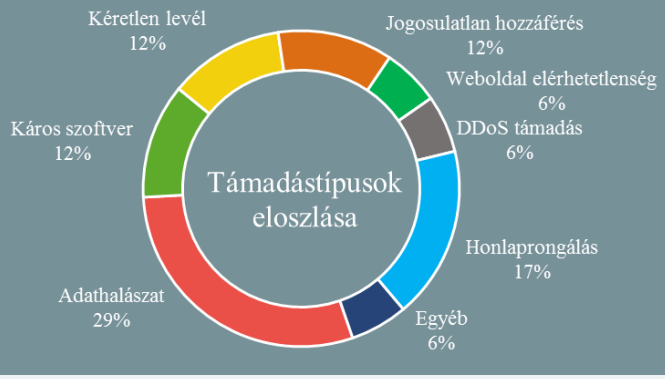
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 30. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.07.19. - 2019.07.25.



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

A Winniti APT csoport jelenti az egyik legnagyobb kiberfenyegetést a német ipar számára

(web.br.de)

Két német televíziós műsor szolgáltató (Bavarian Broadcasting Corporation és a Norddeutscher Rundfunk) közös nyomozásba kezdett a német ipar számára aktuálisan az egyik legnagyobb kiberfenyegetést jelentő APT csoport tevékenységéről. Elemzésükben ─ amelynek összeállításához több IT-biztonsági kutatót is segítségül hívtak ─ átfogó képet kívánnak nyújtani a Winniti hacker kollektíva működéséről és feltételezett motivációiról. A Kínához köthető Winniti csoport legalább 2011 óta létezik, tevékenységére az online játékokkal foglalkozó német Gameforge rendszerének megtámadásával derült fény. Ekkor az elsődleges cél még a profitszerzés volt, a 2014-es Henkel elleni művelet óta azonban a kiberkémkedés vált a fő profillá. **Bővebben...**

Zsarolóvírus támadás ért egy dél-afrikai áramszolgáltatót

(reuters.com)

Johannesburg városi áramszolgáltatója, a City Power közleménye szerint egy zsarolóvírus „szinte valamenynyi" adatbázisukat és alkalmazásukat titkosította. A cég weboldala is elérhetetlenné vált, az ügyfelek pedig emiatt problémát tapasztalhatnak több szolgáltatással kapcsolatban is, beleértve az előrefizetős áramszolgáltatás keretein belül történő vásárlásokat, vagy a számlák feltöltését. A Reuters információi szerint már több johannesburgi lakos is jelezte egy helyi rádiónál, hogy a ransomware támadás miatt áramszolgáltatás nélkül maradtak. A City Power közleménye szerint jelenleg a helyreállításon dolgoznak.

Egyre nagyobb fenyegetést jelentenek a célzott zsarolóvírus támadások

(securityweek.com)

A Symantec új jelentése egy aggasztó kibertámadási trendre kívánja felhívni a figyelmet, ugyanis a biztonsági cég saját telemetriai adatai alapján azt tapasztalja, hogy az elmúlt két év során ugrásszerűen megemelkedett a szervezetek elleni célzott zsarolóvírus támadások száma. A célzott és az általános ransomware támadások között alapvető különbség egyrészt a váltságdíj nagysága, másrészt a támadók technikai tudása. 2018 elejéig csupán a SamSam csoport intézett célzott támadásokat, hozzájuk köthető például az atlantai városi rendszerek elleni tavalyi incidens. **Bővebben...**

A lengyel CERT közzétette a FaceApp elemzésük eredményét

(cert.pl)

A FaceApp-ot ért adatlopási vádak miatt több országban is vizsgálat indult, köztük Lengyelországban, ahol az országos számítógép vészhelyzet kezelő csoport (Computer Emergency Response Team – CERT), a CERT Polska foglalkozott a kérdéssel. Mint, kiderült, a FaceApp 3.4.9.1-es androidos verzióján végzett elemzés során nem találtak bizonyítékot visszaélésre. Az alkalmazás hálózati kommunikációval kapcsolatban megállapították, hogy az applikáció a vizsgálatkor nem kommunikált gyanús szerverek felé, valamint a vádakkal ellentétben nem továbbított tetszés szerint képeket, csupán azon fényképeket töltötte fel a felhőbe, amelyeket a felhasználó a kép manipulálásához kiválasztott. Megjegyzik ugyanakkor, hogy az alkalmazás a kiválasztott képfájlok Exif metaadataihoz is hozzáfér, amelyek között ─ az adott eszköz beállításaitól függően ─ a kép készítésének GPS helyadatai is megtalálhatóak lehetnek. Az elemzés eredményeképp valószínűtlennek tartják, hogy a szoftver rosszindulatú kódot tartalmazna. **Bővebben...**

Ijesztő arzenállal bír egy újonnan felfedezett spyware

(thehackernews.com)

