Ani „bezpečná“ hesla nemusí chránit dostatečně

V ohrožení jsou dokonce i hesla obsahující speciální symboly a čísla. K jejich dešifrování stačí jen několik triků.

Při téměř každé krádeži dat z komerčních webů se útočníkům podaří získat hesla uživatelů. Jelikož se obvykle jedná o šifrovaná data, ve většině případů firmy a instituce věří v jejich bezpečnost a incident zlehčují.

V běžných počítačích jsou kódovaná hesla uložena jako tzv. hash a pro hackera není příliš obtížné je převést zpět na aktuální heslo. U hesla se šesti znaky potřebují útočníci na útok hrubou silou jen několik hodin. "Pokud heslo obsahuje více než šest znaků, doba trvání dekódování exponenciálně roste," říká Robert Graham, generální ředitel společnosti Errata Security. Proto pro prolamování dlouhých hesel používají útočníci seznamy slov, která hesla nejčastěji využívají. Hackeři počítají například i s využitím speciálních symbolů, například „h@llo“ však není pro odhalení příliš obtížné.

V testu provedeném bezpečnostním expertem Jeremim Gosneyem bylo tímto způsobem možné dešifrovat 90 procent získaných hesel.

POMŮŽE JEDINĚ TREZOR SPRÁVCE HESEL A LHANÍ

Proti nebezpečí takovýchto slovníkových útoků jsou chráněni pouze ti, kdo používají heslo se zcela nezávisle zadanými speciálními znaky a čísly. Nevýhodou ale je, že takováto hesla se špatně pamatují, a i proto je uživatelé neradi používají. Řešením je tedy využívání správců hesel – v ideálním případě pro všechny mobilní a desktopové operační systémy (jako například 1Password z webu **agilebits.com**), které mohou být automaticky synchronizovány.

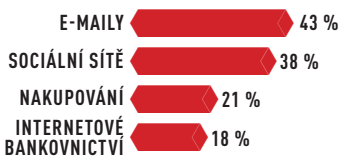
Slabým místem celé řady služeb je navíc možnost resetování hesla, obvykle chráněná jen primitivní otázkou typu „Jaká je vaše oblíbená barva“ – což je ve věku sociálních sítí a exhibicionistických uživatelů hodně slabá ochrana. Řešením tak může být lhaní. Zvolte si méně obvyklou kontrolní otázku a místo logické odpovědi si vymyslete něco neobvyklého.

Správce hesel

Nejlepším místem pro vaše hesla je elektronický trezor.

CO DĚLAJÍ UŽIVATELÉ NA BEZPLATNÝCH WI-FI SÍTÍCH?

Lukrativní příležitost pro hackery: Na nechráněných bezdrátových sítích provádí bankovní transakce téměř každý pátý uživatel.



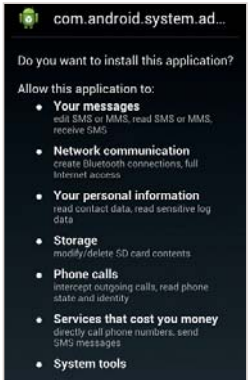
ZDROJ: SYMANTEC

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.

Android: Nesmazatelný trojský kůň

Odborníci společnosti Kaspersky objevili v OS Android trojského koně, který je vnořen tak hluboko v systému, že jakmile je nainstalován na mobilní telefon, nemůže být odstraněn. Aby se vyhnul detekci antivirovým programem, využívá dvě bezpečnostní mezery, díky kterým může běžet zcela v pozadí systému. Vývojáři z firmy Kaspersky již pracují na rutině umožňující jeho odstranění.



DATOVÉ ÚNIKY MĚSÍCE

DRUPAL.ORG: E-MAILOVÉ ADRESY ODCIZENY

Redakční systém Drupal byl napaden hackery. Pachatelům se podařilo získat balík uživatelských dat se záznamy o více než 935 000 uživatelích. Podle Drupalu byla odcizena uživatelská jména, e-mailové adresy, informace týkající se zemí a hashe hesel. Společnost všechna hesla obnovila – zpočátku však byly Drupal servery přetíženy. Zaslání e-mailu, pomocí něhož bylo heslo resetováno, trvalo skoro hodinu.

