Hackeři pronikají do počítačů jednoduchým trikem

Útočníci přišli na nový trik, jak proniknout do počítače uživatelů: přesvědčí je po telefonu a získají kompletní přístup k jejich systému.

Taková služba skutečně nevypadá špatně: jakmile je počítač s Windows napaden virem, Microsoft uživatele varuje telefonicky – a dokonce mu pomůže při odstraňování malwaru. Chápavější čtenáře ale ihned napadne, že jde o podvod: útočníci se představí jako zaměstnanci Microsoftu a snadno přesvědčí uživatele, aby jim dal přístup do počítače. Nejprve ho po telefonu navigují do systémových nastavení přímo k seznamu událostí systému Windows, který obsahuje celou řadu (obvykle neškodných) výstrah. Podvodníci méně zkušené uživatele přesvědčí, že jde o činnost malwaru, a požádají jej o nainstalování softwaru pro vzdálenou správu, který jim poskytne přístup pro odvirování systému. V reálu do počítače nahrají specializovaný malware, který jim umožní nejen kompletně ovládat počítač uživatele, ale

také nahrávat další specificky zaměřené hrozby – například pro záznam stisknutých kláves nebo pro hledání citlivých dat.

STEJNÝ TRIK ZA PENÍZE

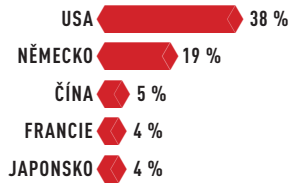
Podobným způsobem funguje i hacker označovaný jako Itman Koool. Nejprve se v komunikačním programu objeví zpráva nabízející zajímavý software za výhodnou cenu: například kancelářský balík od Microsoftu za pouhých 22 eur – s platbou po dodání zboží! Mají-li uživatelé zájem, hacker je požádá o stažení aplikace pro vzdálený přístup (obvykle TeamViewer) a poté o ID a heslo. Pokud mu uživatel oboje poskytne, nainstaluje mu pirátskou verzi softwaru a poté vyžaduje platbu na PayPal účet. To, že se na počítač oběti dostane zároveň i nebezpečný malware, je asi zbytečné dodávat. V současné době jsou tyto útoky omezeny pouze na anglicky mluvící země a obě metody využívají pouze skupiny hackerů v Indii a USA, nicméně podle bezpečnostních expertů je jen otázkou času, než se podobné podvody dostanou i do Evropy. Jejich provedení je totiž příliš snadné a výdělek příliš lákavý.

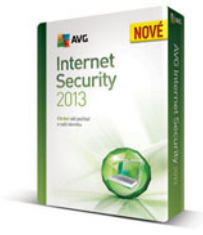
Nebezpečná sleva

Počítačoví zločinci využívají extrémní spořivosti některých uživatelů.

ODKUD POCHÁZÍ SPAM

Podle studie bezpečnostní firmy G data pochází nezanedbatelný podíl e-mailových reklamních sdělení z USA.





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.

Kyberválka: Severní Korea útočí na Jižní Koreu

Podle mluvčího jihokorejského internetového a bezpečnostního úřadu stojí za hackerským útokem na televizní stanice a banky severokorejská zpravodajská služba. Nejprve byl malware rozšířen na různé routery do deseti zemí a poté došlo k nakažení přibližně 48 700 počítačů v Jižní Koreji.

DATOVÉ ÚNIKY MĚSÍCE

VUDU: UKRADENÉ ÚDAJE O ÚČTECH

Krádež dat tak trochu jiným způsobem: 24. března se neznámí pachatelé vloupali do ústředí video-on-demand služby Vudu. Ukradeny byly pevné disky obsahující uživatelská data – tedy konkrétně jméno, datum narození, e-mailovou adresu, údaje o kreditní kartě a heslo. Služba informovala všechny své zákazníky a doporučila jim změnit si uživatelská hesla.

AMAZON S3: VOLNĚ PŘÍSTUPNÉ SOUBORY

Více než 126 miliard souborů – včetně osobních fotografií a přístupových údajů – je volně přístupných na internetovém disku S3 Amazon Cloud. V tomto případě však není na vině hack. Problém je v tom, že velké množství zákazníků služby svá data ukládá špatně a nevhodně nastavuje konfigurační možnosti. Tento fakt zjistila bezpečnostní společnost S7 během kontroly cloudového úložiště.

