Současné smartphony bez ochrany heslem

Heslo uživatele představuje významnou bezpečnostní funkci smartphonů, v případě iOS a Androidu však příliš bezpečí nezaručí.

Chrání soukromé e-maily, textové zprávy, citlivé poznámky a vše ostatní, co bylo uloženo do smartphonu: zamykací heslo, kterým disponují zařízení se systémem Android a iOS. U obou systémů je však v současné době možné tuto důležitou ochranu obejít. V případě Applu to není nic nového: nedávno byla zveřejněna slabina využívající nouzové funkce alarmu k průniku do systému. Ta umožňuje externím uživatelům zobrazit adresář telefonu, získat přístup k VoiceBoxu, nebo dokonce volat.

Mezera ovlivňující mobil Samsung Galaxy SIII s OS Android je ještě škodlivější. Pomocí speciálního triku lze zařízení aktivovat a poté získat přístup k datům, která byla uložena v zařízení. A jak získat přístup k zamčenému telefonu? Stačí zavolat na číslo v nouzových kontaktech, ukončit ho pomocí tlačítka Domů a stisknout tlačítko napájení. V praxi je u smartphonů Samsung kvůli jiné chybě dokonce možné odhalit i skutečné heslo.

Zranitelný
Zabezpečení heslem na Galaxy SIII a všech iOS zařízeních je zbytečné.

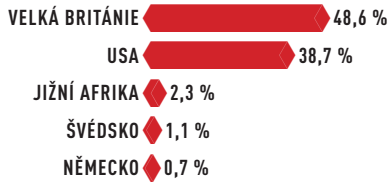
VÝROBCI NEDODÁVAJÍ ŽÁDNÉ ZÁPLATY

Kromě ukládání textu SMS zpráv funkce automatických oprav v korejském mobilu také ukládá hesla, která byla zadána do přístroje. Díky tomu smartphone navrhuje celé heslo, jakmile byly zadány první tři znaky. Nicméně ani Samsung, Google nebo Apple nenabízí žádné opravy nebezpečných zranitelností. V případě Applu existuje mezera již více než měsíc – což je pro zlomyslné hackery spousta času – a v době uzávěrky stále nebylo jasné, kdy bude mezera opravena. Od mluvčí firmy Trudy Mullerové jsme obdrželi pouze následující komentář: „Této chyby jsme si vědomi. Bude odstraněna při následné aktualizaci softwaru."

Dokud k ní ale nedojde, bude ochrana heslem na dvou oblíbených smartphonech téměř zbytečná.

ODKUD PŘICHÁZÍ VIRY V E-MAILECH

Velká Británie předstihla USA a stala se největším světovým distributorem virů. Zpoza Lamanšského průlivu pochází téměř 50 % světového malwaru.



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.

Adobe: Google detekoval chyby ve Flashi

Záplaty, které firma Adobe uvolnila v rámci březnových oprav, odstranily pouze tři ze čtyř mezer ve Flashi. Tým Adobe zapracoval na zranitelnostech, na které ho upozornil Google. Další důležitá mezera, která byla zjištěna v rámci soutěže hackerů Pwn20wn, dosud nebyla Adobe opravena. Nepříjemné je, že všechny zmiňované zranitelnosti umožňují hackerům na zasaženém počítači spuštění libovolného kódu.

DATOVÉ ÚNIKY MĚSÍCE

AVAST: UNIKLA DATA 16 000 ZÁKAZNÍKŮ

Avadas, německý prodejce firmy Avast, byl napaden tureckým hackerem, kterému se podařilo ukrást data 16 000 zákazníků. Ukradené údaje, které obsahují adresy, čísla bankovních účtů, data narození a hesla, se již objevily na internetu. Postiženi byli všichni zákazníci, kteří se přihlásili na web Avadasu před 10. březnem 2013. Bezpečnostní mezera již byla opravena.

MICROSOFT: KRÁDEŽ UŽIVATELSKÝCH ÚČTŮ

Čínská hackerská skupina Evil Shadow Team pronikla na indický Microsoft Store a ukradla přihlašovací údaje a hesla uživatelů, kteří v internetovém obchodě společnosti Microsoft nakupovali. Poté, co hackeři údaje ukradli, zveřejnili skutečnost, že údaje byly uloženy ve formátu prostého textu.

