Tajné služby masově nakupují exploity

Pro zpravodajské služby jsou takové zranitelnosti jednoduchým řešením, jak se beze stop dostat do klíčových cizích systémů.

Jedním z nejdůležitějších zdrojů příjmů pro IT bezpečnostní firmy jsou „zero-day exploity". Tyto slabiny jsou v danou chvíli neznámé i pro velké firmy nebo bezpečnostní společnosti, a tak útočníkům nabízí efektní způsob, jak proniknout ke chráněným datům – za snadného obejití všech bezpečnostních mechanismů.

Hlavními odběrateli těchto „super mezer" jsou tajné služby. To potvrdil v rozhovoru s agenturou Reuters i bývalý pracovník nejmenované tajné služby: „Mojí prací bylo mít vždy na USB disku připravených dvacet pět zero-day zranitelností." Pomocí těchto mezer mohly tajné služby proniknout do cizích systémů bez povšimnutí. K příkladům využití těchto zranitelností patří známé kybernetické zbraně Flame Stuxnet a Duqu. Například jedna z nejnebezpečnějších hrozeb Flame využívala ke svému šíření aktualizační služby Microsoft Update. Díky tomu dokonce někteří experti tipovali, že se tajným službám povedla infiltrace v samotném Redmondu.

Faktem ale zůstává, že hledání softwarových zranitelností je mimořádně lukrativní záležitost: jejich cena se na černém trhu pohybuje (v závislosti na rozsahu slabiny) přibližně od 50 tisíc až po milion amerických dolarů. A na internetu dokonce existují aukce, na kterých se nalezené chyby prodávají.

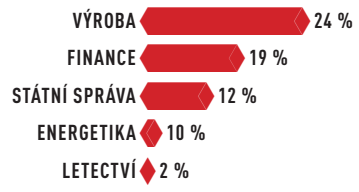
OCHRANA PROTI ZRANITELNOSTEM: TĚŽKÝ BOJ

Pro běžné uživatele je boj se zero-day zranitelnostmi velmi obtížný a nepomůže jim v tom žádný antivir či firewall. Bezpečnostní firmy se na tyto útoky snaží reagovat heuristickými algoritmy, jejich snažení má ale jen nepatrný úspěch. Podle bezpečnostních expertů zranitelností „nulového dne" neustále přibývá a příčinou je i rostoucí konkurence, tlak uživatelů a následná honba za novými verzemi. Softwarové firmy mají kvůli tomu méně času na testování a detekci bezpečnostních mezer.

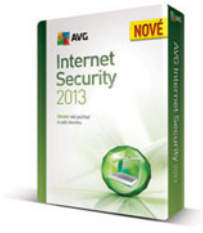
Tajný projekt:
Stuxnet používal zero-day zranitelnosti pro útoky na jaderná zařízení.

CÍLE HACKERŮ

Většinou se hackeři snaží útočit na firmy v oblasti výroby produktů.



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.

Apple: iPad vypíná kardiostimulátory

Čtrnáctiletá Američanka Gianna Chienová by to mohla Applu nepříjemně zavařit. Zjistila totiž, že magnety používané v krytu iPadu jsou tak silné, že pokud je přístroj položen na hrudi, může dokonce vypnout kardiostimulátor. Většina kardiostimulátorů se znova zapne, mnoho modelů těchto zachránců života však zůstane vypnutých, i když iPad s krytem z hrudi odstraníte. Apple se prozatím k celému problému nevyjádřil.

DATOVÉ KRÁDEŽE MĚSÍCE

NAME.COM: ÚDAJE O ZÁKAZNÍCÍCH ODCIZENY

Když byl hacknut americký registrátor domén a poskytovatel webhostingu Name.com, hackeři ukradli e-mailové adresy, hesla a kódované údaje o kreditních kartách. Provozovatelé stránek předpokládali, že útok byl veden na konkrétní účty firemních zákazníků. Společnost doposud nepřišla na to, jak se hackerům podařilo úspěšně proniknout do jejích systémů. Všem zákazníkům ale doporučila z bezpečnostních důvodů zvolit nové heslo.

MĚSTO SCHNEVERDINGEN: ODCIZENY ÚDAJE O OBYVATELSTVU

Kvůli softwarovým problémům ve vlastních systémech převedlo německé město Schneverdingen všechny údaje o obyvatelích, včetně jmen, adres a bankovních dat, k externí softwarové firmě. Tato společnost data uložila v nešifrované podobě na notebook, a ten byl v polovině dubna odcizen. Občané města museli zpřísnit kontrolu svých bankovních účtů a jakékoliv podivné transakce hlásit.

