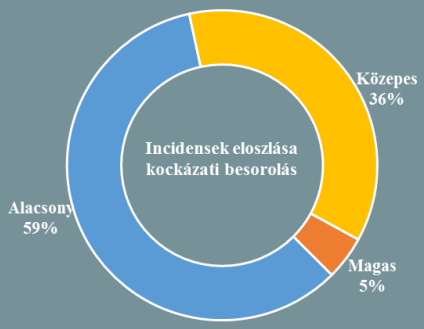
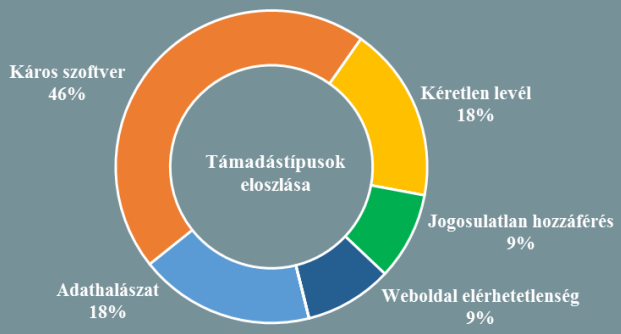
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 39. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.09.21. - 2018.09.27.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

A német rendőrségnek főleg a drog elleni harcban van szüksége trójai programokra

(www.heise.de)

Németországban a rendőrségnek az úgynevezett „állami trójai" programok használatára leginkább a kábítószerügyek kapcsán van szüksége ─ állapította meg egy 2014-es szövetségi jelentés, amelyhez a Netzpolitik.org az információszabadságról szóló szövetségi törvényre (IFG) hivatkozva fért hozzá. Eszerint az esetek 53 százalékában a narkotikumokkal összefüggő bűncselekmények utáni nyomozások során vetették be a trójai programokat, amikor a cél az volt, hogy a kódolt telekommunikációs csatornák (Messenger, WhatsApp, Signal, stb.) már a „forrásnál" ellenőrzésre kerülhessenek. E tekintetben szintén neuralgikus pontnak számít a vagyonelleni bűncselekmények köre, ezen ügyek a kapacitások mintegy 23 százalékát kötik le. A Német Szövetségi Parlament jogi szabályozás keretében rögzítette azon – súlyosabbnak minősülő – esetköröket, amelyek kapcsán a tárgyalt módszert igénybe vehetik a hatóságok. **Bővebben...**

Nem kell többé jelszavakkal bajlódni a Yubico új termékével

(techcrunch.com)

A Yubico bejelentette a Yubikey elnevezésű biztonsági kulcs termékének legújabb, 5-ös szériáját, amely a hasonló megoldások közül elsőként támogatja a FIDO 2-es szabványt, amivel biztonságos módon, teljes mértékben kiváltható a jelszavak használata. A cég közleménye szerint az új termék USB mellett NFC támogatással is bír, így asztali és mobil platformon egyaránt használható. Azt is kiemelik, hogy a kulcsok teljes mértékben az USA-ban és Svédországban készülnek, ellentétben például a Google nemrég piacra dobott termékével. **Bővebben...**

Illegális kriptovaluta bányászat ─ egy perzisztens fenyegetés

(www.cyberthreatalliance.org)

A Cyber Threat Alliance a növekvő fenyegetés miatt helyzetértékelő jelentést készített az illegális kriptovaluta bányász programokról, tudniillik 2017 és 2018 között 459%-kal nőtt a detektált fertőzések száma. Az anyag több fontos megállapítást is tesz a témában, például, hogy a WannaCry fertőzés során felhasznált EternalBlue exploit kód továbbra is használatban van, annak ellenére, hogy kihasznált sérülékenységet megszüntető patch már mintegy 18 hónapja elérhető. **Bővebben...**

Minden eddiginél szofisztikáltabb módon támadnak az orosz hackerek

(www.wired.com)

Az ESET kutatói szerint az Oroszországhoz köthető Fancy Bear (Sednit) néven azonosított hacker csoport olyan technikát alkalmaz európai kormányzati célpontok ellen, amelyre eddig nem volt példa ─ írja a Wired. A biztonsági cég bizonyítékot talált arra, hogy a hírhedt csoport egy támadás során a célkeresztben lévő gép alaplapi firmware-ébe ágyazott UEFI rootkit (LoJax) segítségével teljes hozzáférést szerzett a rendszerhez, amelyre ezután tetszés szerint tölthetett le további káros komponenseket. A fertőzést nem csak detektálni nehéz, de eltávolítani is problémás, ugyanis a káros kód minden bootoláskor betöltésre kerül, egyedül a firmware update vagy az alaplap cseréje nyújthat megoldást. **Bővebben...**

Kriptovaluta bányász programokat fedeztek fel a Google Play-en

(www.securityweek.com)

