Indie a Ekvádor – i tam mohou skončit vaše peníze

Moderní platební karty jsou díky celé řadě bezpečnostních prvků bezpečné. I toto na první pohled logické tvrzení má však své výjimky.

Naprostá většina platebních karet vydávaných v České republice má kromě magnetického proužku i takzvaný EMV čip. Ten zajišťuje, že při použití karty a schválení nákupu bude nutné zadat PIN kód. Toto pravidlo ale bohužel platí pouze v České republice a civilizované Evropě. V USA či ve zbytku světa terminály s podporou EMV téměř nenajdete – zde se pro platby stále využívá samotný magnetický proužek. A právě toho zneužívají mezinárodní gangy podvodníků, kteří z odcizených karet vysávají finance v zahraničí. Princip je jednoduchý: prostřednictvím nějakého triku podvodníci zkopírují kartu a pomocí duplikátu s magnetickým proužkem nakoupí v obchodech v zemích třetího světa. Banky sice mají určité algoritmy hlídající transakce, ty ale nejsou neomylné.

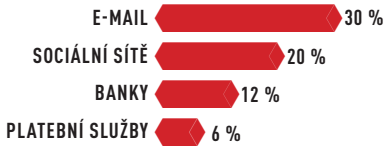
ZE SUPERMARKETU DO EKVÁDORU A INDIE

O neuvěřitelné drzosti a šikovnosti podvodníků se mohli nedávno přesvědčit v sousedním Německu. Do jednoho z velkých supermarketů v Dolním Sasku se v noci vloupali zloději a do pokladen nainstalovali skryté snímače s Bluetooth modulem. Než bylo zařízení odhaleno, získali podvodníci kopie více než 800 kreditních karet se všemi údaji. S těmito daty zločinci pomocí kopií karet získali peníze z bankomatů v Ekvádoru a Indii. V nich totiž (na rozdíl například od Evropy) nejsou EMV čipy podporovány a pro výběr peněz stačí magnetický proužek a znalost PIN kódu.

Dříve putovalo nezanedbatelné množství karet i do USA (kde se také používají především magnetické proužky), ale od konce dubna 2013 USA nabízí tzv. EMV posun odpovědnosti. U některých karet (viz Wikipedie EMV – **bit.ly/bAGp0p**) jsou za škodu z falešné transakce zodpovědní obchodníci, kteří nepodporují technologii EMV. To ale zdaleka neplatí pro země jako Indie nebo Ekvádor, takže podvodníci své kopie kreditních karet využívají v těchto zemích.

KTERÉ STRÁNKY JSOU NEJČASTĚJI FALEŠNÉ?

Pokud chtějí hackeři získat soukromé informace, lákají nejčastěji své oběti na kopie webových stránek freemailových služeb.



ZDROJ: KASPERSKY

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.

D-Link: Chyba v routerech a kamerách

Kvůli kritické mezeře, kterou najdete v celé řadě routerů a webových kamer D-Link, může útočník na těchto zařízeních spustit libovolný příkaz. K tomuto účelu například útočníci používají pro router zmanipulovaný UPnP požadavek. Pro většinu chybou postiženého hardwaru už D-Link nabízí aktualizace firmwaru, jedinou výjimkou jsou modely DIR-300 Rev B a DIR-865. I pro ně by ale měly být příslušné aktualizace firmwaru brzy k dispozici.

DATOVÉ ÚNIKY MĚSÍCE

FACEBOOK: MILIONY DAT O UŽIVATELÍCH ZTRACENY

Kvůli chybě v softwaru byly volně k dispozici informace z účtů na Facebooku, které jsou normálně uživatelem pro veřejnost zablokovány. Z profilů tak bylo možné stáhnout například e-mailové adresy nebo telefonní čísla. Podle mluvčího Facebooku bylo chybou ovlivněno méně než jedno procento uživatelů – tedy přibližně šest milionů lidí.

UBISOFT: UKRADENA DATA UŽIVATELŮ

V polovině června se neznámým osobám podařilo získat přístup na server výrobce her, firmy Ubisoft. Zde mohli útočníci získat jména zákazníků, jejich e-mailové adresy a hesla. Podle Ubisoftu prý nebyly odcizeny informace o kreditních kartách nebo finančních transakcích. Firma nesdělila informace o počtu napadených uživatelských účtů, ale doporučila všem zákazníkům změnit si svá hesla.

HOSTING ZAP: VŠECHNA DATA ODCIZENA

Firma ZAP, nabízející hosting, se stala obětí komplikovaného hackerského útoku. Kvůli zadním vrátkům získali útočníci přístup ke všem zákaznickým datům uloženým na hostingu. Útočníci tato data zkopírovali a původní verzi dat na serverech firmy ZAP odstranili. Vzhledem k tomu, že data byla automaticky obnovena ze starší zálohy, firma nemá žádné podrobnější stopy o identitě útočníků nebo jejich motivech.

