Hackeři používají router jako bránu do domácí sítě

Prostřednictvím hacknutí routeru mohou útočníci monitorovat kompletní webový provoz, aniž by oběti tušily, že se něco děje.

Bezpečnostní expert Bogdan Calin nalezl ve firmwaru routerů Arcor, Asus a TP-Link mezeru, kterou lze využít pomocí zmanipulovaného e-mailu. Pokud oběť upravenou zprávu otevře, pak se jeho domácí router automaticky nakonfiguruje takovým způsobem, že je celý síťový provoz přesměrován na server hackera. Nejhorší je, že vzhledem k absenci jakýchkoliv příznaků útoku nemá oběť šanci podvod zaregistrovat. Pro útok využil Bogdan Calin tzv. Cross Site Cross-Site Request Forgery (CSRF): poštovní program se pokusí načíst vložený obrázek, místo toho je ale pomocí příkazu příkazové řádky upraveno DNS nastavení v routeru. Útoku je možné zabránit změnou výchozího hesla.

Chyba byla nalezena i v bezdrátových routerech s označením 4421 a 6431. U nich je dokonce možné získat přístup ke konfiguračnímu rozhraní routeru i z internetu přes webovou službu na portu 7170. V rozhraní routeru může hacker nejen přesměrovat data, ale také získat kompletní záznamy historie internetového provozu. Jediným řešením tohoto problému je aktualizace firmwaru.

Cíl: Routery

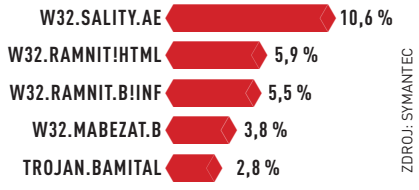
Routery firem Arcor, Asus a TP-Link mohou být snadno napadeny hackery.

VLASTNÍ HESLA ZARUČUJÍ VĚTŠÍ BEZPEČÍ

Prvním krokem, který by měl nový majitel routeru udělat, je změna implicitního hesla, protože hesla jednotlivých výrobců lze na internetu snadno najít. V některých případech ale nestačí jen pouhá změna hesla. U některých modelů routerů od firmy Belkin může být dokonce i Wi-Fi klíč spočítán pomocí MAC adresy routeru. O tom, že podcenění bezpečnosti může mít katastrofální následky, se přesvědčili uživatelé v Brazílii. Zde se hackeři zmocnili více než 4,5 milionu přístrojů firmy Comtrend a přesměrovali uživatele na falešné weby bank.

TOP VIRY V EVROPĚ

Malware W32.Sality.AE, který napadá registry, je zodpovědný za každý desátý útok.



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.

Prohlížeč: Krádeže dat pomocí vyhledávací funkce

Ben Toews, blogger bezpečnostní firmy Neohapsis, objevil zajímavou multiplatformní mezeru prohlížečů. Ta využívá standard v podobě klávesové zkratky [Ctrl] + [F], sloužící pro hledání na WWW stránce. Pokud hacker obsah stránky zmanipuluje, může pomocí JavaScriptu vytvořit falešné okno hledání a získat hledaná data. Hackeři už tuto mezeru využívají, a to tak, že vytvoří falešné weby (prý) obsahující odcizená hesla a uživatele vyzývají, aby si vyhledali, zda je mezi odcizenými i jejich vlastní heslo.

DATOVÉ ÚNIKY MĚSÍCE

NASA: TISÍCE ODCIZENÝCH DATOVÝCH ZÁZNAMŮ

Americké úřady potvrdily, že zaměstnanci americké vesmírné agentury NASA (National Aeronautics and Space Administration) byl odcizen notebook s několika tisíci datovými záznamy o zaměstnancích a dodavatelích. Notebook byl sice chráněn heslem, pevný disk ale nebyl šifrován. Jako poučení z tohoto případu nařídila NASA zaměstnancům od 21. 12. 2012 kompletně šifrovat všechna zařízení obsahující důležitá data.