EVERNOTE: ODCIZENA UŽIVATELSKÁ JMÉNA

Bezpečnostní systémy on-line poznámkové služby Evernote byly úspěšně napadeny útočníky, kteří ukradli uživatelská jména a e-mailové adresy. V důsledku toho se služba Evernote rozhodla provést celosvětový reset hesel.

LIVINGSOCIAL: ODCIZENA DATA 50 MILIONŮ UŽIVATELŮ

Údaje zákazníků jednoho z největších slevových serverů světa LivingSocial byly odcizeny skupinou neznámých hackerů. Podle informací provozovatele se hackerům nepodařilo získat čísla kreditních karet ani podobné citlivé informace.

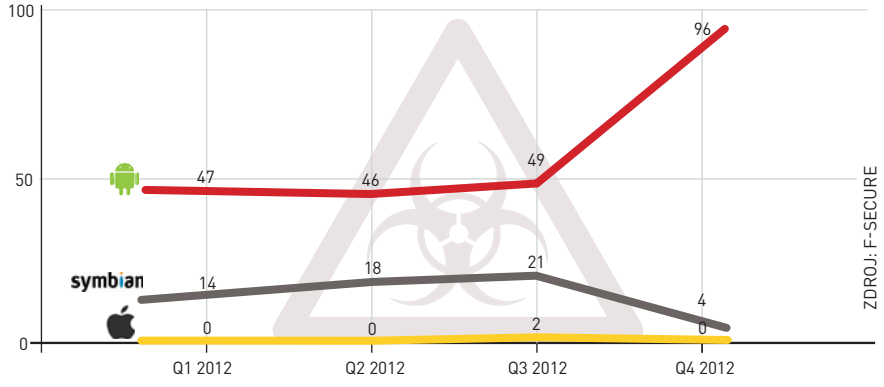
600 %

ČINÍ PODLE ANALÝZY FIRMY WEBSENSE NÁRŮST POČTU HACKNUTÝCH STRÁNEK V ROCE 2012.

ANDROID POD PALBOU

Za pouhé čtvrté čtvrtletí loňského roku bylo objeveno 96 nových rodin malwaru spojených s operačním systémem Android. Pro iOS se neobjevil žádný nový malware.

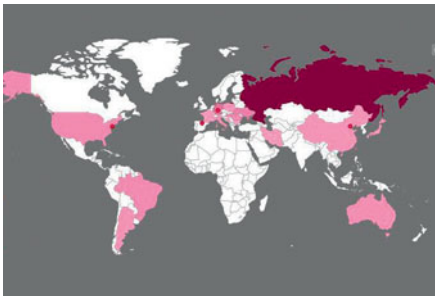
NOVÉ RODINY MALWARU



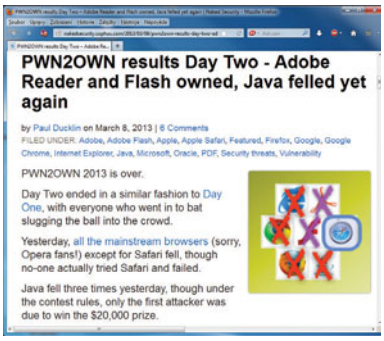
ZDROJ: F-SECURE

Útoky v reálném čase

Německý Telekom nabídl pomocí webové stránky **sicherheitstacho.eu** zobrazení útoků na sítě po celém světě v reálném čase. Data pochází ze sta tzv. honeypots – počítačových systémů, které mají pouze jeden jediný cíl: být napaden hackery. Kromě identifikace země původu a druhu útoku web nabízí i přehled hlavních pěti způsobů útoku a celkový počet útoků (viz obrázek vpravo).



ÚTOKY ZA POSLEDNÍ MĚSÍC



Peněžní ceny za nejlepší hacky

Na hackerské akci Pwn2Own, která se konala v březnu, předvedli hackeři své útoky a získali peněžní ceny za nejúspěšnější hacky. Hlavní cena, kterou představovala částka 100 000 dolarů, byla udělena dvěma týmům. První hackl aplikaci Internet Explorer 10 ve verzi, která byla používána na tabletech Surface Pro, zatímco druhý pronikl do nejnovější verze Sandboxu Chrome. V rámci soutěže byly také hacknuty Adobe Reader, Firefox a Java. Pro nalezení těchto chyb stačily týmům pouhé dva dny.

