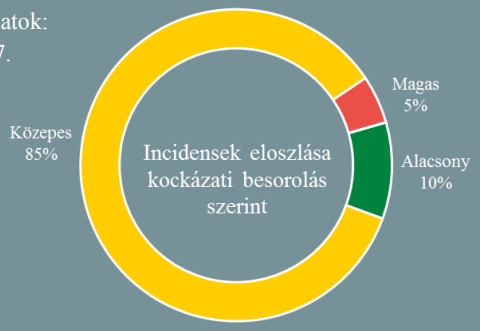
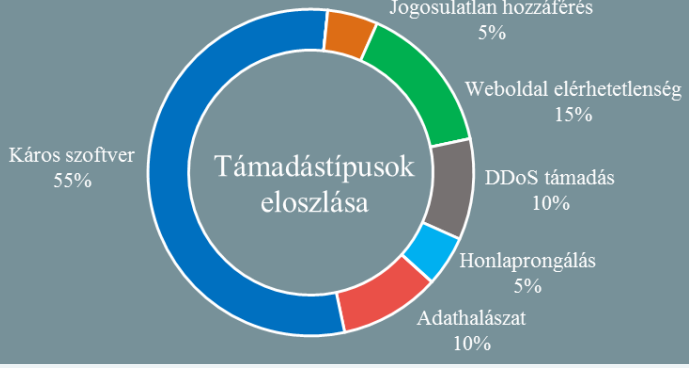
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 42. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.10.11. - 2019.10.17.





Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Üzbég hacking műveletre derült fény, „elképesztően rossz” műveleti biztonság miatt

(vice.com)

Korábban ismeretlen fenyegetési csoportot (SandCat) azonosított a Kaspersky, amelyről feltételezik, hogy az üzbég hírszerzéshez (SSS) tartozik. A felfedezés nem csak amiatt érdekes, hogy ez az első eset, hogy az országhoz nagy volumenű kiberművelet köthető, hanem a csoport által elkövetett súlyos műveleti biztonsági (OPSEC) mulasztások miatt is. A SandCat ugyanis többek közt olyan jelentős hibákat is vétett, mint, hogy egy domain név regisztrációjakor egy SSS-hez köthető katonai csoport nevét használta, vagy, hogy a malware fejlesztésre használt gépen a Kaspersky vírusirtót futtatták. Utóbbi ugyanis azt eredményezte, hogy az orosz biztonsági cég hozzáfért a káros kódokhoz, valamint egyéb információkhoz, például a műveleteik során felhasznált négy nulladik-napi sebezhetőséghez, amit harmadik féltől ─ vélhetően két izraeli kémszoftver gyártótól, az NSO Group-tól, valamint a Candiru-tól ─ vásároltak. **Bővebben...**

Megjelent a kiberbűnözés helyzetét összefoglaló idei Europol jelentés

(blog.malwarebytes.com)

Az Europol minden évben összesíti a számítógépes bűnözéssel kapcsolatos főbb trendeket és fenyegetéseket. Az idei Internet Organized Crime Threat Assessment (IOCTA) jelentés szerint a támadások tekintetében továbbra is a zsarolóvírusok jelentik a legnagyobb problémát. Ennek kapcsán megfigyelhető, hogy bár a zsarolóvírus támadások volumene csökkent, azonban jóval célzottabban jelentkeznek, és az okozott gazdasági károk is jelentősebbek. A pénzügyi szervezetek számára továbbra is jelentős veszélyt jelentenek az ATM-ek elleni támadások (jackpotting, Card-not-present), amelyek a „Cutlet Maker”-hez hasonló toolok könnyű hozzáférhetőségével egyre gyakoribbá váltak. **Bővebben...**

Még lementhetők az adatok a Yahoo Groups törlése előtt

(engadget.com)

A Yahoo bejelentette a Yahoo Groups weboldal megszüntetését, amely a cég egyik legrégebb óta működő szolgáltatása volt. A leállítást két fázisban végzik, október 21-től nem lehet majd új tartalmat létrehozni az oldalon, december 14-én pedig törlésre kerülnek a korábban közzétett anyagok is. A felhasználók ugyan e-mailen keresztül továbbra is csatlakozhatnak csoportjaikhoz, azonban a weboldalon valójában nem lesz már tartalom, a csoportok mindegyike privát lesz, és a csoportokhoz történő csatlakozáshoz adminisztrátori jóváhagyás lesz szükséges. A törlés előtt a felhasználók letölthetik adataikat és korábbi műveleteiket közvetlenül a bejegyzéseknél, illetve a Yahoo adatvédelmi felületén keresztül. **Bővebben...**

Nulladik napi sérülékenység érinti az iTunes-t, amit már ki is használnak

(securityaffairs.co)

A BitPaymer zsarolóvírus támadásokkal gyanúsított kiberbűnözői csoport a Morphisec biztonsági kutatói szerint egy Apple iTunes-t és iCloudot érintő windowsos sérülékenységet kihasználva új támadási kampányba kezdett. A biztonsági rés a Bonjour frissítéskezelőt érinti, valamint általa megkerülhetővé válik az antivírus védelem, valamint jogosultság kiterjesztés érhető el. Ennek hátterében egy programozói figyelmetlenség áll, ugyanis ha egy parancsfájl elérési útvonala nincs megfelelően ─ azaz idézőjelek között ─ megadva, emellett szóközöket is tartalmaz, azt egy támadó kihasználhatja oly módon, hogy a sérülékeny program legitim processzével a saját állományát futtatja. **Bővebben...**

Apple: a Safari nem küld böngészési adatokat a Tencentnek

(securityweek.com)