MICROSOFT: TRAPAS PŘI VYHLAŠOVÁNÍ CEN

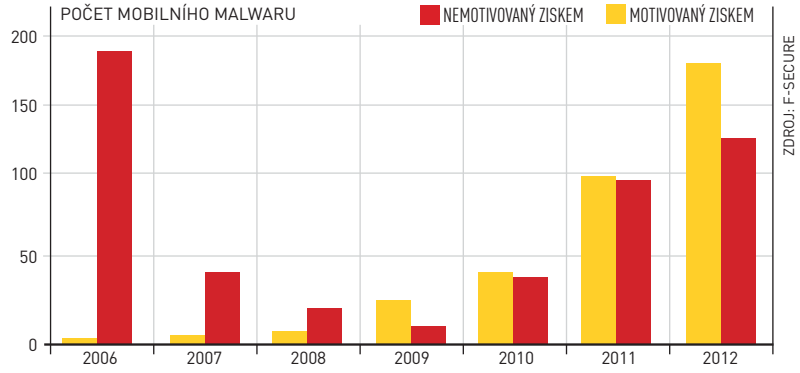
V rámci akce Xbox Entertainment Awards 2013 měl být vybrán nejlepší multimediální obsah roku. Na webových stránkách byl ale omylem zveřejněn seznam obsahující osobní údaje 3 000 hlasujících účastníků. Volně k dispozici bylo například jméno, přezdívka hráče, e-mailové adresy a data narození. Microsoft se účastníkům omluvil a nabídl jim 1 600 „Microsoft bodů" (virtuální platidlo). Není známo, zda se všichni postižení spokojili s tímto dárkem v hodnotě asi 500 Kč.

35 %

EVROPANŮ SI PODLE STUDIE FIRMY SYMANTEC NECHRÁNÍ SVŮJ SMARTPHONE HESLEM

HLAVNÍ DŮVOD PRO VÝVOJ MOBILNÍHO MALWARU: ZISK

Během posledních šesti let se motivace pro rozvoj virů pro smartphony otočila o 180 stupňů. Peníze jsou dnes ta nejdůležitější věc.



Falešné reklamy obsahují malware

Nový trik pro šíření malwaru je jednoduchý, ale účinný: útoky jsou zaměřeny na reklamní systém OpenX, fungující na platformě PHP+MySQL. Do něj hackeři proniknou a vloží škodlivý kód. Ten je automaticky převeden z OpenX serverů reklamních agentur a zveřejněn na známých webových stránkách – nejčastěji zpravodajských a informačních webech.

Velmi nepříjemné: Stačí jen, aby uživatel navštívil stránku se zmanipulovaným reklamním bannerem, a na počítač se mu nainstaluje škodlivý kód. Pro infikování už tedy není nutné na cokoliv klikat.

Malware pro útok na počítač uživatele využívá mezer v Javě, Flashi, Adobe Readeru nebo Internet Exploreru. Cílem malwaru je instalace trojských koní, které se zaměřují na získání přístupových údajů k internetovému bankovnictví.

Zároveň je ale nutné zdůraznit, že tato hrozba funguje pouze u počítačů s operačním systémem Windows a na všechny využívané zranitelnosti jsou již k dispozici opravy. Důrazně tedy uživatelům doporučujeme zkontrolovat si, zda mají na svém počítači nainstalovány všechny aktualizace systému Windows a také nejnovější verze Javy, Flashe a Adobe Readeru.

12 procent všech aplikací pro platformu Android zjišťuje telefonní čísla a odesílá je autorům aplikace.

62 procent uživatelů používá veřejné Wi-Fi sítě. Zároveň se 42 procent z nich obává o svá data.

Přísnější kontrola při nákupu domén

Registrátoři domén by měli provádět přísnější kontroly svých zákazníků. Po téměř dvou letech jednání se na tom dohodli ICANN a registrátoři. Na základě dohody by měli registrátoři ověřit totožnost zákazníka a do databází Whois vyplnit kompletní a správné údaje. To by mělo usnadnit provozovatelům nalezení a odhalení pochybných webových stránek.

200 milionů eur od trojského koně

Pomocí trojského koně Carberp získali počítačoví zločinci z Ukrajiny a Ruska více než 200 milionů eur. Podle informací z ukrajinské zpravodajské služby byly peníze ukradeny z firemních účtů. Do uzávěrky tohoto čísla ale nebylo jasné, jakým způsobem se hackerům podařilo na firemní počítače trojské koně nainstalovat. Skupina podvodníků využívajících tyto trojské koně byla před několika týdny zatčena v Rusku.