Útočníci crackli přes internet tiskárny HP

Německý bezpečnostní výzkumník Christoph von Wittich identifikoval slabé místo v síťové komunikaci používané tiskárnami Hewlett-Packard. Otevřený telnet port může být totiž použit k ovládání zařízení přes internet. A co je horší, útočník pro přístup k telnet konzoli nepotřebuje ani heslo, protože konzole byla navržena pouze pro použití v lokální síti. Útočník díky tomu může například použít konzoli pro deaktivaci šifrování dat používaného u služby HP ePrint a zobrazit nešifrované verze všech ePrint hesel.

DoS útok pak může být použit k přetížení tiskárny. Tento nedostatek se týká následujících modelů: P1102w, P1606dn, M1212nf MFP, M1213nf MFP, M1214nfh MFP, M1216nfh, M1217nfw, M1218nfs, M1219nf a CP1025nw. Společnost HP již vydala aktualizaci firmwaru, která slabinu opravuje.

Fotbaloví fanoušci cílem útoků

Počítačoví zločinci využívají ke svým útokům téměř každou příležitost. Tentokrát jsou i díky blížícímu se konci sezóny na mušce milovníci fotbalu.

Phisheři (kyberzločinci používající podvodné techniky pro vylákání citlivých dat od uživatelů internetu) se stále častěji zaměřují na fotbalové fanoušky. Tým Norton společnosti Symantec zaznamenal řadu různých phishingových útoků spojených s fotbalovými tématy už v roce 2012. Kyberzločinci navíc prokázali svou snahu zneužít mistrovství světa v roce 2014 v Brazílii, fotbalové celebrity i fotbalové kluby. Jako příklady mohou sloužit phishingové útoky zneužívající Lionela Messiho a FC Barcelona. Podvodníci pochopili, že když se zaměří na fotbalové osobnosti s obrovskou základnou fanoušků, získají tak možnost zaútočit na velké množství cílů a zvýší své šance na získání citlivých uživatelských dat.
V dubnu 2013 tento trend pokračoval a phisheři používali stejnou strategii. Phishingové stránky byly zatím ve francouzštině, je však jen otázkou času, než začnou vznikat lokalizované a důmyslnější varianty útoků.

Phishingové stránky lákají na Lionela Messiho, FC Barcelonu nebo Cristiana Ronalda a nabádají uživatele k zadání přihlašovacích údajů do Facebooku pro více informací. Stránky obsahují snímky populárních fotbalistů a snaží se tak vytvořit falešný dojem, že jde o jejich oficiální facebookové profily. Na některých falešných stránkách je uvedeno „První sociální síť na světě". Uživatelé jsou vyzváni k zadání svých přihlašovacích údajů do Facebooku, aby bylo možné se ke stránce připojit. Následně jsou přesměrováni na legitimní fanouškovské stránky, aby byla vytvořena iluze platného přihlášení. Pokud se uživatelé stali obětí phishingu a zadali své přihlašovací údaje, phisheři se prostřednictvím nich mohou dostat k dalším důležitým informacím a využít je ke krádeži identity.

Patrick Müller z týmu Norton společnosti Symantec proto doporučuje pro ochranu před phishingovými útoky dodržovat na internetu osvědčené postupy:
► Neklikat na podezřelé odkazy v e-mailech.
► Být opatrní při klikání na lákavé odkazy na sociálních sítích.
► Neposkytovat žádné citlivé osobní informace v e-mailové komunikaci.
► Nezadávat osobní informace ve vyskakovacích oknech.
► Ujistit se před zadáním osobních nebo finančních údajů, že webová stránka je šifrována a obsahuje SSL certifikát – adresní řádek by měl být zelený a měl by obsahovat text https a ikonku zámku.
► Používat komplexní bezpečnostní software.

Odhalení firem Eset a Sucuri: Zranitelné servery Apache

Výzkumníci antivirové společnosti Eset analyzují společně s bezpečnostní firmou Sucuri novou hrozbu, která zasáhla tisíce Apache webserverů, což jsou celosvětově nejznámější a nejpoužívanější webové servery. Hrozbou je backdoor, který dokáže obejít určité mechanismy a tím poskytuje útočníkovi přístup k operačnímu systému napadených serverů.