WEBHOSTING HETZNER: ZKOPÍROVÁNY ÚDAJE O ÚČTECH

O tom, že bezpečný nemusí být ani oblíbený a zavedený hosting, se přesvědčili zákazníci německého webhostingu Hetzner. Podle společnosti byl pomocí backdooru nainstalován na server rootkit, který umožnil instalaci sledovacího programu. Podle sdělení společnosti byla odcizena kompletní data, a to včetně informací, jako jsou údaje o kreditní kartě nebo hesla. Společnost své zákazníky o útoku okamžitě informovala.

MOBILNÍ POSKYTOVATEL TERRACOM: ÚDAJE O ZÁKAZNÍCÍCH NA GOOGLU

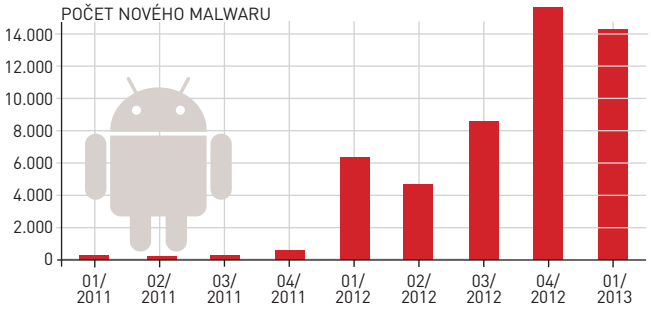
TerraCom, jeden z amerických poskytovatelů mobilních služeb, uložil data zákazníků na nezabezpečený a volně přístupný server. Proto mohla být data narození a čísla sociálního pojištění snadno nalezena, například pomocí Googlu.

2 500

KYBERNETICKÝM ÚTOKŮM BYLY V ROCE 2012 VYSTAVENY SERVERY NATO. ŽÁDNÝ PRÝ NEBYL ÚSPĚŠNÝ.

MASIVNÍ NÁRŮST VIRŮ PRO ANDROID

Na konci roku 2011 existovalo pro Android jen několik set verzí nového malwaru. V prvním čtvrtletí roku 2013 ohrožovalo OS Googlu už téměř 14 000 nových virů.



ZDROJ: MCAFEE

SMS ochrana na Twitteru prolomena

Twitter představil dvoufaktorové zabezpečení přihlášení – pomocí SMS zprávy. To na první pohled vypadá jako dobrá zpráva, odborníci z bezpečnostní firmy F-Secure však našli způsob, jak tento bezpečnostní prvek zneužít. SMS se totiž používají i k zasílání a odesílání tweetů, takže pokud zná útočník číslo oběti, může pomocí SMS spoofingu dvoufaktorové zabezpečení zakázat. Podrobnější informace najdete na webu firmy F-Secure (**bit.ly/16egGJS**).

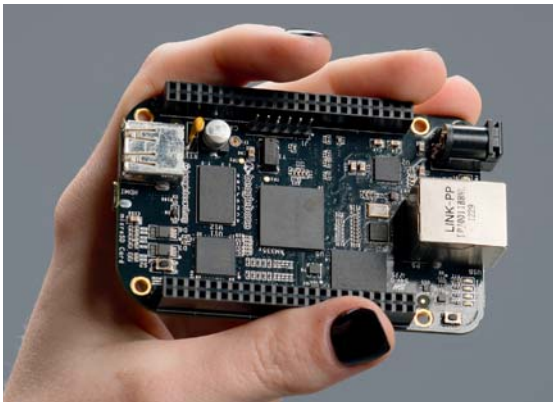
Microsoft a FBI odpojily botnety

Microsoft ve spolupráci s různými finančními společnostmi a FBI podnikl úspěšné kroky proti 1 462 botnetům. Vyřazení sítí osvobodilo 5 milionů dálkově infikovaných a ovládaných počítačů. Škody způsobené malwarem se odhadují na půl miliardy amerických dolarů. Operace s kódovým označením B54 byla zahájena již v roce 2012, několik měsíců ale trvalo dekódování sítí.

