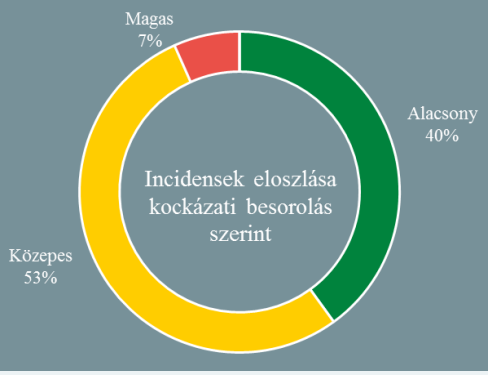
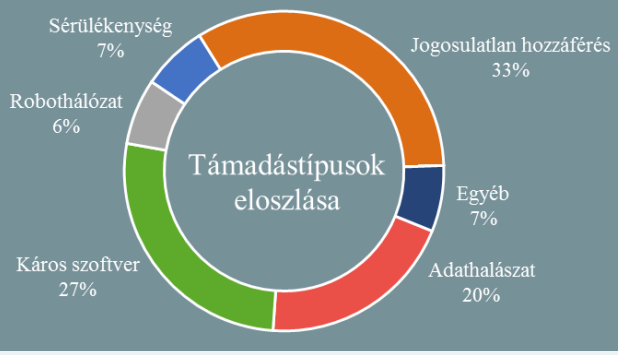
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 04. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.01.18. - 2019.01.24.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta olvashatja legújabb híreinket!

Dél-koreai katonai beszerzésekről próbáltak információt szerezni egy kibertámadás során

(theregister.co.uk)

A dél-koreai védelmi minisztérium közleménye szerint hackerek sikeresen kompromittáltak 10 munkaállomást a minisztérium katonai beszerzésekért is felelős területén ─ írja a The Register. Az érintett számítógépeken bizalmas ─ például újgenerációs vadászgépek vásárlásáról szóló ─ anyagok is elérhetőek voltak, ezekhez azonban a hivatalos információk szerint a mindeddig nem azonosított támadók nem fértek hozzá. A támadás 2018. október 4-én kezdődött, majd három héten át felfedezetlenül folytatódott. Jelenleg is tartanak a vizsgálatok, amelyek többek közt arra keresik a választ, hogy Észak-Korea állt-e az eset mögött.

A Let's Encrypt megszünteti a TLS-SNI támogatást

(theregister.co.uk)

A Let's Encrypt közleményben tudatta, hogy 2019. február 13-tól megszűnteti a TLS-SNI-01 domain validációs eljárás támogatását, annak tavaly januárban felfedezett komoly sérülékenysége miatt, amely a támadók számára lehetővé teszi, hogy felhasználhassák a támadott website HTTPS tanúsítványait. A cég közleménye szerint ügyfeleik többsége már a javasolt alternatívákat használja (DNS-01, HTTP-01), azonban feltételezik, hogy még előfordulhatnak olyanok, akik nem tértek át ezekre ─ velük igyekeznek közvetlenül is felvenni a kapcsolatot.

Egy zsarolóvírus, ami egyben PayPal adathalászatot is végez

(www.infosecurity-magazine.com)

Támadók rafinált módon igyekeznek PayPal fiókokhoz tartozó hitelesítési azonosítókat szerezni egy zsarolóvírus segítségével ─ hívja fel a figyelmet a MalwareHunterTeam. A támadások során a ransomware által titkosított állományok feloldását lehetővé tévő kulcs megadását nem csupán Bitcoin átutaláshoz kötik, az áldozat számára felajánlják a lehetőséget, hogy PayPal átutalással fizesse ki a váltságdíjat, azonban a felkínált link egy csaló oldalra navigálja az érintettet, ahol a bejelentkezési adatait lementik. **Bővebben...**

Egyes linuxos malware-ek törlik a védelmi szoftvereket

(unit42.paloaltonetworks.com)

A Palo Alto Networks Unit 42 ─ a cég fenyegetés felderítő csoportja ─ felfedezett egy olyan malware családot, amelynek célja a támadott Linux szerveren adminisztrátori szintű jogosultságot szerezni, hogy ennek birtokában egyszerűen uninstallálja a védelmi szoftvereket, ezután pedig olyan további modulokat töltsön le, amelyekkel a támadók Monero kriptovaluta bányászatába kezdhetnek. A felfedezett támadások felhő infrastruktúrák ellen zajlottak, a vizsgálat alá vont malware példányok pedig két kínai nagyvállalat, a Tencent Cloud, valamint az Alibaba Cloud mesterséges intelligenciát is alkalmazó termékeit tudták eltávolítani. Az elemzések során megállapítást nyert, hogy a szóban forgó hacker csoport Apache Struts 2, Oracle WebLogic, valamint Adobe ColdFusion sérülékenységek kihasználásával végezte a kezdeti fertőzést. A támadásokat a kínai hátterűnek tartott „Rocke" nevű csoporthoz kötik, amelyről először a Cisco Talos adott hírt 2018 júliusában.