Tento vyspělý backdoor využívají útočníci k přesměrování internetového uživatele na škodlivé stránky infikované Blackhole exploit sadou. „Jde o známou a rozšířenou sadu, která k infikování systému uživatele během jeho návštěvy postižené webové stránky používá známé, ale i nové exploity, které jsou součástí Blackholu," vysvětluje Righard Zwienenberg, výzkumník společnosti Eset.

Výzkumníci tento backdoor pojmenovali Linux/Cdorked.A. Jedná se o nejdůmyslnější Apache backdoor, s jakým se dosud setkali. Do dnešního dne identifikovali zásluhou technologie Eset LiveGrid stovky kompromitovaných webových serverů. „Kromě modifikovaného „httpd" souboru (Apache webserveru) po sobě Linux/Cdorked.A na harddisku nezanechává žádné stopy. Všechny informace související s backdoorem jsou uloženy ve sdílené paměti serveru, kvůli čemuž je jeho detekce a analýza mnohem komplikovanější," říká Pierre-Marc Bureau, výzkumník společnosti Eset.

Hrozba je zajímavá tím, že nekontaktuje svůj vzdálený řídicí server aktivně, ale akceptuje příkazy z jakéhokoli serveru. Tyto příkazy přicházejí formou standardního HTTP protokolu, i když o nich tento server nevede žádný záznam.

Další zajímavostí je, že backdoor jen zřídka uživatelům prezentuje škodlivý kód. Každému návštěvníkovi se snaží škodlivý obsah zobrazit jen jednou,

čímž snižuje možnost svého odhalení. Taktéž se snaží nezobrazovat podvržený obsah na stránkách, které souvisejí s administrací příslušného webového serveru (například když si webmaster prohlíží stránky s nastaveními).

Eset doporučuje systémovým administrátorům, aby zkontrolovali své servery a ověřili, zda nejsou touto hrozbou postiženy. Při této příležitosti vytvořila společnost bezplatný nástroj, který administrátorům pomůže při detekci této hrozby (dump_cdorked_config.py). Celá technická analýza je k dispozici na blogu společnosti Eset s názvem **welivesecurity.com**. Další informace o Linux/Cdorked.A najdete na blogu společnosti Sucuri.

avast! Premier

Společnost ALWIL Trade nyní nabízí nový produkt avast! Premier, určený především malým firmám. Ten poskytuje zákazníkům mnohem více funkcí než řešení Internet Security. Je kombinací antiviru, antispywaru, antispamu a firewallu. Navíc obsahuje zcela nové funkce, například skartovač dat pro trvalé smazání citlivých dat z disku nebo vylepšenou funkci pro vzdálený přístup, se kterou je možné se automaticky připojit k PC odkudkoli a kdykoli. Nový Software Updater nabízí přehled všech zastaralých programů, včetně těch, které vyžadují bezpečnostní opravu.

MEZI NOVÉ FUNKCE PATŘÍ NAPŘÍKLAD:

► **avast! Software Updater:** Podporuje automatické aktualizace. Udržuje vaše programy aktuální, včetně bezpečnostních záplat. Již nemusíte pro zjištění nové verze aktivně kontrolovat každý program zvlášť. Software Updater nabízí přehled všech zastaralých programů na vašem počítači a pomůže tak odhalit případná bezpečnostní rizika.

► **avast! Skartovač dat:** Nabízí možnost zcela nevratně mazat diskové oddíly i jednotlivé soubory s citlivými daty (osobní data, licence k softwaru atd.).

Data nemohou být později obnovena žádným nástrojem na obnovu dat. Soubory můžete smazat zvolením některé z bezpečných metod: Náhodný přepis, DoD nebo Gutmann.

► **avast! AccessAnywhere:** Umožňuje nastavit i několik počítačů, které budete vzdáleně ovládat. Máte tak stálý přístup ke svému PC, bez ohledu na to, kde se právě nacházíte.

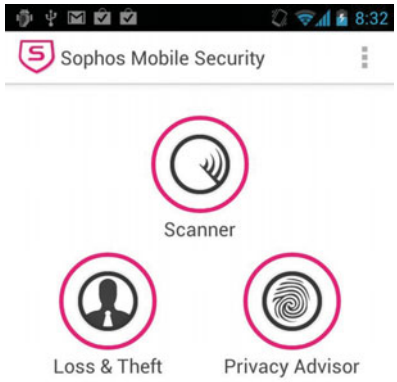
► **avast! Čištění prohlížečů (Browser cleanup):** Umožňuje ve webových prohlížečích spravovat a odstranit všechny otravné panely nástrojů a zásuvné moduly, které si uživatel často nainstaluje nevědomě s jinými aplikacemi. Browser cleanup navíc využívá hodnocení komunity uživatelů avast! a dává informace o tom, jestli je doplněk spolehlivý, nespolehlivý, nebo dokonce škodlivý.