A Sophos munkatársai 25, a felhasználók tudtán kívül kriptovalutát bányászó applikációt fedeztek fel a Google Play-en, amely tevékenységet a Google már egy ideje tilt az alkalmazás áruházában megjelenő appok számára. A biztonsági cég szerint eddig több, mint 120 000 felhasználó tölthette le a szóban forgó alkalmazásokat, amelyek a káros tevékenységet játékoknak és egyéb segédprogramoknak álcázták. Legtöbbjük Monero kriptopénzt termelő Coinhive kódokat használ, amelyek a szokványos megoldástól eltérő módon nem az eszköz grafikus vezérlőjét veszik célba a számításokhoz, hanem a CPU-t. Ezek az appok az észrevétlenség érdekében már szabályozzák a CPU használatot és figyelnek az akkumulátor merülésére és a túlmelegedésre, így sokszor a felhasználó nem is vesz észre teljesítményromlást. A szakemberek szerint az ilyen kódok lényegében bármilyen mobilos alkalmazásba beilleszthetőek, amelyek a beágyazott WebView böngészőt használják a webes tartalmak megjelenítésére. A Google -t már augusztusban értesítették a problémáról, azonban az alkalmazások egy része továbbra is letölthető a Google Play-ből. **Bővebben...**

IT biztonsági Tanács

Az FBI riasztást adott ki a távoli adminisztrációhoz használt RDP protokoll kibertámadások során történő felhasználásának megnövekedett száma miatt. Ebben ─ többek között ─ javasolják a nyitott RDP portok alkalmazásának mellőzését, vagy amennyiben ez nem lehetséges, legalább a VPN-en keresztüli elérés kikényszerítését.

Osztrák államkötvény blokklánc alapon

(thenextweb.com)

A TheNextWeb szerint az osztrák Oesterreichische Kontrollbank (OeKB) 1,3 milliárd dollár értékű államkötvényt bocsát ki, amely kezelését az Etherum blokklánc alapú rendszere végzi majd. Hartwig Löger, osztrák pénzügyminiszter elmondása szerint országa elkötelezett a blockchain technológia iránt, amely ─ ahogy fogalmazott ─ gazdaságpolitikájuk fókuszában áll. Az aukció a tervek szerint október 2-án fog megtörténni, a kötvényekre vonatkozó adatok az osztrák államkötvények kibocsátására szolgáló speciális rendszerből (Austrian Direct Auction System ─ ADAS) kerülnek át az Etherum blokkláncába. Az osztrák kezdeményezés bár Európában úttörőnek számít, világszinten nem egyedülálló, ugyanis a Commonwealth Bank of Australia korábban már megtette ugyanezt, igaz jóval kisebb ─ mindössze 80 millió dollár ─ értékben. **Bővebben...**

Fertőznek-e még USB kulcsokkal?

(securelist.com)

Az USB eszközök közel 20 éve jelentenek egyszerű és kényelmes megoldást az adatok mozgatására olyan rendszerek között, amelyek nem rendelkeznek internet eléréssel, illetve manapság is gyakorta alkalmazzák őket otthoni környezetben, vagy például marketing célra promóciós kampányok során. Népszerűségük okán az elmúlt évtizedben a kiberbűnözők előszeretettel használták fel őket kibertámadások során (lásd Stuxnet, 2010). A Kaspersky az USB eszközök által okozott aktuális fenyegetéseket felmérő friss jelentése szerint a fertőzött kulcsokkal történő támadások száma bár 2014 óta folyamatosan csökken, azonban egyre lassuló ütemben. Jellemző, hogy növekvő arányban fertőznek kriptovaluta bányász programokkal, a legnépszerűbb kripto miner (Trojan.Win64.Miner.all) használata például évről-évre nő. **Bővebben...**

Önbeteljesítő jóslat Barcelonában

(www.bleepingcomputer.com)

Nem egészen két nappal azután, hogy a barcelonai kikötő közétett egy Twitter bejegyzést, miszerint senki sem érezheti magát biztonságban a kibertámadásokkal szemben, maga a kikötő is kibertámadás áldozatává vált. A kikötő Twitter csatornáján megjelent információ szerint az áruk ki- és beszállítása késedelmet szenved egy több kiszolgálót is érintő kibertámadás miatt, mindazonáltal az informatikai részleg elindította a katasztrófa helyreállítási folyamatot. Más források szerint a kikötő működését nem befolyásolta a támadás sem a földi, sem a vízi kiszolgálás tekintetében. A kikötő tájékoztatása szerint értesítették az illetékes hatóságokat, és megtették a szükséges jogi lépéseket is. **Bővebben...**

A Microsoft szerint a jelszavak ideje lejárt

(www.zdnet.com)

A Microsoft az Ignite 2018 konferenciáján bejelentette, hogy az Azure Active Directory immár támogatja a saját fejlesztésű autentikátor alkalmazással történő hitelesítést. Mindez azt jelenti, hogy az Azure AD-t használó vállalatok alkalmazottjai jelszavak helyett az okostelefonjaikra telepített applikáció segítségével azonosíthatják magukat a vállalati IT környezetben, de az Office 365, Azure és a Dynamics CRM Online szolgáltatások esetében is használható az app. Az elképzelés mögött az a feltevés áll, hogy a támadóknak nehezebb ellopni a felhasználó telefonkészülékét, mint megszerezni a jelszavát. A cég emellett több újdonságot is bejelentett, például az MI-t is felhasználó Microsoft Threat Protection-t, ami a Microsoft 365 számára nyújt védelmet. **Bővebben...**