Zranitelné disky NAS

V NAS systémech firmy QNAP existuje nebezpečná mezera, díky které mohou hackeři provádět libovolný příkaz s právy administrátora. Pokud je systém připojen k internetu, mohou útočníci i na dálku převzít kontrolu nad celým systémem. Výrobce na problém okamžitě reagoval a nabízí potřebné záplaty v rámci aktualizace firmwaru.

Každé zařízení s iOS může být hacknuto za jednu minutu



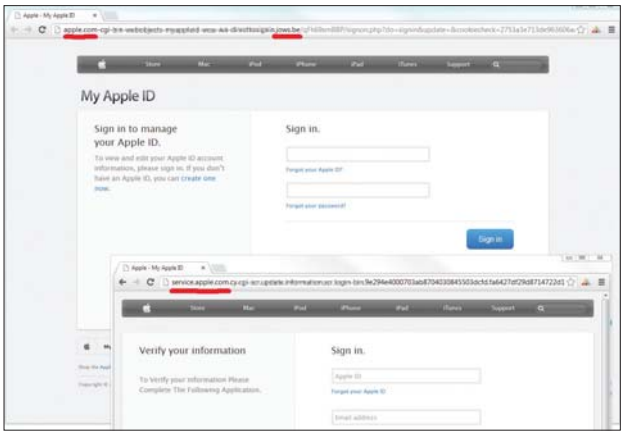
Bezpečnostním výzkumníkům z Georgia Institute of Technology se podařilo zmanipulovat nabíječku baterií pro zařízení s Apple iOS takovým způsobem, že získali přístup s plnými administrátorskými právy ke smartphonům a tabletům, které jsou k ní připojeny.

Oběť se o útoku nemá šanci dozvědět, protože útok probíhá zcela na pozadí. Hackeři mohou později také na pozadí instalovat do zařízení další aplikace, i když přístroj již není připojen nabíjecím kabelem. Nabíječka baterií není příliš velká – má rozměry kreditní karty. Vědci již dokonce pracují na ještě menší verzi. Jak přesně tato technologie funguje, to prý odborníci prozradí na hackerské konferenci Black Hat.

7500 dolarů vyplatí Google každému, kdo objeví cross site scripting mezeru na jeho serverech.

10 % všech mobilních uživatelů se podle průzkumu společnosti Symantec již stalo oběťmi trestných činů.

Cíle phishingu: Zákazníci Applu



Společnost Kaspersky Lab zaznamenala dramatický nárůst phishingových útoků s cílem odcizit údaje uživatelů produktů Applu.

Phishingové stránky imitují oficiální webovou stránku **apple.com**. Pomocí odcizených přihlašovacích údajů se kybernetičtí zločinci snaží získat osobní data uživatelů a čísla jejich kreditních karet uložených na účtech služeb iTunes a iCloud. Od ledna 2012 do května 2013 odhalila cloudová služba Kaspersky Security Network (KSN) denně v průměru 200 000 případů, v nichž byli uživatelé přesměrováváni na phishingové stránky. Produkty Kaspersky Lab tyto pokusy o podvod odhalily, zastavily a nahlásily do systému. V porovnání s rokem 2011 je to významný nárůst – tehdy bylo denně v průměru detekováno jen 1 000 pokusů o phishing. Dle analýzy Kaspersky Lab lze vypozorovat určitou fluktuaci útoků. Nárůst pokusů o phishing, někdy v češtině označovaný jako rhybaření, byl zaznamenán často v souvislosti s velkou událostí společnosti Apple. Například 6. prosince 2012, ihned po spuštění obchodu iTunes v 56 nových zemích, zablokovaly produkty Kaspersky Lab rekordních více než 900 000 pokusů o phishing v jediném dni.