Odhalení firmy Eset: Kybernetický útok v Pákistánu

Eset rozkryl a analyzoval cílenou kampaň kybernetických zločinců, kteří se snažili krást citlivé informace z různých organizací, zejména na území Pákistánu. Hrozba se však omezeně šířila i v dalších zemích po celém světě.

V průběhu vyšetřování, které Eset provedl, se zjistilo, že hrozba pochází z Indie a je aktivní již nejméně dva roky. Tento cílený útok využíval šifrovaný podpisový certifikát, vydaný zdánlivě legitimní společností k podpisu škodlivých binárních souborů, čímž se zvyšuje jejich potenciál při dalším šíření. Společnost byla založena v Novém Dillí v Indii a certifikát byl vydán v roce 2011. Malware se šíří v dokumentech posílaných jako e-mailová příloha.

„Identifikovali jsme několik různých dokumentů obsahujících řadu motivů, které by mohly být lákavé pro potenciální příjemce. Jedním z nich měly být indické ozbrojené síly. Nemáme ještě úplně přesné informace, na které konkrétní osoby nebo organizace byly tyto soubory zaměřeny, na základě našeho šetření ale předpokládáme, že mělo jít o lidi a instituce v Pákistánu," řekl Jen-Ian Boutin, výzkumník společnosti Eset.

Jeden z falešných PDF souborů se šířil prostřednictvím samorozbalovacího archivu s názvem „pakistandefencetoindiantopmiltrysecereat.exe" a jeho telemetrická data podle Esetu ukazují, že tato hackerská kampaň postihla ze 79 % právě počítače v Pákistánu.

První infikovaný vektor, který se výrazně rozšířil, zneužíval zranitelnost známou jako CVE–2012–0158. Tato chyba může být zneužita prostřednictvím speciálně upravených dokumentů Microsoft Office a umožňuje spustit libovolný škodlivý kód. Infikované dokumenty byly rozesílány elektronickou poštou a malware se spustil bez vědomí uživatele počítače ve chvíli, kdy byl soubor otevřen. Další malware, který se také šířil e-mailem, se skrýval ve spustitelných souborech, které vypadaly jako dokumenty z Wordu nebo PDF. Aby se autoři vyhnuli podezření, v obou případech se po spuštění zároveň s hrozbou otevřel i falešný dokument. Malware kradl citlivá data z infikovaného počítače a posílal je na servery útočníků. Pro tuto činnost používal hned několik různých technik určených ke krádeži dat, mezi nimi keyloggery, které snímají stisky jednotlivých kláves na počítači a snímky obrazovky pak ukládají do počítače útočníků. Je zajímavé, že ukradené informace z infikovaného počítače se nahrávaly na server útočníka v nešifrované podobě. „Rozhodnutí nepoužívat šifrování je pro nás záhadou. Přidání základního šifrování by bylo snadné a poskytlo by útoku lepší utajení," dodává Jean-Ian Boutin. Kompletní technická analýza je dostupná na odborném serveru WeLiveSecurity.com, platformě společnosti Eset, která obsahuje aktuální informace a analýzy kybernetických hrozeb a užitečné bezpečnostní tipy.