LIVINGSOCIAL: 50 MILIONŮ ÚČTŮ PROZRAZENO

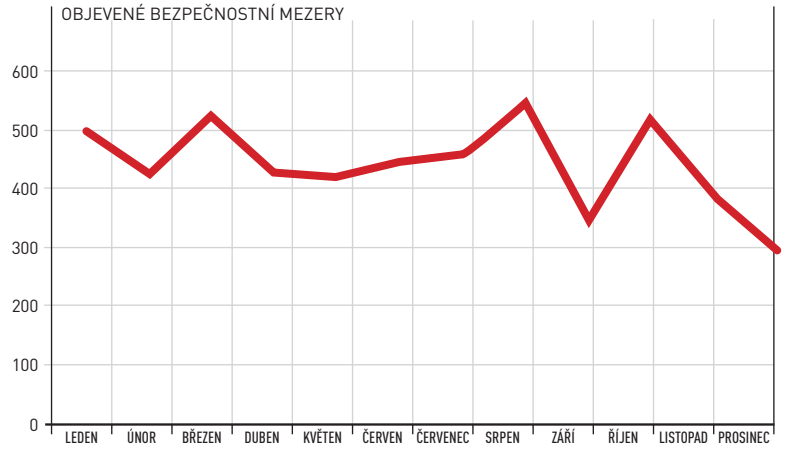
Oběťmi hackerů se stalo 50 milionů zákazníků jednoho z největších slevových portálů světa. Podle interních údajů se hackerům podařilo získat jména, e-mailové adresy, data narození a kryptovaná hesla. Hackeři vypátráni nebyli, dokonce nebyl ani zjištěn způsob, jakým se jim podařilo do systémů proniknout. Podle vyjádření firmy hackeři nezískali data o kreditních kartách zákazníků, ti by ale přesto měli změnit svá hesla.

7,5 %

JE NÁRŮST POČÍTAČOVÉ KRIMINALITY, KE KTERÉMU DOŠLO VE SROVNÁNÍ S LOŇSKÝM ROKEM VE SVĚTĚ.

POČET ZRANITELNOSTÍ KLESÁ

Podle statistik firmy Symantec bylo v průběhu celého roku 2012 registrováno 5 291 chyb. Ve srovnání s předchozím rokem se tento počet mírně zvýšil (2011: 4 989), v současné době je ale trendem spíše mírný pokles.



Antispyware Applu není k ničemu

Firma F-Secure objevila malware pro Apple OS X, který v pravidelných intervalech vytváří screenshoty a snaží se na internetu komunikovat s „command-a-control" serverem. Za normálních okolností takové útoky antispywarový nástroj Applu Gatekeeper blokuje. Nicméně v případě, že vir je certifikován platným ID vývojáře, je tento program Applem považován za bezpečný.

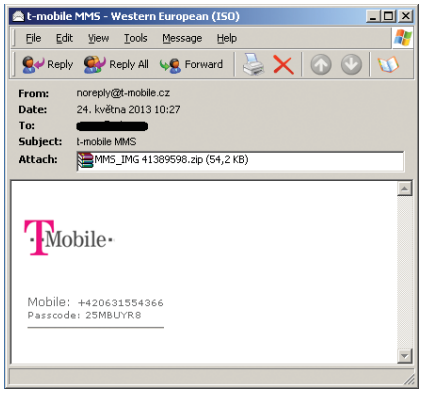
Malware zastaví virový scanner

Bezpečnostní experti z G Data našli nový virus, který dokáže vypnout asi třicet antivirových programů. Pro tento krok potřebuje malware administrátorská práva, ke kterým se dostane pomocí ošklivého triku: malware simuluje chybu pevného disku a zobrazí odpovídající varovné hlášení. Program poté při odstraňování zobrazené chyby požádá o zvýšení práv v systému. Podle G Data je malware v současné době na internetu k dispozici asi za 500 eur. Cílem viru je transformace počítače na dálkově ovládanou zombie, která je součástí botnetu. Malware navíc hledá na disku uživatele důvěrné informace.