AGENTURA PRO ATOMOVOU ENERGII IAEA: UNIKLY KONTAKTNÍ ÚDAJE

Hackerská skupina Parastoo se vloupala do komunikačního serveru mezinárodní agentury pro atomovou energii IAEA a odcizila kontaktní údaje vědců, kteří úzce spolupracují s agenturou. Podle tiskové agentury DPA však nejmenovaný zdroj prozradil, že za hackerským útokem nestojí žádná vláda či organizace, protože útok byl proveden jednoduše a poněkud nemotorně.

ŘECKO: UKRADENO 7 MILIONŮ DATOVÝCH ZÁZNAMŮ

Řečtí vyšetřovatelé byli ohromeni, když při prohledávání bytu podezřelého našli sedm milionů datových záznamů. Šlo především o osobní údaje typu ID karty nebo daňová čísla občanů. Únikem dat byly postiženy přibližně dvě třetiny řecké populace. V době uzávěrky doposud nebyla známa původní příčina prohlídky a zdroj odcizených dat.

39 %

VŠECH MALWAROVÝCH ÚTOKŮ JE PROVEDENO POMOCÍ E-MAILU S ODKAZEM NA ZMANIPULOVANÉ WWW STRÁNKY S MALWAREM.

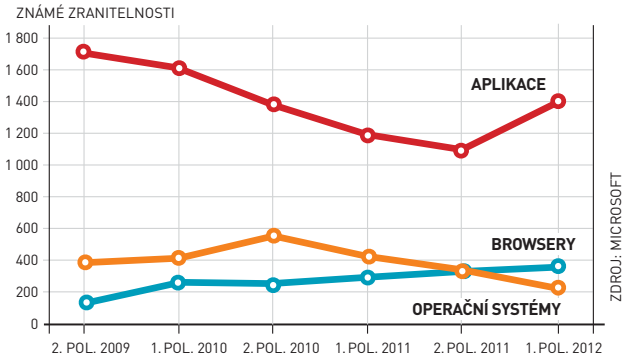
FOTO: THINKSTOCK/HEMERA

Přihlašovací mezera v Instagramu

Bezpečnostní expert Carlos Reventlov objevil slabé místo ve fotografické aplikaci Instagram. Ve verzi pro iOS program komunikuje se serverem pomocí nešifrovaného HTTP spojení. Pokud je síťový provoz ve stejné síti odposlechnut jiným zařízením, útočník získá uživatelské jméno a heslo oběti a přístup k účtu na Instagramu. Prozatím žádné systémové řešení tohoto problému neexistuje, a tak doporučujeme připojovat se k Instagramu pouze přes důvěryhodné Wi-FI sítě.

ÚTOČNÍCI POHRDAJÍ ZRANITELNOSTMI OS

Více než 70 procent všech známých využívaných zranitelností je v současné době v aplikacích. Naopak jen zřídka používají hackeři mezery v prohlížečích. Útoky na operační systém jsou na nejnižší úrovni od roku 2003.



ZDROJ: MICROSOFT

Virus Stuxnet je na webu stále aktivní

V loňském rozhovoru pro Technology Review bezpečnostní expert Eugene Kaspersky upozornil, že od malwaru Stuxnet stále ještě hrozí obrovské nebezpečí. Aktuální zprávy ukazují, že měl pravdu. Na počátku prosince bylo odhaleno, že Stuxnet napadl firemní sítě ropného koncernu Chevron. Další podrobnosti o tomto odhalení ani objem odcizených dat prozatím nebyly zveřejněny.

Síťové tiskárny Samsung zranitelné

Americká IT agentura US-Cert (United States Computer Emergency Readiness Team) vydala varování pro všechny, kdo vlastní síťovou tiskárnu Samsung. Přes hardwarově nastavené hlavní heslo mohou u tiskárny útočníci získat kompletní práva pro čtení a zápis. Zmiňované heslo již skutečně koluje na internetu, a tak majitelům pomůže pouze blokování UDP datového portu 1118 a deaktivace protokolu SNMP v1 a v2.

Kyberšpionážní útok Red October

Odhalení společnosti Kaspersky varuje před aktivitami nebezpečného malwaru útočícího na registry systému.