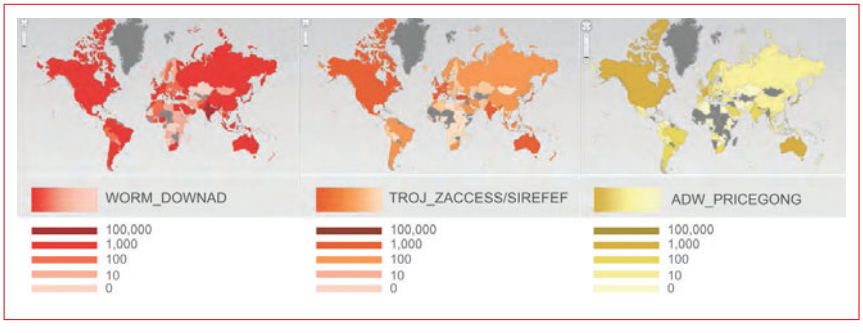
Trend Micro: Hlavní hrozby v roce 2013

Z nových útoků proti platformám Java společnosti Oracle a Flash Player, Acrobat a Reader společnosti Adobe jasně vyplývá, že zranitelnosti se objevují rychleji, než mohou být opraveny pomocí příslušných patchů, a že jsou rychle začleňovány do profesionálních útočných nástrojů typu Black Hole Exploit Kit. „Java je samozřejmě pro útočníky atraktivní i tím, že se jedná o univerzální platformu, ale hlavním důvodem, proč se na ni orientují, jsou její zranitelnosti a její všudypřítomnost," vysvětluje Rik Ferguson, viceprezident Trend Micro pro bezpečnostní výzkum. „Určitě to nebude poslední zero-day zranitelnost v Javě a určitě to není konec rozsáhlého potenciálu, který v současné době Java kyberzločincům nabízí."

ÚTOKY NA JIŽNÍ KOREU

Vysoce cílené útoky, které byly v průběhu letošního března směrovány na Jižní Koreu, potvrzují, že v počítačovém zločinu již nejde výhradně o krádeže, ale že záměrem útoků je ochromit významné sítě prostřednictvím celé řady zajímavých a inovativních metod:

- multiplatformní zaměření, například kombinace Unixu a Linuxu;
- speciální protiopatření vůči instalovanému bezpečnostnímu softwaru;
- převzetí kontroly nad správou softwarových oprav.



Takto si podmaňuje svět trojice nejrozšířenějších malwarů. Mapa zobrazuje počet infikovaných počítačů.

„Vzhledem k charakteru útoků, ke kterým došlo v Jižní Koreji, je pravděpodobné, že hrozba vysoce destruktivních útoků bude i nadále trvat," uvedl Tom Kellermann, viceprezident Trend Micro pro kybernetickou bezpečnost. S každým čtvrtletím nabývají útoky na rozsahu a na cílenosti a potenciální dopady sahají mnohem dál, než je ohrožení osobních dat. Plné znění zprávy najdete na adrese **bit.ly/14AeNk1**.

Kaspersky: Historie spamu se opakuje

Množství nevyžádané elektronické pošty v prvních třech měsících roku 2013 vzrostlo jen nepatrně. Vyplývá to z pravidelné zprávy o stavu spamu bezpečnostní společnosti Kaspersky Lab.

E-maily se zákeřnými přílohami dosáhly 3,3 % a phishingové e-maily se více než čtyřnásobně propadly, na 0,004 %. Spammeři se v období od ledna do března 2013 vrátili ke starým metodám. Znovu si oblíbili takzvaný white text – náhodné kusy textu (v tomto případě části novinových zpráv) v našedlém odstínu na šedém pozadí přidávají do těla e-mailu. Tyto texty jsou od hlavního obsahu reklamy v e-mailu oddělené množstvím zalomení řádků. Útočníci předpokládají, že tyto e-maily spamové filtry považují za newslettery, navíc náhodnost textů dělá každý takový e-mail unikátním, a tedy těžko odhalitelným.

Spammeři navíc začali zkoumat možnosti legálních služeb a využívat je k obcházení spamových filtrů. Škodlivý link je zamaskován hned dvěma legálními způsoby. Nejdříve spammeři využijí Yahoo službu ke zkrácení URL odkazu a tento link ještě zpracují pomocí Google Translate. Ten totiž vytváří přeloženou verzi stránek a poskytuje na ni zvláštní odkaz. Tato metoda maskování vytváří jedinečný odkaz pro každý zaslaný spam a v očích příjemce mu přidává na důvěryhodnosti.

Kybernetičtí zločinci posílající spam využili v prvním čtvrtletí 2013 i dvou velkých zpravodajských událostí – smrti venezuelského prezidenta Huga Chavéze a výměny na papežském postu. Mnoho hromadných e-mailů imitovalo zpravodajský servis stanic BBC nebo CNN a slibovalo senzační fotky a záběry. Na špici zemí, z nichž spamy pocházejí zůstávají Spojené státy. Zajímavé je, na které oblasti tyto spamy cílí – z Číny je spam posílán hlavně do Asie, z USA pak po Severní Americe – znamená to, že většinu spamů je možné považovat za interní. Jihokorejské spamy přitom míří hlavně do Evropy. Plnou verzi zprávy o spamu z prvního čtvrtletí roku 2013 včetně dalších podrobností naleznete na adrese **bit.ly/10G0GHj.**