NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 48. hét

HÍREK

- A WinZip sérülékenysége kártékony kód futtatását teszi lehetővé
- A Meta több mint 2 millió felhasználói fiókot törölt, amelyek csalásokban vettek részt
- Vállalati Wi-Fi hálózatokon keresztül támadott az orosz APT csoport
- A RomCom hackercsoport ismét zero-day sérülékenységeket használ ki
- Feltehetően Orosz hackerek áldozata lett több mint 60 ázsiai és európai intézmény

SÉRÜLÉKENYSÉGEK

- Riasztás állami szervezetek megszemélyesítésével történő adathalász kísérletekről

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

További érdekességekért, látogasson el **weboldalunkra**!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Riasztás állami szervezetek megszemélyesítésével történő adathalász kísérletekről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) riasztást ad ki állami szervezetek nevével való visszaéléssel elkövetett adathalász üzenetekről.

A riasztás megjelenésének idején a **Nemzeti Infokommunikációs Szolgáltató Zrt.**, az **Építési és Közlekedési Minisztérium**, a **Magyar Nemzeti Bank**, a **Debreceni Egyetem**, a **Szépművészeti Múzeum** nevével történt a visszaélés, de feltételezehető, hogy további intézmények is megszemélyesítésre kerülnek.

Bővebben...

Amennyiben ilyen megkeresés érkezik, kérjük jelezzék ezt az NBSZ NKI incidensbejelentési elérhetőségén: csirt@nki.gov.hu

NEWS

IT biztonsági

HÍREK

A Meta több mint 2 millió felhasználói fiókot törölt, amelyek csalásokban vettek részt

(bleepingcomputer.com)

A Meta bejelentette, hogy az év eleje óta több mint 2 millió fiókot távolított el platformjairól, amelyek az ún. “pig butchering” és egyéb csalásokhoz kapcsolódtak. A fiókok többsége Mianmarból, Laoszból, az Egyesült Arab Emírségekből, a Fülöp-szigetekről és Kambodzsából származik. **Bővebben...**

Vállalati Wi-Fi hálózatokon keresztül támadott az orosz APT csoport

(volexity.com)

A Volexity olyan felfedezést tett, amely az eddigi egyik legizgalmasabb és legösszetettebb incidensvizsgálatához vezetett. Az orosz APT28-hoz kötötték a támadást, aki egy új támadási technikát vetett be, amely a célpont közelében lévő Wi-Fi hálózatokat használja ki. **Bővebben...**

A RomCom hackercsoport ismét zero-day sérülékenységeket használ ki

(bleepingcomputer.com)

A feltehetően orosz székhelyű RomCom (más néven Storm-0978, Tropical Scorpius vagy UNC2596) APT csoport két zero-day sérülékenységet kombinált a legutóbbi támadásaiban, amelyek a Firefox és a Tor böngészők felhasználóit célozták Európában és Észak-Amerikában. **Bővebben...**

Feltehetően Orosz hackerek áldozata lett több mint 60 ázsiai és európai intézmény

(securityweek.com)

Egy feltehetően Oroszországhoz köthető kiberkémkedési hálózat több mint 60 áldozatot ejtett Ázsiában és Európában, főként a kormányzati, emberjogi és oktatási szektorban – számolt be róla a Recorded Future. **Bővebben...**

A WinZip sérülékenysége kártékony kód futtatását teszi lehetővé

(securityonline.info)

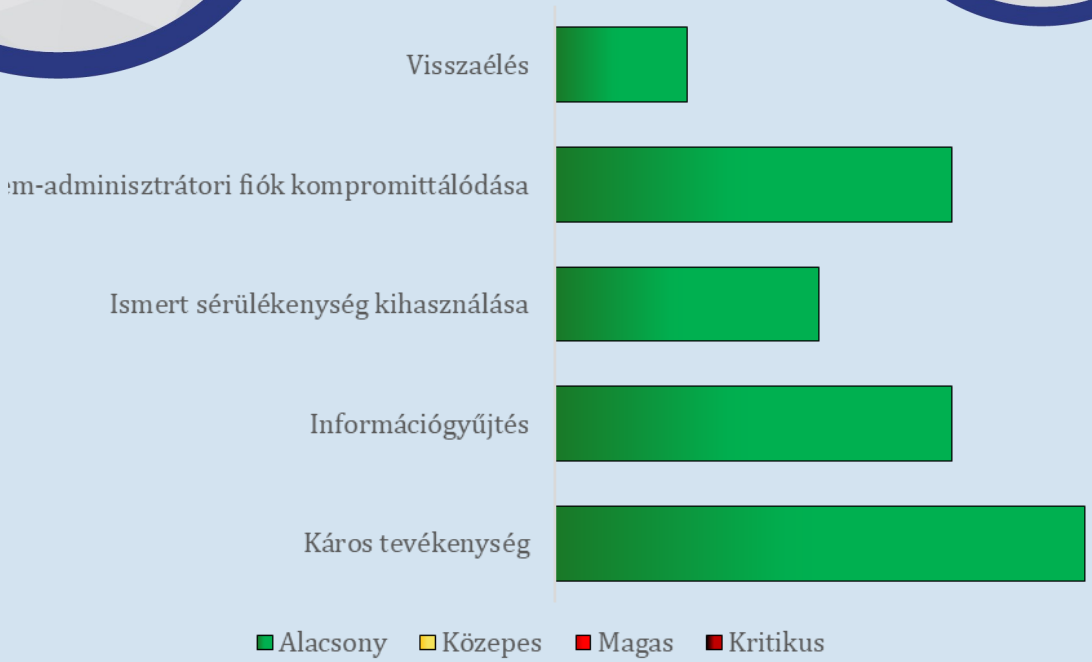
Egy magas súlyosságú sérülékenység került felfedezésre a nagy népszerűségnek örvendő WinZip nevű fájlarchiváló szoftverben. **Bővebben...**

Statisztikai Adatok

2024.11.22.-2024.11.28.

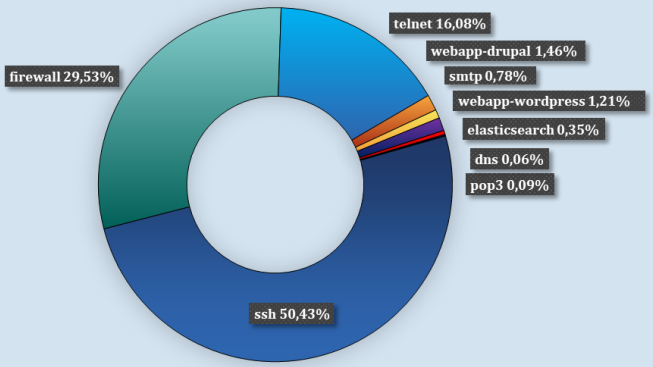
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

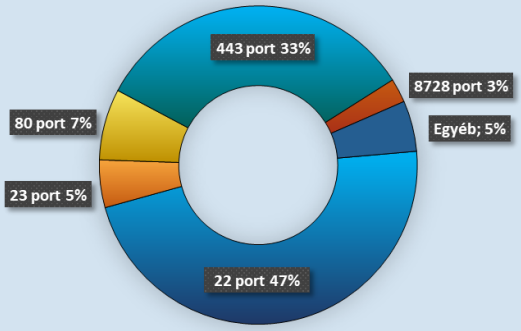
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:





További érdekességekért, látogasson el **weboldalunkra**!