► **Optimalizace pro dotykové obrazovky:** Zjednodušuje pomocí uživatelského rozhraní s velkými tlačítky použití programů avast! na dotykových zařízeních s Windows 8.

Sophos Mobile Security 2.5

Sophos představil nejnovější verzi volně dostupného bezpečnostního řešení pro Android Sophos Mobile Security 2.5. Nová verze softwaru obsahuje i filtr proti spamu pro textové zprávy a hovory.

Filtrovací pravidla umí zablokovat podezřelá telefonní čísla a hovory se skrytým ID, stejně jako textové zprávy s potenciálně nebezpečnými URL. Všechny příchozí hovory nebo textové zprávy jsou prověřeny aplikací Spam-Protection. Blokované hovory a textové zprávy jsou automaticky uloženy do karanténní složky, odkud mohou být v případě potřeby opět vyzvednuty. Nová verze Sophos Mobile Security je volně ke stažení na Google Play: **play.google.com/store/apps/details?id=com.sophos.smsec**.



Jarní epidemie šířená přes Skype

Odborníci Kaspersky Lab odhalili dva kybernetické útoky šířící se přes Skype. V obou případech využívají kybernetičtí zločinci sociálního inženýrství k nalákání uživatelů na škodlivé odkazy s příslibem zajímavé fotografie nebo videa. K distribuci těchto odkazů jsou využívány napadené nebo podvodné účty na Skypu.

První útok se objevil už na začátku března, nicméně i nyní zaznamenali analytici Kaspersky Lab 2,7 kliknutí na tento škodlivý odkaz za sekundu, tedy 10 tisíc za hodinu. Většina napadených pocházela z Ruska, Ukrajiny, Bulharska, Číny, Tchaj-wanu a Itálie. Při zkoumání kódu nahraného do počítače obětí nalezli experti zmínku „Bitcoin wallet" (peněženka bitcoinů, virtuální peněžní měny). Nedávno byl odhalen nový trojský kůň. Uživatelé byli vyzváni k tomu, aby klikali na odkaz, místo toho byl ale na jejich počítač instalován škodlivý software, který kybernetickým zločincům generuje právě bitcoiny. Tato měna pak může být směněna za skutečnou měnu nebo využita k placení za reálné produkty či služby na internetu. Během prvního dne spuštění útoku (4. dubna) na odkaz klikalo 2 000 uživatelů za hodinu – zejména v Itálii, Rusku, Polsku, Španělsku, Německu, na Kostarice a na Ukrajině.

Podle odborníků Kaspersky Lab není náhoda, že se kybernetický útok objevil v době, kdy směnný kurz bitcoinu dosáhl historické výše – 132 USD za bitcoin (v roce 2011 to bylo jen necelé dva dolary). „Undergroundová fóra jsou plná nabídek na prodej či nákup za bitcoiny. S touto měnou lze zaplatit drogy, zbraně, 0-day zranitelnosti, trojské koně a viry," říká analytik Kaspersky Lab Sergej Ložkin. Tyto transakce je přitom těžké vystopovat. K takzvané „těžbě" bitcoinů, složitým operacím, je třeba stále více hardwaru, proto se kybernetičtí zločinci snaží napadnout nic netušící uživatele Skypu. Na jejich počítače instalují těžební modul a jejich hardwarové zdroje využívají k činnosti botnetu, který se může stát zdrojem příjmů.

Kaspersky Lab doporučuje dodržet základní pravidla ochrany před podobnými útoky – pokud vám na Skype (nebo jinou síť) přijde podezřelý odkaz od známého, je možné, že byl jeho účet a počítač napaden. Kliknutí na každý odkaz proto pečlivě zvažujte. Aktualizujte pravidelně antivirovou ochranu, operační systém i aplikace a využívejte bezpečný prohlížeč. Samozřejmostí jsou silná hesla a hlavně selský rozum.