A Lookout kiberbiztonsági kutatói egy új mobil megfigyelésre alkalmas spyware-t azonosítottak, amelyről feltételezik, hogy egy olyan orosz védelmi cég (Special Technology Centre) fejleszthette, amelyet már értek szankciók a 2016-os amerikai elnökválasztásban való közreműködés vádjával. A Monokle nevű RAT (remote-access-trojan) kártevőt legalább 2016 márciusa óta aktívan használják Android telefonok ellen, célzott támadások során. A Lookout szerint a Monokle kiterjedt és fejlett kémkedési funkciókkal rendelkezik, amelyek nem feltétlenül igényelnek root jogoultságot az adott eszköz felett. A káros kód az Android hozzáférhetőségi szolgáltatásokat használja arra, hogy adatokat szerezzen több harmadik féltől származó alkalmazásból, mint például a Google Docs, a Facebook messenger, a Whatsapp, a WeChat és a Snapchat, azáltal, hogy képes beolvasni a képernyőn megjelenített szöveget. **Bővebben...**

IT biztonsági Tanács

Az utóbbi évek során egyre jellemzőbbé vált a PowerShell kiterjedt képességeit rosszindulatú célokra történő felhasználása. Az Európai Unió intézményeinek Számítógépes Vészhelyzeti Reagáló Csoportja (CERT-EU) emiatt egy fehér könyv (white paper) összeállítása mellett döntött, amelynek célja segítséget nyújtani a PowerShell-t érintő támadások detektálásához és azok megelőzéséhez. A javasolt tevékenységek (például a logolás és monitorozás bevezetése, vagy a PowerShell legújabb (5-ös) verziójának használata a 2-es verzió letiltásával) gátat szabhatnak egyes támadási módoknak.

Főbb biztonsági kockázatok az 5G hálózatok kiépítése kapcsán

(securityweek.com)

Az Amerikai Egyesült Államok belbiztonsága alatt működő kiberbiztonsági ügynökség (Cybersecurity and Infrastructure Security Agency – CISA) infografikában foglalja össze az 5G hálózatokat érintő lényeges kockázatokat. A meglévő 4G (LTE) hálózatra épülő ötödik generációs mobil hálózat egyik fő célja a kapacitásbővítés, ugyanis több tízmilliárd csatlakozó eszközt kell kiszolgálnia. Habár az 5G terén számos fejlesztést irányoztak elő, a CISA arra hívja fel a figyelmet, hogy egyes ─ például az ellátási láncot, a telepítést, valamint a hálózatbiztonságot érintő, vagy a piaci versenyből és üzleti döntésekből eredő ─ sérülékenységek negatívan befolyásolhatják az 5G hálózatok bizalmasságát, sértetlenségét és rendelkezésre állását. **Bővebben...**

Megtévesztésre adhat módot egy Twitter funkció

(bleepingcomputer.com)

Egy hónapok óta ismert Twitter hiba lehetővé teszi, hogy rosszindulatú felhasználók a tweetek manipulálásával legitim weboldalnak álcázzák saját, káros tartalmú ─ például adathalászati célú ─ oldalukat. Amikor egy felhasználó egy hivatkozást oszt meg a Twitteren, a platform ellenőrzi a weboldalt, metaadatok után kutatva. Találat esetén ezeket arra használja fel, hogy a hivatkozás számára létrehozzon egy ún. Twitter Card-ot, amelyben a megosztott weboldalhoz kapcsolódó kiegészítő információk, például egy rövid leírás, valamint média elemek (kép, videó) jeleníthetők meg. A problémát a funkció kapcsán az okozza, hogy a Card generálásához adatot gyűjtő Twitterbot átirányítható egy másik oldalra, ebben az esetben pedig már az átirányított oldal metaadatai kerülnek felhasználásra. **Bővebben...**

Titkos adatgyűjtéssel vádolják a Huawei cseh képviseletét

(securityaffairs.co)

A cseh közrádió információi szerint a Huawei helyi képviselete titokban személyes adatokat gyűjtött ügyfeleiről, üzleti partnerekről és állami tisztviselőkről. A rádió két, nevük elhallgatását kérő korábbi Huawei menedzserre hivatkozik, akik szerint a kínai tech óriás arra kötelezte őket, hogy adott személyek privát adatait Kínából elérhető ügyfélkapcsolati (Customer Relationship Management-CRM) rendszerekbe is felvigyék. Olyan információk álltak az érdeklődés középpontjában, mint például az érintettek gyermekeinek száma, pénzügyi helyzete, hobbija és érdeklődési köre. Az AFP szerint a Huawei azt állítja, hogy mindez megfelelt a GDPR követelményeinek. **Bővebben...**

Kötelezővé tennék bizonyos szoftverek előtelepítését orosz törvényhozók

(reuters.com)

Egy új törvényjavaslat az orosz szoftvergyártók támogatásának elősegítése céljából kötelezővé tenné egyes orosz gyártmányú szoftverek előtelepítését az országban értékesített digitális eszközök (okostelefonok, okos televíziók, számítógépek, stb.) esetében. Amennyiben egy gyártó ennek nem tesz eleget, 50-200 000 rubel büntetésre számíthat. Az orosz mobil telefon piacon elsősorban az Apple, a Samsung, valamint a Huawei gyártók termékei az egyeduralkodók. A szóban forgó javaslat múlt hét csütörtökön került benyújtásra, amit amennyiben az alsó-, valamint a felsőház, illetve az elnök által is jóváhagy, legkorábban 2020 júliusában léphet hatályba.