Hlavní metodou kybernetických zločinců jsou falešné e-maily, které se tváří jako zprávy od zákaznické služby Apple Support s falešnou adresou odesílatele typu **services@apple.com**. Běžně uživatele vyzývají k tomu, aby na uvedeném odkazu zadali své přihlašovací údaje. Vzhled těchto e-mailů je propracován do nejmenších detailů, aby uživatele snadno zmátl. V jiném případě se tyto e-maily snaží adresáty přesvědčit k zadání čísel kreditních karet s tím, že je třeba údaje aktualizovat.

Jedním ze způsobů, jak rozlišit pravou a falešnou stránku, je soustředit se na políčko s webovou adresou. Ta sice může mít v textu výraz „apple.com", ten je ale zabalený do dalšího neautentického textu. Pokud se však uživatelé přihlašují například v prohlížeči Safari na iPhonu či iPadu, nemusí se jim webová adresa zobrazit celá. Důležité je proto zkontrolovat i odesílatele falešného e-mailu lákajícího na falešný odkaz. Apple nabízí dvoustupňový proces autentizace před přihlášením ve formě zaslání čtyřmístného kódu na předem určené zařízení uživatele. To zabraňuje například neautorizovaným nákupům na Apple ID napadeného uživatele.

Tyto metody nicméně nezabrání kybernetickým zločincům ve zneužití odcizených čísel kreditních karet. Analytici Kaspersky Lab proto zdůrazňují, že je nutné být obezřetný a společně s využitím bezpečnostních nástrojů jako Kaspersky Security for Mac se řídit zejména zdravým rozumem. Více informací o phishingových útocích na zákazníky Applu je k dispozici na stránkách Securelist.com (**bit.ly/12dyWux**).

Spamu opět přibývá

Ve druhé čtvrtině roku 2013 se podíl spamu na celkové e-mailové komunikaci zvýšil v porovnání s předchozím čtvrtletím o 4,2 % na 70,7 %. Vyplývá to z analýzy spamu za Q2 2013 společnosti Kaspersky Lab. Mnoho z e-mailů se škodlivou přílohou byly určeny firemním uživatelům. Tyto e-maily se tvářily jako automatické odpovědi, například oznámení o nedoručení, nebo jako oznámení o doručení e-mailu, faxu či skenu. Jejich odesílatelé spoléhají na to, že zaměstnanci nebudou mít čas zabývat se detaily zprávy a budou ji považovat za pravou, otevřou přílohu a škodlivý program tak spustí.

Jedním z neobvyklých druhů škodlivých příloh za minulé čtvrtletí byla elektronická přání. V minulosti se objevovala kolem hlavních svátků, ale v poslední době jejich množství ubývalo. Nicméně v období letošního dubna až června zaznamenali analytici Kaspersky Lab jejich nárůst – tentokrát se útočníci zaměřili na americkou firmu vyrábějící slavnostní přání Hallmark.

Elektronická přání ale nebyla jediným návratem zapomenuté taktiky spammerů. Tak jako v první čtvrtině roku i v té druhé využívali takzvaný „white text" – náhodný text (v tomto případě části novinových zpráv o Hugo Chávezovi, bostonském maratonu nebo konfliktu v Koreji) v našedlém odstínu na šedém pozadí, který přidávají do těla e-mailu. Tyto texty jsou od hlavního obsahu v e-mailu oddělené množstvím zalomení řádků. Útočníci předpokládají, že tyto e-maily spamové filtry považují za newslettery, a navíc náhodnost textů dělá každý takový e-mail unikátním a tedy těžko odhalitelným.

Stále méně se spammeři spoléhají jen na lidský faktor a na to, že jim uživatelé omylem sdělí svá data. Místo toho stále častěji posílají škodlivé e-maily poseté trojskými koni a odcizují uživatelské údaje a hesla, včetně těch k internetovému bankovnictví.

