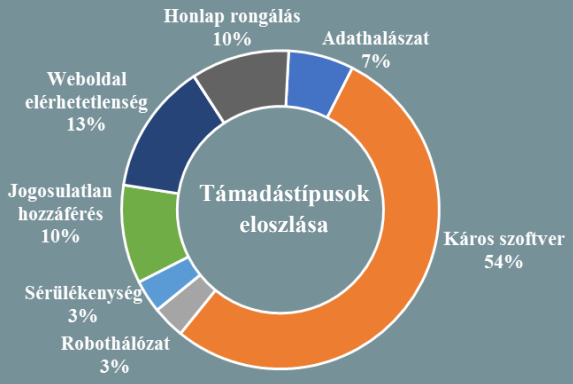
Incidens adatok: 2017.11.29. — 2017.12.05.



Szándékosan sértett törvényt az NSA?

(www.searchsecurity.techtarget.com)

Újabb információk szivárogtak ki az amerikai Nemzetbiztonsági Ügynökség (NSA) 'Ragtime' megfigyelő szoftverével végzett titkos információgyűjtéssel kapcsolatban, amit eszerint az ügynökség amerikai állampolgárok ellen is alkalmazhatott. Korábbi adatszivárgásoknak köszönhetően a szoftver négy variánsa már ismertté vált, azonban ez a szám most tizenegyre bővült, köztük egy 'USP' kódnevű verzióval, amely elnevezéséről – a hírszerző terminológiára hivatkozva – feltételezik, hogy a "U.S. person", azaz "amerikai személy"-t jelentheti. Nem ez az első eset, hogy illegális adatgyűjtéssel vádolják a szervezetet, azonban az eddigi védekezés – miszerint nem szándékos tevékenység zajlott – kérdőjeleződik most meg. Szakértők szerint a biztonsági kontrollok hiánya azonban egy ilyen szenzitív adatokat tartalmazó adatbázis esetében az információgyűjtés okától függetlenül rendkívül komoly probléma. **Bővebben...**

Az android kriptovaluta-zseb alkalmazások időzített bombák?

(www.bleepingcomputer.com)

A svájci illetékességű kiberbiztonsági cég, a High-Tech Bridge szerint a Google Play alkalmazásboltban található legtöbb kriptovaluta-zseb alkalmazásban van kihasználható biztonsági rés, azok védtelenek a leggyakoribb és jól ismert sérülékenységekkel szemben. A vizsgált, mintegy 90 alkalmazás több, mint 90%-a érintett volt valamilyen biztonsági problémában: az alkalmazások nagy része tartalmazott beépített API kulcsokat és jelszavakat, nem alkalmaztak titkosítási eljárást, és sérülékenyek voltak a MitM (Man-in-the-Middle) támadásokkal szemben. A kutatók szerint a feltárt probléma leginkább az Android fejlesztői közösség felelőssége, ahol a fejlesztés során a biztonságos kódolás jellemzően nem prioritás. **Bővebben...**

A német belügyminiszter nem tett le a "backdoor"-ok létesítéséről

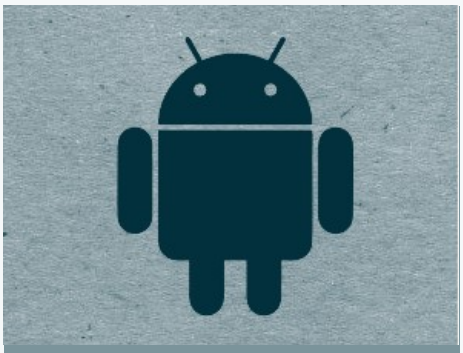
(www.itwire.com)

Thomas de Maizière törvényjavaslatot készített elő a héten Lipcsében megrendezésre kerülő miniszteri találkozóra, melyben a hírszerző ügynökségek és a hatóságok számára biztosítana titkos hozzáférést minden, az internethez csatlakozó eszközhöz. Ennek célja, hogy az érintett szervek az eszköz tulajdonosának tudta nélkül képesek legyenek titkos megfigyelést végezni, akár olyan kifinomult biztonsági rendszerekkel rendelkező eszközökön keresztül is, mint a modern gépjárművek. Konstantin von Notz, a német Zöldpárt helyettes frakcióvezetője szerint az intézkedés komoly adatvédelmi aggályokat vet fel. Úgy véli, ebben az "orwelli rémálomban" az állampolgárok elveszítenék a magánélethez való jogukat. **Bővebben...**

Az etióp kiberkémek mindenki számára hozzáférhetővé tették a kémszoftverük naplófájljait

(www.bleepingcomputer.com)

Az etióp kormány egy izraeli kémszoftvert használt fel annak érdekében, hogy disszidensek után kémkedjen bel- és külföldön egyaránt. A megfigyelni tervezett célszemélyek közül azonban néhányan felismerték, hogy spear-phishing kampány folyik ellenük és jelentették azt a Citizen Lab nevű szervezetnek, amely komoly tapasztalatokkal rendelkezik a politikai motivációjú kiberműveletek kivizsgálásában. Miután szándékuk napvilágra került, az etióp kormány úgy döntött nem függeszti fel a kampányt, hanem kiterjeszti azt a Citizen Lab nyomozóira is. A káros kód analizálását követően a kutatók feltárták, hogy a spyware-t irányító vezérlő (C&C) szerveren publikusan hozzáférhető mappákban kerültek letárolásra a kód által generált naplófájlok, valamint a célszemélyek IP címei is. **Bővebben...**