Společnost Kaspersky Lab upozornila na malware Red October, který se v průběhu nejméně posledních pěti let zaměřoval na diplomatické, vládní a výzkumné organizace. Špionáž cílila především na východní Evropu, země bývalého Sovětského svazu a Střední Asie, oběti lze ale nalézt po celém světě. Hlavním cílem útočníků byl sběr citlivých dokumentů, obsahujících například tajné geopolitické informace, autorizační údaje pro tajné počítačové systémy a údaje z osobních mobilních zařízení i síťových zařízení.

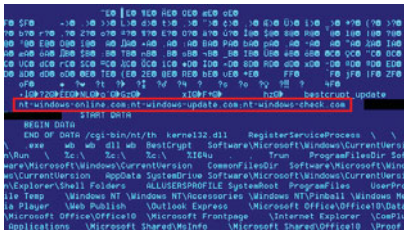
V říjnu 2012 začal tým odborníků společnosti Kaspersky Lab vyšetřovat sérii napadení počítačových sítí zacílených na mezinárodní diplomatické instituce. V rámci tohoto vyšetřování byla odhalena a analyzována rozsáhlá kybernetická špionážní síť. Podle závěrů analýzy Kaspersky Lab je virus Red October (Rudý říjen), zkráceně Rocra, stále aktivní i nyní. Jeho působení lze přitom vystopovat až do roku 2007.

Vedle diplomatických a vládních organizací se kampaň zaměřuje i na výzkumné instituce, energetická a jaderná uskupení, obchodní subjekty či organizace působící v leteckém průmyslu. Útočníci Red October vyvinuli vlastní malware s označením Rocra, který má unikátní modulární architekturu sestávající ze škodlivých rozšíření, modulů pro krádeže informací a trojských koní umožňujících vzdálený neautorizovaný přístup k infikovanému systému (backdoor). Informace, potají odcizené z infikovaných sítí, útočníci nezřídka využívali k získání přístupu do dalších systémů. Například z ukradených autorizačních údajů byl zkompilován seznam, který byl následně využíván vždy, když útočníci potřebovali zjistit bezpečnostní hesla či fráze nutné ke zpřístupnění dalších systémů.

K řízení sítě infikovaných zařízení útočníci zřídili více než 60 internetových domén a také několik serverů v různých zemích, přičemž většina byla umístěna v Německu a Rusku. Analýza, jíž společnost Kaspersky Lab podrobila řídicí (Command & Control) infrastrukturu malwaru Rocra, zjistila, že tyto propojené servery ve skutečnosti fungovaly jako proxy servery, jejichž úlohou bylo maskovat umístění mateřského řídicího serveru. Z napadených systémů byly odcizovány informace v souborech s těmito

RED OCTOBER

Nebezpečný malware zaútočil na cíle v desítkách států...



Analýza obsahu

Každý vzorek malwaru měl v sobě připraven odkaz na tři řídící servery. Celkově jich bylo ale odhaleno více než 60!

koncovkami: txt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau, cif, key, crt, cer, hse, pgp, gpg, xia, xiu, xis, xio, xig, acidcsa, acidsca, aciddsk, acidpvr, acidppr, acidssa. Zvláštní pozornost zaslouží koncovky „acid*“, které, jak se zdá, souvisí s tajným softwarem „Acid Cryptofiler“, jenž využívá hned několik významných organizací včetně Evropské unie a NATO.

INFIKOVÁNÍ OBĚTÍ

Vybrané cíle útočníci infikovali prostřednictvím cílených phishingových e-mailů obsahujících upravený dropper pro infikování trojským koněm. K instalaci malwaru a infikování systému používaly tyto škodlivé e-maily exploity využívající zranitelnosti programů Microsoft Office a Microsoft Excel. Exploity použité v těchto cílených phishingových e-mailech byly vytvořeny jinými útočníky a již dříve byly využity k různým kybernetickým útokům, zaměřeným mimo jiné proti tibetským aktivistům či vojenským cílům a energetickým subjektům v Asii. V dokumentu použitém Rocrou byl změněn pouze zabudovaný spustitelný soubor, který útočníci nahradili vlastním kódem. Zvláštní pozornost náleží jednomu z příkazů, kterým použitý dropper pozměňoval standardní kódování relace příkazového řádku na 1251, což je podmínka nezbytná pro zobrazování cyrilice.