Kaspersky v Praze

Naše hlavní město navštívil Eugene Kaspersky, majitel a generální ředitel Kaspersky Lab. V rámci setkání s novináři například varoval před hrozbou kyberterorismu, která podle něj může zasáhnout téměř kohokoliv. V své vtipné prezentaci také upozornil na případ zavirování mezinárodní kosmické stanice ISS nebo riziko útoků na průmyslová a energetická zařízení.

Eset objevil trojské koně zneužívající známý anonymizační systém Tor

Antivirová společnost Eset objevila v červenci dva trojské koně, jejichž řídicí servery maskují svou skutečnou polohu pomocí známého anonymizačního systému Tor. Řídicí servery útočníků k tomu používají službu Tor Hidden Services (skryté služby), díky čemuž dokážou utajit skutečné umístění serveru, a tím pádem významně zkomplikovat jeho odhalení, zablokování a odstranění bezpečnostními výzkumníky či policejními složkami.

V případě trojanu Win32/Atrax.A jde zřejmě o úplně nový škodlivý kód, který byl vytvořen v červenci. Nasvědčují tomu informace ze souboru, které udávají jeho vznik. K infikování počítačů používá e-mailem šířenou přílohu, která se maskuje za PDF soubor. Ve skutečnosti však jde o downloader, jehož úkolem je připojit se na stránku **kundenservice-paypal.com**, ze které do počítače stáhne trojského koně Atrax.A. Stránka **kundenservice-paypal.com** nijak nesouvisí se známým platebním systémem PayPal a byla zaregistrována také v červenci. Eset však nevylučuje, že Atrax.A používá ke svému šíření i jiné metody.

Trojský kůň se pokouší skrýt nejen svůj řídicí server, ale i sebe – například před bezpečnostními výzkumníky. Atrax.A průběžně zjišťuje, zda právě není analyzován – taková analýza většinou probíhá na virtuálním počítači, a právě těm se Atrax.A vyhýbá. Plug-iny stažené z řídicího serveru potom ukládá trojský kůň na disk v zašifrované formě. K šifrování používá jedinečné identifikátory přístroje DigitalProductID a MachineGUID. „To znamená, že když nám takto zašifrovaný plug-in pošle někdo k analýze, bez těchto identifikátorů ho nedokážeme rozšifrovat, a tedy analyzovat," říká Petr Šnajdr, bezpečnostní odborník společnosti Eset. Při analýze našel Eset dva odlišné typy plug-inů. První z nakaženého počítače odesílá vyplněné on-line formuláře, do kterých uživatel vpisuje například osobní údaje. Druhý zase z počítače krade hesla. „Tor Hidden Service protokol je účinným způsobem, jak vytvořit anonymní spojení s řídicím serverem, pro krádeže velkých objemů dat je však příliš pomalý," dodává k odesílání údajů Petr Šnajdr.

V průběhu zkoumání tohoto trojského koně se Esetu podařilo získat přístup k řídicímu panelu serveru, který obsahuje nápis Atrax (viz obrázek). Na základě nápisu na této vstupní bráně se Eset rozhodl pojmenovat trojana jako **Win32/Atrax.A**.

Podvodníci nabízejí předražené domény po telefonu

Živnostníci a malé firmy bývají často terčem spekulantů, kteří se snaží dobře připraveným telefonickým rozhovorem přimět podnikatele ke koupi domény s názvem jeho firmy. Podvodníci využívají zákonné možnosti uzavřít smlouvu po telefonu a není-li oslovený subjekt dostatečně obezřetný, může dojít k závazku finančního plnění, aniž by došlo k reálnému podpisu smlouvy.

Podvodníci jsou zkušenými manipulátory a argumentují tím, že se doménu nesoucí název firmy podnikatele pokouší koupit jiný subjekt. Prodejce má velkorysou nabídku na odkup domény a tím dává živnostníkovi možnost doménu získat dříve než fiktivní zájemce. Podnikatel slovně souhlasí s registrací domény, aniž by tušil, že se tím zavazuje k zaplacení vysoké částky, která se značně liší od běžné ceny registrace domén.