Az Apple reagált a vádra, miszerint a Safari böngésző egy biztonsági funkcióján keresztül a kínai vállalatóriás Tencent hozzáfér az ügyfelek böngészési adataihoz. Az amerikai cég közleményében azt állítja, hogy bár a kínai ügyfelek káros oldalaktól való védeleméhez valóban igénybe veszik a Tencent szolgáltatását, azonban a böngészett weboldalak teljes URL-jét sosem küldik meg, hanem csupán korlátozott mennyiségű felhasználói információt továbbítanak, mindazonáltal azt elismerik, hogy a felhasználók IP címei továbbításra kerülhetnek. A Google Safe Browsing funkciója kezdetben valóban elküldte a meglátogatott weboldalak teljes címét a szolgáltatónak, azonban adatvédelmi aggályokra reagálva a Google módosította az eljárást. Jelenleg az ismert káros oldalak URL-jéből egy hasító függvény (SHA256) segítségével lenyomatot képeznek, majd a hashek 32 bites prefixéből összeállított adatbázist küldik el a böngészőknek. **Bővebben...**

IT biztonsági Tanács

Fontos, hogy okos eszközeink üzembe helyezése után első dolgunk legyen az alapvető biztonsági beállítások elvégzése. Az alábbiakban erre vonatkozóan találhat javaslatokat.

- Mindig változtassuk meg az alapértelmezett jelszót. Különböző eszközök, alkalmazások és felhasználói fiókok esetén használjunk eltérő, lehetőleg minél hosszabb, egyedi jelszavakat.
- A gyártók általában adnak ki biztonsági frissítéseket termékeikhez, ezeket mindig telepítsük, vagy ha elérhető az opció, kapcsoljuk be az automatikus frissítést.

További javaslatokat az NBSZ NKI weboldalán, itt találhat.

Kék halál: A Symantec Endpoint Protection a Windows összeomlását okozhatja

(heise.de)

A Symantec Endpoint Protection biztonsági megoldásának felhasználói egyre többet panaszkodnak a Windows összeomlására, ami kék halállal (Blue Screen of Death – BSOD) végződik. Az összeomlásért a Symantec LiveUpdate által 2019. október 14-én kiadott 2019/10/14 r61 aláírásfrissítés a felelős. A hibát már javították, továbbá a Symantec egy áthidaló megoldást is közzétett az érintett felhasználók számára. A probléma elhárítása érdekében telepíteni kell a 2019/10/14 r62 frissítést, vagy vissza kell állni egy korábbi verzióra, ennek módjáról a Symantec egy leírást adott ki. **Bővebben...**

A Huawei visszautasítja az észt vádakat

(securityweek.com)

A Huawei kedden éles kritikát fogalmazott meg az észt kormánnyal és a médiával szemben, amiért szerintük önkényes és megalapozatlan állításokat tettek a cég mobiltelefonjainak kiberbiztonsági kockázataival összefüggésben. A nyilatkozat egy észt televíziós műsor szeptemberi adására utalt, amelyben a külgazdasági és technológiai miniszter, Kert Kingo fejtette ki álláspontját a Huawei termékek biztonsági kockázatairól. Később kiderült, hogy Kingo Huawei headsetet és telefont használt a munkahelyén, azonban a minisztérium szerint idő közben iPhone-ra váltottak. Hong Yang, a Huawei balti-térségbeli területi vezetője visszautasítja, hogy a cég személyes adatokat gyűjtene és osztana meg harmadik felekkel az ügyfelek engedélye nélkül. **Bővebben...**

A kínai ipari kémkedés egyik legnagyobb sikere lehet a Comac C919 utasszállító

(infosecurity-magazine.com)

A CrowdStrike jelentésében azt állítja, hogy a kínai kormány többéves komplex ipari kémkedés során jutott olyan technológiai információkhoz, hogy megépíthesse a Comac C919 kereskedelmi célú utasszállító repülőgépét, ennek részeként kényszerített technológiaátadást, belsős anyagok ellopását, és kiberkémkedést is alkalmaztak. A 2010-től kezdődő hírszerzési műveletek hátterében a kínai Állambiztonsági Minisztérium Jiangsu irodáját sejtik, amire a CrowdStrike „Turbine Panada”-ként hivatkozik. A célpontok között volt több nagyobb légügyi gyártó, mint például a Honeywell, a Safran, és a Capstone Turbine. A kampány során a kínai hírszerzés sikeresen beszervezett egy General Electronics alkalmazottat, aki a kulcsfontosságú LEAP-X turbóventillátor gyártásánál dolgozott, valamint egy kínai születésű tartalékost, aki F1-es szintű (tanulói) vízummal rendelkezett. **Bővebben...**

Egy európai reptér munkaállomásainak több, mint fele kriptovalutát gyűjtött

(securityaffairs.co)

A Cyberbit biztonsági szakértői egy Monero kriptovaluta bányász programmal fertőző támadási kampányt fedeztek fel, amely egy európai reptér munkaállomásainak több, mint 50%-át érintette. Az esetre egy nemzetközi reptéren végzett EDR (Endpoint Detection and Response) vizsgálat során derült fény. A Cyberbit megállapította, hogy a munkaállomások mindegyike rendelkezett a szabványban előírt vírusvédelmi rendszerekkel, ennek ellenére a kriptobányász program észrevétlen maradt a gépeken. Bár a rosszindulatú program üzleti hatása a repterekre nézve viszonylag alacsony volt, a Cyberbit jelentése szerint ezzel együtt teljesítményromlás, a szolgáltatások időleges megszakadása, valamint az energiafelhasználás jelentős növekedése volt tapasztalható. **Bővebben...**