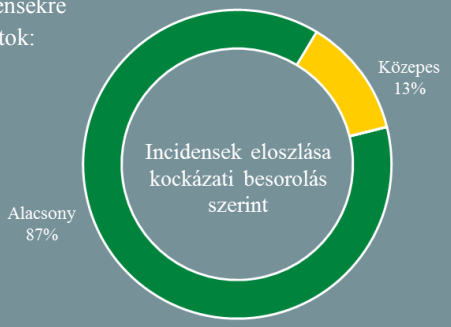
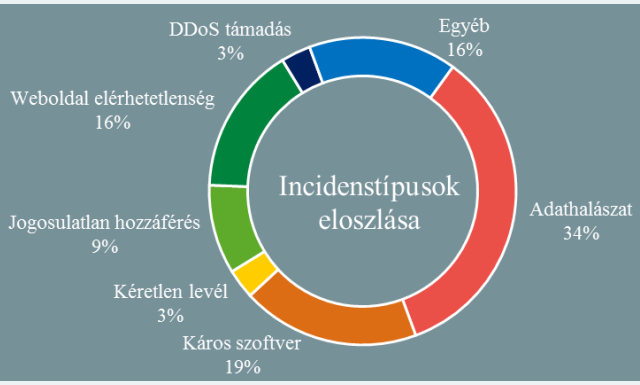
Nemzetközi IT-biztonsági sajtószemle

2021. 15. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.04.09. - 2021.04.15.





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

Még el sem indult, a Brave böngésző máris tiltja a Google új nyomkövető rendszerét

(zdnet.com)

A Google a harmadik féltől származó sütiken alapuló reklámozási rendszerét váltaná fel a FLoC (Federated Learning of Cohorts) szisztémával, amelynek lényege, hogy a felhasználókat online tevékenységük alapján kohorszokba (csoportokba) sorolná, amit a hirdetők felhasználhatnak tematizált reklámok megjelenítésére. A csoportba sorolás a felhasználók böngészési előzményei alapján zajlik, a Chrome böngésző FLoC komponense minden héten begyűjti és elemzi az adott heti böngésző history-t, majd egy FLoC csoport ID-t rendel a felhasználóhoz. **Bővebben...**

Egy remek példa, hogy miért ne kísérletezzünk nem hivatalos alkalmazás-boltokkal

(bleepingcomputer.com)

Biztonsági kutatók rosszindulatú kódot találtak a hivatalos **APKPure** alkalmazásban, amely egy népszerű 3rd-party alkalmazásbolt, azaz segítségével a Google Play Store-hoz hasonlóan a felhasználók alkalmazásokat tudnak letölteni és telepíteni, amelyek elvileg megegyeznek a hivatalos Store-ban találhatóakkal. A Kaspersky és a Dr.Web által felfedezett vírus a **Triada trójai** program család tagja, képes a fertőzött eszközök felhasználóinak mindennapjait felugró hirdetésekkel és további rosszindulatú programok telepítésével megkeseríteni. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arról, miként tehető biztonságosabbá az Instagram fiókunk.

Zero-day sebezhetőséget találtak a Chrome-ban

(bleepingcomputer.com)

Egy biztonsági kutató távoli kódfuttatást (Remote Code Execution – RCE) lehetővé tévő zero-day sebezhetőségről posztolt kihasználási bizonyítást (proof of concept – PoC) a Twitteren. A sérülékenység Chromium-alapú böngészők V8 JavaScript Úmotorját érinti, és a Google Chrome és a Microsoft Edge aktuális verziói (előbbi esetében a 89.0.4389.114, utóbbinál a 89.0.774.76) is sérülékenyek. Megjegyzendő ugyanakkor, hogy a biztonsági rés önmagában nem tesz lehetővé kódfuttatást, ahhoz ugyanis szükség van egy másik sebezhetőség kihasználására is, a Chromium sandbox környezetéből való kilépéshez. **Bővebben...**

Saint Bot: újabb veszélyes kártevő a színen

(thehackernews.com)

„Saint Bot” névre keresztelték az először 2021 januárjában észlelt kártevőt, amelyet kiberbűnözők főképp más rosszindulatú programok telepítésére használnak. A Malwarebytes elemzői szerint a káros kódot elsősorban adathalász e-mailek útján terjesztik, egy utóbbi kampány során például egy bitcoin pénztárca telepítő programjának álcázott tömörített csatolmányként (bitcoin.zip). A fájl kicsomagolás és futtatás esetén valójában egy PowerShell szkriptet indít el, ami további futtatható káros fájlokat (**WindowsUpdate.exe, InstallUtil.exe, def.exe, putty.exe**) tölt le a fertőzött eszközre. **Bővebben...**

Izraeli kibertámadás miatt állhatott le az iráni atomlétesítmény

(securityweek.com)

Továbbra sem ismert, hogy pontosan miért állt le a vasárnap kora reggeli órákban a natanzi urándúsító létesítmény Iránban, csupán egy nappal az újgenerációs urándúsító centrifugák üzembe helyezése után. Akbar Salehi, az iráni atomprogram vezetője az állami tévében tett nyilatkozata szerint azonban országa szabotázsként értékeli az incidenst, és felszólítja a Nemzetközi Atomenergia-ügynökséget, hogy lépjenek fel a „Nukleáris terrorizmussal” szemben. **Bővebben...**