10 %

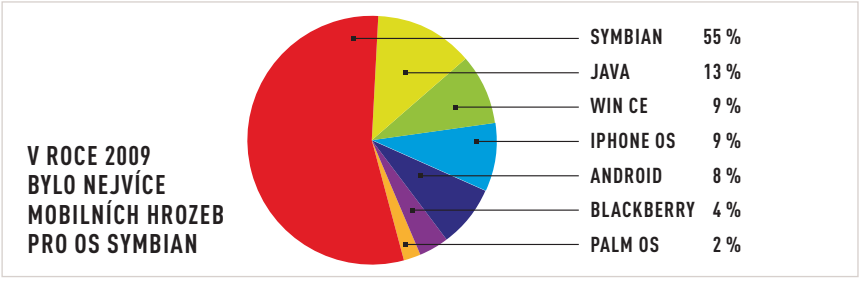
ZEMÍ JE ZDROJEM 56 % VŠECH PHISHINGOVÝCH ÚTOKŮ.

PLACENÁ INZERCE

Přineste si své vlastní problémy

Zpráva společnosti Fortinet konstatuje třicetiprocentní nárůst škodlivých kódů pro mobilní zařízení během půl roku: 1 300 nových vzorků denně!

Společnost Fortinet zveřejnila závěry svého výzkumu bezpečnostních hrozeb v období od 1. ledna do 31. července letošního roku. „Dle naší laboratoře FortiGuard Labs došlo v uplynulém období ke třicetiprocentnímu nárůstu škodlivých kódů pro mobilní zařízení," uvádí Vladimír Brož, country manager společnosti Fortinet. „Výzkumníci aktuálně analyzují 1 300 nových kusů malwaru denně a sledují přes 300 unikátních skupin malwaru pro Android. Celkově pak přes čtvrt milionu unikátních kusů malwaru." Kompletní zprávu najdete na webu Fortinetu na adrese **bit.ly/145XhYC.**



MOBILNÍ HROZBY

Fenomén BYOD (Bring Your Own Device, „přines si své vlastní zařízení") má pro podnikání mnoho přínosů. K nejvýznamnějším patří zvýšená efektivita práce a nárůst produktivity. Je tu ale i odvrácená strana BYOD: nekontrolovaná zařízení zaměstnanců se mohou stát rizikem pro celou podnikovou síť. „Před třemi lety nebyly škodlivé kódy pro mobilní zařízení vážnější hrozbou pro uživatele ani pro organizace. Většina malwaru napadajícího tehdy chytré telefony a tablety nebyla ničím jiným než obtěžující variantou viru Cabir nebo podvodným softwarem, který se pokoušel bez vědomí uživatele odesílat zpoplatněné SMS nebo měnil podobu ikon," uvádí analytik mobilních virových hrozeb Axelle Apvrille. „Jenže mobilní zařízení vyspěla a kyberzločinci pochopili jejich potenciál."

NA POČÁTKU BYL SYMBIAN

V roce 2009 většina škodlivých kódů pro mobilní zařízení směřovala na Symbian OS. Systémy jako iOS nebo Android byly tehdy na trhu relativně nové. Kromě toho byla většina těchto škodlivých kódů vytvořena ve východní Evropě a Číně. Tedy tam, kde měl Symbian širokou uživatelskou základnu. V roce 2013 došlo k dramatické změně v podobě útoků proti mobilním zařízením. Poté, co většina výrobců přijala Android od Googlu jako hlavní systém, došlo k velkému rozšíření chytrých telefonů. Zařízení s Androidem jsou k dispozici na každém trhu a ve všech cenových kategoriích. Od neuvěřitelně levných až po extrémně vybavená a na funkce bohatá monstra. Možnosti mobilních zařízení pak rozšiřuje ohromná lavina aplikací, které přinášejí neomezené množství funkcionalit. Kyberzločinci proto vnímají tuto platformu jako novou příležitost k podnikání.

NOVÉ I STARÉ HROZBY

Zajímavé je, že ačkoliv pro platformy Ruby on Rails, Java, Adobe Acrobat či Apache přichází čím dál více aktualizací, specialisté z FortiGuard Labs konstatují, že útočníci se stále zaměřují na staré zranitelnosti. Například v lednu 2013 bylo oznámeno, že kritická chyba v infrastruktuře Ruby on Rails umožňuje vzdáleným útočníkům spustit kód na obsluhovaném webovém serveru. Ruby on Rails (RoR) je infrastruktura pro webové aplikace pro programovací jazyk Ruby. Jednoduše řečeno, umožňuje rychlé, snadné a elegantní nasazení webových stránek Web 2.0. RoR je přitom velmi oblíbená platforma, kterou v určité podobě celosvětově využívají statisíce webů.