Malware v květnu: INF/Autorun sesazen, na vrcholu WIN32/Bundpil

Malware INF/Autorun, který více než rok okupoval vrchol žebříčku nejrozšířenějších celosvětových hrozeb, přenechává trůn svému nástupci. V květnu nahradila INF/Autorun hrozba Win32/Bundpil. Pravidelné statistiky počítačových hrozeb ESET Live Grid, využívající data o malwaru od uživatelů řešení ESET z celého světa, ukazují, že za těmito dvěma škodlivými kódy se umístily hrozby HTML/ScrInject a Win32/Sality. V České republice je ale situace naprosto odlišná. INF/Autorun ani Win32/Bundpil se vůbec nevešly do první desítky a třetí měsíc po sobě je na vrcholu českého žebříčku hrozba HTML/Fraud, a to s podílem 6,94 %. Hrozba Win32/Bundpil se do světové TOP 10 dostala teprve minulý měsíc. V květnu se jí podařilo dokonce obsadit první místo, a to s poměrně výrazným náskokem. Jedná se o červa šířícího se pomocí přenosných médií. Hrozba obsahuje URL adresy, z nichž se pokouší stahovat další soubory. HTML/ScrInject.B je generická detekce webových HTML stránek, obsahující falešný script nebo iframe tag, který automaticky přesměruje uživatele ke stahování škodlivého kódu. Win32/Sality je polymorfní hrozba napadající soubory. Prostřednictvím screenshotů rozesílá informace, stahuje soubory ze vzdálených počítačů a internetu a vypíná a restartuje počítač. HTML/Fraud, který řádí v České republice, je hrozba lákající na výhry v imaginárních soutěžích, většinou o produkty Apple. Uživatel, který poskytne své osobní údaje pro další využití nebo prodej, může očekávat pravidelný přísun prémiových SMS zpráv na svůj mobilní telefon.

V České republice se objevily falešné MMS



AVG Web Threat Research Team zaregistroval v České republice spam šířící se prostřednictvím MMS, které předstírají, že pocházejí od místního mobilního operátora. Na screenshotu je zobrazen případ, ve kterém byl zneužit T-Mobile. Spam má přílohu, kterou je škodlivý spustitelný soubor s dvojitou příponou tvářící se jako obrázek formátu JPG (např. „MMS img 76897644.jpeg.exe"). Většinou se jedná o botnet Zeus, který při stažení kontaktuje svůj C&C (command&control) server a stáhne tak do přístroje další škodlivé soubory. Z technického hlediska má tento malware velmi zajímavé vlastnosti:

1) Po spuštění souboru dojde k dešifrování dat a k zahájení kontroly za účelem prozkoumání daného prostředí, např. ověření identifikačního čísla diskové jednotky, zda neobsahuje emulátory procesoru qemu, virtual, vmware nebo xen (pomocí příkazu HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum\).

2) Pokud jsou úspěšně provedeny všechny potřebné testy a není objeven žádný debugger, provede program v přístroji změny prostřednictvím registrace callback funkce FileIOCompletionRoutine.

3) V dalším kroku se malware pokusí aplikovat kód a zašifrovat data do procesu explorer.exe. Podle dané verze Windows (32b/64b) je poté zvolena jedna ze dvou dostupných metod aplikace malwaru.

Podrobnější informace najdete na webu AVG Web Threats Research Teamu.

Spammeři zneužívají Tumblr a lákají na zázračnou dietu

Popularita mikroblogovací služby Tumblr roste, především mezi mladými uživateli internetu, což přitahuje pozornost spammerů.

Laboratoře Symantec Security Response odhalily spamovou kampaň, která zneužívá v Tumblr funkci Ask, která je podobná oblíbeným funkcím pro komentování a zpětnou vazbu na blozích či jiných sociálních sítích. Tato funkce je ve výchozím nastavení zakázána, ale lze ji povolit v nastavení účtu, a dokonce lze povolit i anonymní komentáře. Spammeři se snaží využít funkce k prodávání svého zboží. Uživatelé tak mohou narazit například na komentáře v angličtině typu: „WOW, zhubnul jsem díky oficiální Tumblr dietě!! Už jste to zkusili také? Podívejte se na adresu..."

Je samozřejmé, že neexistuje nic podobného jako oficiální Tumblr dieta. Místo toho URL uvedené v nevyžádané zprávě vede na webové stránky, které napodobují populární zdravotnický časopis a propagují nové dietní pilulky. Stránka je plná informací o zázračné pilulce a obsahuje i odborné posudky a odkazy na stránky, kde si uživatelé pilulky mohou objednat. Nicméně stránky uvádí, že mají pouze omezené zásoby. Skladové zásoby shodou okolností dojdou ve stejný den, kdy uživatel stránku navštíví. Přestože Symantec si není jistý, zda stránky skutečně posílají originální nebo falešné pilulky na hubnutí, nebo zda je to jen další podvod, doporučuje nenakupovat

