaz ve zprávě, stáhne si kromě hry i trojského koně, a zatímco sleduje instalaci hry, na pozadí se instaluje hrozba. Oběti potom vidí pouze ve zprávě propagovanou aplikaci, takže snadno uvěří, že vše je bezpečné. Jakmile je trojský kůň Android. Pikspam aktivní, připojí se k řídicímu serveru a automaticky rozesílá nevyžádané SMS zprávy na telefonní čísla získaná z tohoto serveru.

Tým Norton společnosti Symantec už dříve zaznamenal různé druhy nevyžádaných SMS a podvodů na sociálních sítích. Útoky byly využívány například k partnerskému marketingu. Za propagaci produktů dostávali kyberzločinci provizi z prodejů.

Uživatelé mobilních zařízení musí být ostražití nejenom před madwarem. Stále častěji se objevuje i mobilní malware, který napodobuje starší počítačové hrozby a snaží se ukrást informace o zařízení. Nový malware často jen kopíruje a vylepšuje starší varianty škodlivého kódu. Čím více se lidé zajímají o mobilní technologie, tím více se o ně zajímají i kyberzločinci.

Více informací o Android.Pikspam a SMS spamu najdete na adrese **www.symantec.com/connect/blogs/pikspam-sms-spam-botnet**.