VZDÁLENÉ SPUŠTĚNÍ MALWARU V JAVĚ

Další nepříjemná chyba se týká Javy, kterou v současnosti najdete na většině počítačů. Tato chyba, která byla objevena v lednu 2013, umožňuje obejít sandbox. Díky tomu lze poté spustit v počítači libovolný škodlivý applet a získat plný přístup ke zranitelnému počítači. Útoky zneužívající tuto chybu byly brzy objeveny v reálném světě a příslušný exploit si rychle našel cestu do mnoha nástrojů pro provádění útoků, jako jsou BlackHole, Redkit nebo Nuclear Pack. Uživatelé těchto nástrojů mohou pomocí této zranitelnosti jednoduše instalovat škodlivé kódy na vzdálené počítače. Vznikl i nový modul Metasploit pro vyhledávání zranitelných systémů. Tím se stává nalezení obětí a jejich napadení otázkou jediného kliknutí. Společnost Oracle sice záplatu na problém vydala rychle, jenže ne každý uživatel ji použije. Zde navíc hraje roli i otřesná ergonomie aktualizací Javy. Kvůli tomu stále existuje mnoho nezáplatovaných systémů Java, takže útočníci stále mají široké pole působnosti.

Americký nouzový systém USA varoval před útokem zombie

Nouzový systém, který využívá Úřad pro národní bezpečnost (Homeland Security) pro varování před přírodními katastrofami nebo jinými mimořádnými událostmi, byl hacknut. Na počátku roku tento systém využili neznámí vtipálci a varovali občany před útoky zombie. Bezpečnostní experti nyní odhalili mezeru, pomocí které se mohou lidé připojit k zařízení jako správci. Také zjistili, že pro přístup do sekce zabezpečení jsou stále použita nezměněná standardní hesla.

Upravená aplikace pro Android obelstí kontrolu

Mezera v podepisování kódu pro aplikace pro OS Android umožňuje útočníkům upravovat aplikace, aniž by to si toho bylo při instalaci možné všimnout. Ohroženi jsou ale pouze ti uživatelé, kteří instalují aplikace z pochybných zdrojů, a ne z oficiálního obchodu Google Play. V současnosti už existuje patch pro Samsug Galaxy S4 a brzy budou následovat opravy i pro další modely.

10 %

všech počítačů se systémem Windows XP je infikováno virem. U Windows 7 jsou to jen 4 procenta.

Odhalení Esetu: Trojský kůň v Brazílii

Výzkumníci společnosti Eset provedli analýzu zajímavé formy bankovního trojského koně, která se šířila v Brazílii. Výzkum odhalil, že trojský kůň využíval k šíření a infikování počítačů technik sociálního inženýrství. Hrozba také zneužívala ke shromažďování informací o obětech brazilský vládní server. Trojan navíc využíval plug-iny v prohlížeči Google Chrome, jejichž prostřednictvím kradl uživatelům data. Mezi údaje, které tento škodlivý kód získával, patřila brazilská osobní identifikační čísla, hesla, PIN kódy nebo čtyřmístná ověřovací čísla ke kreditním kartám. Díky analýze Esetu, spolupráci s brazilskými úřady a firmě Yahoo! již tato sofistikovaná hrozba není aktivní. *„V tomto případě škodlivý kód využíval server, aniž by ho musel infikovat, neboť server postrádal adekvátní ochranu před zneužitím ze strany třetích osob. V důsledku toho kyberzločinci zůstávali anonymní a mohli se pokusit o přístup ke všem možným funkcím poskytovaným legitimním serverem. Vzhledem k důvěryhodnému jménu serveru se rozptýlilo jakékoli podezření,“* říká Sebastian Bortnik, manažer Esetu pro Jižní Ameriku. Eset označil tohoto zvláštního bankovního trojského koně jako JS/Spy.banker.G.

Škodlivý soubor se šířil pomocí technik sociálního inženýrství, aby se dostal mezi co největší počet uživatelů. Jedná se o tzv. dropper, škodlivý program vytvořený k tomu, aby do cílového systému nainstaloval další složky, díky čemuž dosáhne hrozba plné operační schopnosti. Škodlivý kód, který byl podroben analýze Esetu, byl vytvořen v .NET, populární vývojové platformě od firmy Microsoft. *„Skutečnost, že malware používá ke krádežím dat plug-iny Google Chrome, má přímý dopad na oběť, neboť v tomto případě není napaden operační systém, ale samotný prohlížeč,“* přibližuje Bortnik fungování malwaru. Právě plug-in prohlížeče je zásadním faktorem pro následnou krádež dat. Kompletní technickou analýzu tohoto malwaru naleznete v dokumentu na stránce WeLiveSecurity.com (**bit.ly/18WhwML**).