Egy új kutatás szerint minden ötödik ingyenes VPN alkalmazás veszélyes lehet

(www.bleepingcomputer.com)

A Top10VPN széleskörű kutatást végzett a Google Play Store 150 legnépszerűbb ingyenes Android VPN alkalmazásának körében, amelyből kiderült, hogy minden ötödik applikáció rosszindulatú kódok potenciális forrása lehet. A 27 ellenőrzött alkalmazás egynegyedét a felhasználói adatok bizalmasságát is érintő hibák sújtják, mint például a DNS szivárgás. **Bővebben...**

Microsoftos törekvés az álhírek visszaszorítására

(www.theverge.com)

A Microsoft Edge mobil böngésző felhasználói számára iOS-en és Androidon egyaránt elérhetővé vált egy új funkció, amely figyelmezteti a felhasználókat, amennyiben egy potenciálisan hamis hírportálra tévednek — írja a The Verge. **Bővebben...**

IT biztonsági Tanács

2019 áprilisában várhatóan kivezetésre kerül a Google+ szolgáltatás, ezért érdemes lehet elvégezni a Google+-ban tárolt adatok lementését, amelyre több lehetőség is rendelkezésre áll.

Ilyen például a nyílt forrású Google+ Exporter, ami kimondottan erre a célra dedikált alkalmazás. Másik alternatíva lehet a Google Takeout, ami a Google-fiókba történő bejelentkezést követően az *„Adatok és személyre szabás”* menüben található. Az *„adatok letöltése”* lehetőségre kattintva a megjelenő listából válasszuk ki a szolgáltatást és kövessük az instrukciókat.

ProtonMail: alaposan át kell gondolni az online terrorista tartalmak eltávolításának miként jét

(protonmail.com)

A ProtonMail az idei Tech Against Terrorism nevű konferencián foglalt állást az Európai Unió terrorista tartalmak kezelésére vonatkozó — véleményük szerint több homályos megfogalmazást is tartalmazó — javaslatával (A proposal for a Regulation on preventing the dissemination of terrorist content online) szemben, a téma kapcsán pedig blogjukon is közzétettek egy bejegyzést. Eszerint bár szigorúan elhatárolódnak bármilyen bűnözői tevékenységtől, és támogatják a bűnüldöző hatóságok munkáját, alapvetően ellenzik, hogy szegényes gyakorlatok alkalmazásával olyan törvények szülessenek, amelyek aláásha tják a globális biztonságot. Rossz példaként a szóban forgó EU-s javaslat mellett említik az Egyesült Királyság Investigatory Powers Actjét, valamint az ausztrál Assistance and Access Billt, mint olyan kezdeményezéseket, amelyek a titkosítás gyengítésével komoly károkat okoznak az általános biztonságnak. A terrorizmust érintő online tartalmak eltávolítását hatványozottan érzékeny témakörnek tekintik, amely a szólásszabadságra és a magánélethez való jogra nézve komoly következményekkel jár majd, és csak a különböző szektorok összefogásával kezelhető.

Az DHS sürgős cselekvésre szólítja fel a szövetségi ügynökségeket a DNS hijacking kibertámadások miatt

(cyberscoop.com)

Az amerikai belbiztonsági minisztérium ún. „vészhelyzeti rendeletet” adott ki a szövetségi polgári ügynökségek számára, amelyben a domain adminisztrációs fiókok megerősített védelmét írja elő, amiért azok fokozottan kitettek egy nemrég a FireEye által azonosított, DNS infrastruktúrák ellen zajló célzott kibertámadási művelettel szemben, amelynek során a támadók DNS szerverek, illetve domain regisztrátori fiókok kompromittálásával igyekeznek eltéríteni a hálózati forgalmat az irányításuk alatt álló, fertőzött szerverek felé. A vészhelyzeti rendelet a szóban forgó fiókok vonatkozásában előírja a többfaktoros azonosítás bevezetését, az aktuális jelszavak cseréjét, a DNS rekordok felülvizsgálatát, valamint a tanúsítványokkal kapcsolatos logok monitorozásának bevezetését, amelyek implementálására 10 munkanapot határozott meg. **Bővebben...**

Hatalmas ellenkezést váltott ki szakmai körökben egy Chrome API frissítési terve

(zdnet.com)

A Google Chrome bővítmények által használt webRequest API módosítási tervét elsőként Raymond Hill, a uBlock Origin, valamint a uMatrix népszerű blokkoló kiegészítők készítője kommentálta, miszerint a Chrome fejlesztői csapat által bevezetni szándékolt új DeclarativeNetRequest API jelentősen korlátozni fogja a reklámblokkolók működését. Azóta számos biztonsági kutató és fejlesztő fejezte ki kritikáját, akik igyekeznek felhívni a figyelmet arra, hogy a tervezett változtatás biztonsági célú programokat, például antivírus szoftverek böngésző kiegészítőit is érinti. Mindazonáltal reménykedésre adhat okot, hogy a jelek szerint a Chrome fejlesztők nyitottak a visszajelzésekre, egyikük ugyanis a téma kapcsán úgy fogalmazott, hogy nem céljuk a szkriptblokkolók akadályoztatása, ellenkezőleg, gyorsabbá és biztonságosabbá szeretnék tenni a működésüket, ezért a bejelentett változtatások nem véglegesek.