CÍLE ÚTOKŮ

Pro analýzu obětí útoku použila společnost Kaspersky Lab statistiky z cloudové služby Kaspersky Security Network (KSN). Vytvořila také „sinkhole server“, pomocí kterého monitorovala infikované počítače napojené na C2 servery Rocry. Data získaná pomocí obou metod umožnila porovnat a potvrdit zjištěné nálezy. Pomocí dat z KSN bylo detekováno několik set unikátních infikovaných systémů. Cílem byla především velvyslanectví, vládní sítě a organizace a vědecká pracoviště. Převážná část z nich se nachází ve východní Evropě, ale některá z nich jsou v Severní Americe a v západní Evropě, například ve Švýcarsku nebo Lucembursku. Analýza pomocí sinkhole serveru probíhala od 2. listopadu 2012 do 10. ledna 2013 a zaznamenala více než 55 000 připojení z 250 infikovaných IP adres v 39 zemích. Převážná část pocházela ze Švýcarska, Kazachstánu a Řecka.

IDENTIFIKACE ÚTOČNÍKŮ

Analýza registračních údajů řídicích serverů a četných artefaktů zanechaných ve spustitelných souborech zkoumaného malwaru potvrzuje, že útočníci pochází z některé z rusky mluvících zemí. Spustitelné soubory použité útočníky byly navíc až donedávna zcela neznámé a nebyly ani identifikovány odborníky Kaspersky Lab při analýzách dřívějších kybernetických špionážních útoků. Společnost Kaspersky Lab ve spolupráci s mezinárodními organizacemi, policejními orgány a počítačovými bezpečnostními týmy CERT i nadále pokračuje ve vyšetřování operace Rocra, v rámci něhož poskytuje odborné technické znalosti a zdroje. Plné znění výzkumné zprávy odborníků Kaspersky Lab o malwaru Rocra je k dispozici na internetových stránkách Securelist. Kompletní tiskovou zprávu v angličtině najdete na webu Kaspersky.

Předpověď FortiGuard Labs: Šest trendů pro rok 2013

Fortinet zveřejnil předpovědi hrozeb na rok 2013, které vypracovalo jeho výzkumné středisko FortiGuard Labs. Mezi nimi stojí za pozornost šest trendů, na které bychom si v roce 2013 měli dát mimořádný pozor.

1. CÍLENÉ ÚTOKY

APT je zkratkou z anglického „Advanced Persistent Threats", což znamená pokročilé přetrvávající hrozby. Ty jsou charakteristické schopností využívat sofistikované technologie a více metod či vektorů šíření k tomu, aby dosáhly svého cíle a získaly citlivé nebo rovnou tajné informace. Z nedávných událostí lze vysledovat tři škodlivé kódy (Stuxnet, Flame a Gauss), které reprezentují tuto kategorii. Avšak zatímco tyto kódy byly zaměřeny na průmyslové a vládní cíle, v roce 2013 předpokládáme jejich rozšíření i na „domácí sektor" – stanou se hrozbou i pro běžné, byť významnější uživatele. Jejich obětí se mohou stát například ředitelé velkých firem, celebrity nebo političtí představitelé. Je ale nutné upozornit, že ověření této předpovědi bude velmi obtížné. Útočníci se poté, co získají hledané informace, snaží za sebou odstranit stopy i škodlivý kód tak, aby oběť neměla šanci zaregistrovat, že útok proběhl. Navíc ti, kdo zjistí, že se stali cílem podobného útoku, raději o této situaci z pochopitelných důvodů neinformují média.

2. AUTENTIZACE

Bezpečnostní model založený jen na heslech je mrtvý. Dnešní snadno dostupné nástroje dokážou rozbít heslo o délce čtyř nebo pěti znaků během několika minut. Pomocí nových cloudových nástrojů pro dešifrování hesel mohou útočníci vyzkoušet kolem 300 milionů kombinací hesla za pouhých dvacet minut – a za cenu nižší než 20 USD. Kriminálníci tak nyní mohou snadno kompromitovat i silné alfanumerické heslo se speciálními znaky za dobu, kterou potřebujete na oběd. Přihlašovací údaje uložené v zašifrovaných databázích (často napadané skrze webové portály a SQL injektáž) společně s bezdrátovou bezpečností (WPA2) budou populárním terčem útoků za využití právě cloudových služeb. Předpokládáme, že následující rok bude v organizacích ve znamení narůstající implementace dvoufaktorové autorizace pro zaměstnance i klienty. Webové přihlašovací rozhraní bude vyžadovat uživatelské heslo společně se sekundárním heslem, které bude generováno na samostatném bezpečnostním tokenu nebo přijato na mobilní komunikační zařízení.

