V aktuálním IT Kompasu jsme pro Vás připravili:

105. číslo

Vybrané aktuality ze světa IT
Tipy – Triky
Soutěž
Vtip pro dobrou náladu

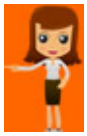
Vybíráme zajímavé aktuality:

ESET rozšiřuje ochranu svých uživatelů proti podvodným e-shopům
Bezpečnostní společnost ESET oznámila spolupráci s Českou obchodní inspekcí (ČOI). Využitím jejích dat, které jsou pravidelně integrovány do databáze bezpečnostních produktů ESET, upozorňuje uživatele na potenciálně rizikové webové stránky. Více...

Jak se na Twitteru vyhnout sledování falešných účtů?
Twitter je v poslední době pod drobnohledem. Hostuje totiž stovky tisíc účtů, které se tváří jako profily vlastněné reálnými lidmi, ale ve skutečnosti jde o "boty" neboli automatizované účty, které jsou hromadně vytvářeny s cílem zahltit danou platformu. Více...

Více aktualit naleznete na www.AntiviroveCentrum.cz nebo na Facebooku .

Tipy a triky



Dělá Váš mobil vylomeniny? Možná je v něm malware od výrobce

Možná patříte mezi ty, kdož si za dobrou cenu pořídili skvěle vybavený chytrý telefon čínské provenience. A možná se Váš telefon chová divně, provádí sám o své vůli různé kejkle, třeba otevírá podezřelé webové stránky nebo sám instaluje aplikace. Čím by to mohlo být? Odpověď je samozřejmě nasnadě - v telefonu se usídlila nějaká potvora. To samo o sobě není nic divného, protože Android je děravý jako řešeto a existuje mnoho potvor, které si na něm rády smlsnou. V případě levných čínských mobilů ale vůbec nemusí být jednoduché se potvor zbavit.

Důvod je jednoduchý - potvora se do mobilu dostala přičiněním jeho výrobce buď přímo ve výrobě, nebo třeba s nějakou aktualizací Androidu, ale prsty v tom může mít klidně i některý z velkých prodejců. Problém se netýká jen obskurních a málo známých výrobců, ale i poměrně velkých značek, jakými jsou například Lenovo, Huawei nebo Xiaomi a jsou popsány i případy infikovaných telefonů zakoupených třeba na Aliexpressu. Potvory jsou v telefonu usazeny velice hluboko na úrovni ROM paměti (ROM obsahuje samotný operační systém a další drobnosti nutné pro fungování telefonu), což v praxi znamená, že je nelze odstranit třeba resetem zařízení do továrního nastavení nebo v nouzovém režimu.

Dobrá zpráva je, že existuje řešení, špatná zpráva ale je, že je poměrně komplikované a běžný uživatel postup nejspíše nezvládne. Stručně řečeno je potřeba se zbavit infikované ROMky a přehrát ji nezávadnou. V některých případech se lze vrátit k předchozí verzi ROM přímo v telefonu, většinou ale bude nutné "někde sehnat" čistou ROM a osvojit si postup přeflešování telefonu.

Přesný návod Vám bohužel neposkytneme, protože to je nad rámec informativního charakteru Kompasu, nicméně Vám můžeme dát aspoň pár tipů. Základem všeho může být web XDA Developers , na kterém lze najít jak samotné ROMky pro různá zařízení, tak i přesné postupy přeflešování, bohužel ale pouze v angličtině. Spoustu informací také naleznete na českých webech, namátkou uvedeme například Smartmania.cz nebo SvetAndroida.cz.

Android a podvody s kryptoměnami

Když už jsme nakousli problémy s Androidími zařízeními v prvním tipu, můžeme i druhý tip věnovat Androidu a potenciálním podvodům týkajících se kryptoměn. Kryptoměny se v posledních měsících staly středem zájmu nejen "hodných uživatelů", ale samozřejmě také kyberlumpů. A už dávno neplatí, že se podvody ohledně kryptoměn týkají pouze klasických počítačů. Android je díky své rozšířenosti pochopitelně také v hledáčku kyberlumpů, kteří využívají toho, že jen málo online burz obchodujících s kryptoměnami má vlastní mobilní aplikaci.