A Google Safe Browsing az androidos applikációkat is figyeli

(www.security.googleblog.com)

A tech cég az androidos eszközökre is kiterjeszti az Unwanted Software Policy-t, mely alapján a személyes felhasználói adatokat (például telefonszám, vagy e-mail cím) vagy az eszközre vonatkozó információkat kezelő alkalmazások és weboldalak kötelesek tájékoztatni a felhasználókat az adatvédelmi irányelveikről. Továbbá, amennyiben az alkalmazás a rendeltetésén kívül álló okból gyűjt és továbbít adatot, az adatgyűjtés megkezdése előtt egyértelműen tájékoztatniuk kell a felhasználót az adatkezelés mikéntjéről, valamint a jóváhagyását kell kérniük. A fejlesztőknek 60 nap áll rendelkezésre a követelményeknek való megfeleléshez. Ennek elmulasztása esetén a felhasználók a Google Play Protect szolgáltatáson, vagy az applikáció letöltési oldalán megjelenő figyelmeztetésen keresztül kerülnek értesítésre. **Bővebben...**

IT biztonsági Tanács

A Windows 10 fájlelőzmények szolgáltatásával minimalizálhatjuk egy esetleges zsarolóvírus támadás során bekövetkező adatveszteséget.

Ez a funkció biztonsági másolatot készít az adatfájlokról, valamint eltárolja a fájlok korábbi verzióit is, amelyek így továbbra is elérhetőek lesznek.

Sikeres Europol akció

(www.securityaffairs.co)

Sikerrel zárult a "Neptune" kódnevű művelet, amelynek során az európai hatóságok egy bankkártya-hamisító bűnözői hálózatot számoltak fel. A hírek szerint négy bolgár személyt tartóztattak le, akik kulcsszerepet játszhattak érzékeny pénzügyi információk ellopásában és az azokkal történő visszaélésekben. A támadások során európai városokban található ATM-ekben elhelyezett technikai eszközök (rejtett kamerák és szkimmerek) segítségével szereztek meg bankkártya adatokat, amelyeket azután készpénzfelvételre használtak fel. **Bővebben...**

A Chrome blokkolni fogja a kódbefecskendezést

(www.securityaffairs.co)

A Google bejelentette, hogy a jövőben tiltani fogja a harmadik féltől származó szoftverek részéről a Chrome folyamataiba való kódbefecskendezést. Mindez jelentős hatással lehet több szoftver működésére, ugyanis a Google szerint a felhasználók körülbelül kétharmada rendelkezik olyan applikációval, amelyek interakcióban állnak a Chrome böngészővel. Ezek között találhatók vírusirtók és egyéb biztonsági termékek, amelyek a fenyegetések elhárításának céljából élnek a technikával. A változtatás oka a böngésző stabilitásának növelése, ugyanis a Chrome blogján nyilvánosságra hozott közlemény szerint a kódbefecskendezés átlagosan 15%-kal növeli a böngésző összeomlásának valószínűségét. A fejlesztőknek összesen 14 hónap áll rendelkezésre a felkészüléshez, mely időszak alatt három lépésben kerül bevezetésre az új szigorító intézkedés. **Bővebben...**

Eltolódhat a netsemlegességről szóló szavazás

(www.reuters.com)

Eric Schneiderman, New York állam főállamügyésze arra szólította fel a Szövetségi Kommunikációs Bizottságot (FCC), hogy halasszák el a netsemlegességet biztosító 2015-ös törvény visszavonásáról szóló szavazást, amire eredetileg 2018. február 14-én került volna sor Ajit Pai, a szövetség elnökének javaslatára. A főállamügyész ugyanis nyomozást kezdeményezett az FCC-nek netsemlegesség témában küldött 21,7 millió nyilvános komment körüli kérdések tisztázásához. Ezek szerint a vélemények több, mint fele ideiglenes címről érkezett, illetve ugyanarról a címről több üzenetet is küldtek, valamint az is felmerült, hogy tartalmukat tekintve hamis vagy félrevezető információval bírhatnak. Schneiderman elmondta, a szavazást addig el kell halasztani, amíg ki nem derül, hogy pontosan mi is történt. **Bővebben...**

Az Egyesült Államok kormányának nincs szüksége bírósági határozatra „hátsó kapuk” beépítéséhez

(www.zdnet.com)

A kritikusok már régóta feszegetik a kérdést, hogy az Amerikai Egyesült Államok kormánya igen széles mozgástérrel rendelkezik arra vonatkozóan, hogy megfigyeléseket hajtson végre egy átfogó határozat értelmében (FISC 702-es cikkely). Ron Wyden szenátor kérdésére válaszolva a kormányzat elismerte, hogy bármilyen technológiai céget titokban felkérhet arra, hogy hátsó kaput építésen adott termékébe és amennyiben ellenállásba ütközne, a FISC részére benyújtott kérelemmel végső soron kikényszerítheti a közreműködést. A nyilatkozat szerint mindezidáig nem kellett ilyen módon érvényesíteni az igényüket, ám arról nem tesz említést, hogy kértek-e már meg cégeket arra, hogy szándékosan gyengítsék az alkalmazott titkosítási eljárást. **Bővebben...**