3. M2M EXPLOITY

Komunikace zařízení-zařízení (Machine-to-Machine, M2M) odkazuje na technologii, která umožňuje jednomu zařízení bezdrátově nebo pomocí klasických sítí komunikovat s dalším zařízením. Může jít o ledničku, která komunikuje s domácím serverem, aby upozornil obyvatele domu, že je na čase koupit mléko a vajíčka; může jít o letištní skener, který pořídí fotografii obličeje osoby a porovná ji s databází známých teroristů; může jít o lékařské zařízení, které reguluje přívod kyslíku pacienta a upozorní lékařský personál, že tepová frekvence klesla pod určitou úroveň. Zatímco praktické technologické možnosti M2M jsou úžasné a mají v mnoha případech potenciál odstranit lidskou chybu, mnoho otazníků přetrvává ohledně jejich bezpečnosti. Předpokládáme, že v příštím roce zaznamenáme první pokusy o napadení systémů M2M, velmi pravděpodobně na platformě spojené s národní bezpečností, jako je například objekt určený pro vývoj zbraní.

4. HROZBY PRO SANDBOXY

Sandboxy (virtuálně uzavřená a izolovaná prostředí) jsou využívány v bezpečnostních technologiích k oddělení programů a aplikací tak, aby případný škodlivý kód nemohl přejít z jednoho procesu (např. prohlížeče dokumentů) do druhého (např. operačního systému). K tomuto schématu už přistoupilo několik výrobců (například Adobe) a je velmi pravděpodobné, že se k nim brzy přidají další. S tím, jak se tato technologie stává čím dál tím rozšířenější, útočníci přirozeně začínají řešit i to, jak ji obejít. Středisko FortiGuard Labs už zaznamenalo několik exploitů, které se dokázaly dostat z virtuálního stroje (VM, Virtual Machine) a sandboxu. Šlo například o zranitelnost Adobe Reader X. Předpokládáme, že se v příštím roce setkáme s kódy, které budou navržené k obejití izolovaných prostředí užívaných bezpečnostními aplikacemi a mobilními zařízeními.

5. MEZIPLATFORMOVÉ BOTNETY

V roce 2012 analyzovala laboratoř FortiGuard Labs mobilní botnety, jako je například Zitmo. Proto můžeme konstatovat, že i v mobilním prostředí mají většinu stejných vlastností a funkcionalit jako tradiční botnety pro PC. Díky tomuto sdílení vlastností mezi platformami očekáváme, že v roce 2013 spatří světlo světa nové formy útoků odepření služby DDoS (Distributed Denial of Service), které souběžně využijí PC i mobilní zařízení. Pro představu: Infikované mobilní zařízení a PC budou sdílet stejné ovládací a řídicí servery a protokol útoku a budou schopné zaútočit společně v jednom okamžiku. Díky tomu se možnosti botnetů znásobí.

6. MOBILNÍ ŠKODLIVÉ KÓDY

Dnešní škodlivé kódy jsou vytvářeny pro mobilní zařízení stejně jako pro stolní počítače a notebooky. Dosud přitom byla hlavním cílem pozornosti útočníků právě platforma klasických počítačů, a to proto, že jich bylo tolik a že jsou na světě přece jen delší čas. To se však může již brzy změnit. Laboratoř FortiGuard Labs dnes eviduje a sleduje zhruba padesát tisíc vzorků škodlivých kódů pro mobilní zařízení (pro PC jsou jich řádově miliony). Výzkumníci přitom pozorují významný nárůst v objemu mobilních škodlivých kódů a předpokládají, že tento trend bude v příštím roce ještě dramatičtější, mimo jiné i kvůli tomu, že se dnes prodává více mobilních telefonů než notebooků nebo stolních PC.

Jak se zdá, sandbox už v blízké budoucnosti nebude znamenat dokonalé bezpečí.