Kyberlumpi se tedy snaží do obchodu Google Play propašovat "svoje vlastní aplikace", která se tváří jako oficiální aplikace burzy XY, ale ve skutečnosti je jejím cílem vylákat z neopatrného uživatele jeho přihlašovací údaje k dané burze. Z tohoto pohledu se tedy jedná o klasický phishingový útok, ovšem nikoliv pomocí emailu, ale pomocí podvržené aplikace. Jednou z posledních obětí se stala oblíbená burza Poloniex, která ovšem vlastní mobilní aplikaci nemá. Podobné útoky také byly zaznamenány na různé peněženky, tedy aplikace, pomocí nichž lze "kryptoměnu ukládat". Škodlivé chování bylo například objeveno u peněženky MyEtherWallet, která slouží pro ukládání kryptoměny Ethereum, a samozřejmě neexistuje žádná oficiální mobilní verze této peněženky. Některé verze podvodných peněženek zase generovaly falešné klíče (jde vlastně o veřejnou adresu peněženky), a pokud uživatel danou kryptoměnu v dobré víře převedl na zobrazenou adresu, neskončily kryptomince v jeho peněžence, ale v peněžence kyberlumpa.

Samostatnou kapitolou jsou pak mobilní aplikace, které dokážou kryptoměnu těžit. Existuje několik aplikací pro oficiální těžbu na účet majitele, pochopitelně ale také existuje řada potvor, které těží skrytě na účet kyberlumpa. Časté jsou i podvodné aplikace, které místo těžby kryptoměny jen zobrazují reklamy.

Teď Vás jistě bude zajímat, jak se před těmito problémy ochránit. V prvé řadě doporučujeme zapojit selský rozum a nepodlehnout domnění, že co je v obchodu Google Play, je nutně čisté jako křišťál. Tohle je zkrátka jen iluze... V druhé řadě doporučujeme případným mobilním zájemcům o kryptoměny zapátrat na oficiálních webových stránkách každé burzy či kryptoměnové peněženky a zjistit si informace o tom, jestli nabízí mobilní aplikaci, zjistit si její oficiální název a případně využít link na danou aplikaci umístěnou na oficiálním webu (link pravděpodobně povede také na Google Play, ale měl by zobrazit oficiální aplikaci). Na Google Play věnujte také pozornost počtu stažení a hodnocení aplikace ostatními uživateli!

Dále velice důrazně doporučujeme v aplikaci povolit dvoufaktorové ověření - v online bankovnictví nad použitím dvoufaktorové autentifikace už nikdo ani neuvažuje, takže by nad ní neměl uvažovat ani v případě mobilní aplikace pro kryptoměny. Což tedy znamená, že byste se k peněženkám a burzám v mobilu měli chovat naprosto stejně, jako se chováte ke svému běžnému účtu.

Na závěr ještě jedno důležité moudro - jestli něco vypadá až tak lákavě a skvěle, že se tomu ani nechce uvěřit, pak jde o podvod. Žádný člověk, který je aspoň trochu při smyslech, nebude například tvořit aplikaci, která by rozdávala Bitcoiny zdarma. Všechno kolem kryptoměn je tvrdý obchod a nikdo Vám reálně nenabídne zadarmo vůbec nic...

Soutěž

Vyhodnocení minulé soutěže:
Na otázku z minulého vydání elektronického magazínu IT Kompas odpověděl správně a z mnoha správných odpovědí byl vylosován pan Trnka, kterému tímto gratulujeme k výhře softwaru McAfee Internet Security pro 1 PC na rok zdarma.

Otázka zněla:
Co označuje pojem "EdgeLocker"?

Správná odpověď měla být:
EdgeLocker je virus, který šifruje dokumenty, obrázky a důležité soubory s cílem získat od uživatele finanční prostředky za dešifrovací klíč.

Nová otázka:
Co označuje pojem "Doorway pages"?

Ze správných odpovědí vylosujeme výherce, který od nás získá AVG PC TuneUp pro 1 PC na rok zdarma.

Odpovědi pište do 20. 4. 2018 na e-mail amenit@amenit.cz.

Správnou odpověď a výherce uveřejníme v příštím čísle. Pokud se chcete co nejdříve dozvědět, zda jste vyhráli, staňte se našimi přáteli na Facebooku. Tam se informace o výherci objeví jako první.

Vtip pro dobrou náladu

Farář se ptá na hodině náboženství dětí:
"Kdo chce jít do nebe?" Hlásí se všichni kromě Pepíčka.
"Proč ty do nebe nechceš?"
"Protože maminka říkala, že mám jít ze školy rovnou domů!"

Vydání IT Kompasu od 1. čísla naleznete zde.

Tým Antivirového Centra
Amenit s.r.o.

ANTIVIROVÉ CENTRUM
www.AntiviroveCentrum.cz

Amenit s.r.o. - jsme s vámi již od roku 1998, tel.: 556 706 203, 222 360 250

Nezobrazuje-li se vám e-mail správně, klikněte prosím zde.