Webové stránky podvodného zdravotnického magazínu propagují dietní pilulku.

zboží z podobných nabídek. Tumblr obsahuje funkci „ignorovat", pomocí které uživatelé mohou blokovat účet, IP adresu a/nebo počítač, který zprávu posílá. Celkově tento spam funguje úplně stejně jako jiné spamy spojené s dotazy a komentáři. „Neodpovídejte na podobné podezřelé dotazy, neklikejte na URL odkazy a neuvádějte žádné osobní údaje na neověřených stránkách," doporučuje Patrick Müller z týmu Norton společnosti Symantec. Více informací najdete v příspěvku na blogu společnosti Symantec: **bit.ly/18NovF6**.

Lákavé tragédie

Minulý měsíc byl AVG Web Threats Research Team svědkem náhlého a masivního nárůstu spamových e-mailů lákajících na záběry explozí z bostonského maratonu, které byly distribuovány hned druhý den po události. O necelé dva dny později následovalo totéž po explozi v továrně na hnojiva ve městě Waco. V obou případech spammeři rychle vytvořili spamové e-maily s lákavým předmětem jako „AKTUÁLNĚ – Exploze na bostonském maratonu" či „ZACHYCENO NA KAMEŘE: Exploze v továrně na hnojiva poblíž města Waco v Texasu".

Kliknutí na odkaz v e-mailu přesměruje oběti na internetové stránky nakažené malwarem. Ačkoli mohou stránky navenek vypadat jako legitimní web obsahující slíbené video, obsahují místo toho škodlivý kód ve formátu Exploit Toolkitu vytvořeného tak, aby zjišťoval a vykrádal informace. Krátce po bostonských explozích byly u poskytovatelů DNS narychlo zaregistrovány stovky domén vztahujících se k tragédii, z nichž mnohé byly poté použity k šíření malwaru. Je to krutý způsob, kterým spammeři využívají přirozenou lidskou zvědavost ke svému prospěchu.

Odhalení Kaspersky Lab: Kyberšpionážní operace NetTraveler

Analytici Kaspersky Lab zveřejnili zprávu o nové kampani kybernetické špionáže NetTraveler (Cestovatel po síti). Skupina škodlivých programů infikovala 350 obětí, mezi nimi významné vládní a veřejné instituce ve 40 zemích po celém světě.

Jedná se jak o vládní úřady a ambasády, tak i o ropný průmysl, výzkumná centra, zbrojní firmy i aktivistické organizace. Cílem útoků bylo sledování činnosti obětí a také krádež dat.

Podle zprávy Kaspersky Lab probíhal útok už od roku 2004. Nejvíce aktivity pak analytici zaznamenali v letech 2010 až 2013. Naposledy se útočníci zaměřili na oblasti výzkumu vesmíru, nanotechnologií, energetiky (včetně jaderné), laserů, medicíny a komunikace.

Oběti útočníci napadli pomocí sofistikovaných phishingových e-mailů se škodlivými přílohami – soubory Microsoft Office obsahujícími vysoce zneužitelné zranitelnosti (CVE-2012-0158 a CVE-2010-3333). Přestože Microsoft už dávno vydal jejich záplaty, stále jsou účinnými prostředky cílených útoků.

Podle názvů škodlivých příloh lze odhadnout, jak významné byly cíle útočníků:

- Army Cyber Security Policy 2013.doc (armádní plán kybernetické bezpečnosti)
- Report – Asia Defense Spending Boom.doc (růst výdajů na obranu v Asii)
- Activity Details.doc (detaily činnosti)
- His Holiness the Dalai Lama's visit to Switzerland day 4 (návštěva dalajlamy ve Švýcarsku, den čtvrtý)
- Freedom of Speech.doc (svoboda slova)

Na C&C servery NetTraveleru bylo podle vyšetřování analytiků Kaspersky Lab nahráno více než 22 gigabytů odcizených dat. Mezi nimi byly systémové údaje, záznamy psaní na klávesnici či PDF, excelové a wordové dokumenty a soubory. NetTraveler byl také schopen do počítačů nainstalovat backdoor ve formě malwaru, který kradl citlivé informace, například detaily nastavení aplikací. Ačkoli nebyla prokázána jakákoliv spojitost, NetTraveler si vybral k útoku několik významných obětí, které se staly cílem útoku také kybernetické špionážní kampaně Red October, o níž informovala společnost Kaspersky Lab už v lednu. Kompletní analýzu Kaspersky Lab s detaily útoku NetTraveler naleznete na adrese **bit.ly/17W0ImA**.