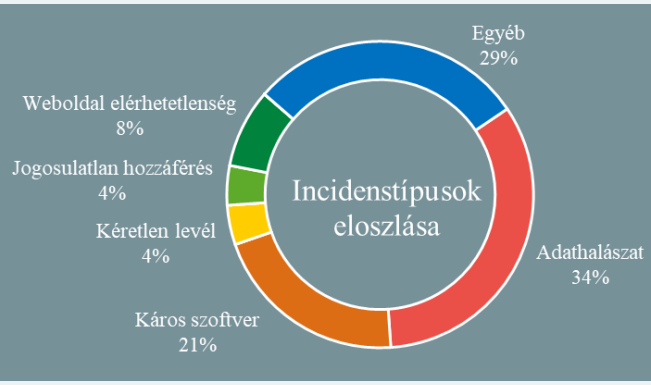
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 14. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.04.01. - 2021.04.08.



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

Kibertámadás alatt áll az Európai Unió

(bleepingcomputer.com)

Az Európai Bizottság szóvivőjének elmondása szerint márciusban több uniós intézmény infrastruktúráját érintő „informatikai biztonsági esemény" következett be. A jelenleg még kezdeti fázisban lévő kivizsgálás során szoros együttműködés tapasztalható az érintett szervezetek, valamint a CERT-EU (Az EU-s intézmények Számítástechnikai Sürgősségi Reagáló Egysége) között. Egyelőre még nincs információ a biztonsági esemény jellegéről és hatásáról ─ habár a nyilatkozat szerint eddig szerencsére nem azonosítottak súlyos információszivárgást ─ mint ahogyan a támadás mögött álló elkövető(k) kilétéről sem tudni. **Bővebben...**

Netflixszet utánzó csaló appot szúrtak ki a Google Play Store-on

(thehackernews.com)

A Checkpoint kutatói fedeztek fel egy **Netflixet utánzó** káros appot a Google Play Store-on. A káros alkalmazás neve **FlixOnline**, és képes WhatsApp üzenetekre adott válaszként automatikusan továbbítani magát, valamint más alkalmazások bejelentkezési oldalait utánozni, annak érdekében, hogy a hitelesítési adatokat megszerezze. A biztonsági szakemberek szerint a malware meglehetősen innovatív technikát alkalmazva támadja a WhatsAppot, ami megegyezik az idén januárban az ESET által detektált **Huawei Mobile** nevű káros alkalmazás működési elvével, ami arra enged következtetni, hogy a káros kód más álruhában, de idővel visszatér majd. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arról, miként állítható be a kétfaktoros azonosítás Facebook fiókunkhoz.

Tetszőleges hangon szólalhatnak meg a hackerek

(securityweek.com)

A pszichológiai manipulációs (social engineering) támadások egy új szintjéről számol be a Cado Security. Egy, a Hamas-hoz köthető hacker csoport, az **APT-C-23** ugyanis a jelek szerint hangmanipulációs szoftver segítségével vehette rá célpontjait káros kódok telepítésére. Az APT-C-23 már korábban is alkalmazta azt a megtévesztési módot, hogy női kamuprofilok álcájával vette fel a kapcsolatot, elsősorban az Izraeli Védelmi Erők katonáival. A Cado Security egy, a hackerek által használt szerver átvizsgálása során azonban olyan hangfájlokat fedezett fel, amelyek arra engednek következtetni, hogy a hackerek újabban női hangon megszólaló hangüzeneteket is küldenek az áldozatoknak, amit káros kódokat tartalmazó videóüzenetek követnek. A biztonsági szakemberek szerint a manipulált hangfájlok a **Morph Vox Pro** programmal készültek.

Káros kódokat telepített egy rendszerfrissítési app androidos Gigaset okostelefonokon

(thehackernews.com)

Újabb androidos malware botrány robbant ki, ezúttal a főleg német piacon érdekelt Gigaset gyártó (korábban: Siemens Home and Office Communications Devices) egyes termékeiről derült ki, hogy az **Update** nevű (csomagneve: **com.redstone.ota.ui**), előtelepített rendszerfrissítés-kezelő applikáció káros kódokat telepít a telefonokra. **Bővebben...**

Itt ellenőrizheti, hogy érintett-e a legújabb Facebook adatszivárgásban

(securityweek.com)

Néhány nappal ezelőtt több, mint **533 millió Facebook felhasználó** személyes adatait tartalmazó adatbázis vált nyilvánossá egy hacker fórumon. A kiszivárgott adatok között sok esetben az érintett személy Facebook azonosítója, neve, telefonszáma, neme, illetve kapcsolati státusza, születési dátuma, földrajzi helyzete és e-mail címe is szerepel. Az adatok vélhetően 2019-ből származnak, és az „Add Friend" funkció egy sérülékenységének kihasználásával kerületek begyűjtésre. **Bővebben...**