NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 21. hét

HÍREK

- Fertőzött KeePass jelszókezelővel támadnak a hackerek
- Célkeresztben a kormányzati levelezőrendszerek
- Kártékony PyPI csomagok
- Automatikus jelszócsere a Google Chrome böngészőben
- 100+ hamis Chrome bővítmény

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

NEWS

IT biztonsági
HÍREK

Fertőzött KeePass jelszókezelővel támadnak a hackerek
(bleepingcomputer.com)

A WithSecure's Threat Intelligence szakemberei egy olyan kampányt tártak fel, amelyben módosított KeePass jelszókezelő alkalmazást terjesztettek azzal a céllal, hogy a felhasználók rendszereibe kártékony vezérlőkomponenseket juttassanak be. **Bővebben...**

Célkeresztben a kormányzati levelezőrendszerek
(bleepingcomputer.com)

A RoundPress nevű globális kiberkémkedési kampány során a hackerek webmail szerverek nulladik napi (zero-day) és már ismert (n-day) sérülékenységeit kihasználva férnek hozzá bizalmas kormányzati e-mailekhez. Az ESET kutatói szerint a kampány az Oroszországhoz kapcsolható, feltehetően államilag támogatott APT28 (Fancy Bear vagy Sednit) nevű csoporthoz köthető. **Bővebben...**

Kártékony PyPI csomagok
(thehackernews.com)

Kiberbiztonsági kutatók kártékony csomagokat fedeztek fel a Python Package Index (PyPI) adattárban. Ezek egyfajta ellenőrző eszközként működtek, melyek azt vizsgálták, hogy az ellopott email címek érvényesek-e egy TikTok, vagy egy Instagram API ellen. **Bővebben...**

Automatikus jelszócsere a Google Chrome böngészőben
(thehackernews.com)

A Google új funkciót jelentett be Chrome böngészőjében, amely jelentősen egyszerűsítheti a felhasználók számára a jelszóbiztonság fenntartását. A beépített Jelszókezelő ezentúl képes lesz automatikusan megváltoztatni a felhasználói jelszót, amennyiben a rendszer kompromittáltként azonosítja. **Bővebben...**

100+ hamis Chrome bővítmény
(thehackernews.com)

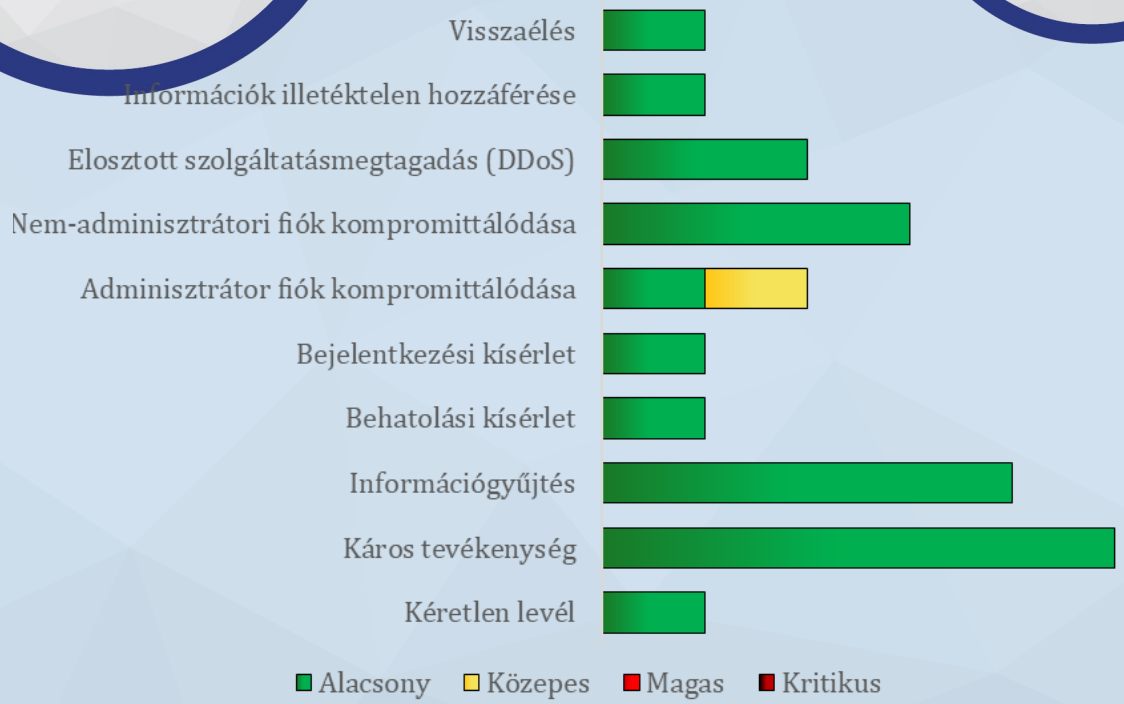
Egy eddig ismeretlen támadóhoz köthető, rosszindulatú Chrome-bővítményeket azonosítottak, melyek 2024 februárja óta folyamatosan helyeztek el a Chrome Web Strore-ba. Ezek az első ránézésre ártalmatlannak tűnnek, de rejtett funkciókkal rendelkeznek, mint például adatszivárogtatás, kártékony kódok futtatása, és egyebek.
Bővebben...

Statisztikai Adatok

2025.05.16.-2025.05.22.

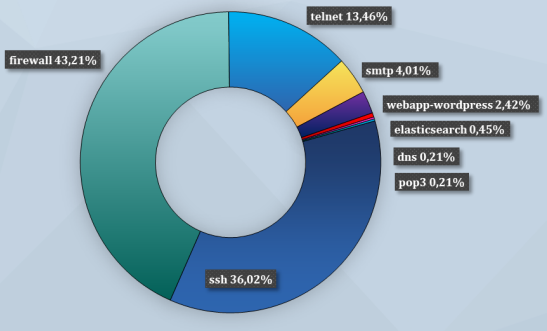
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

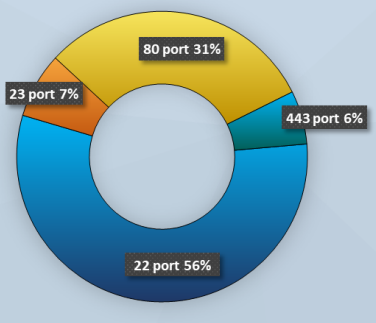
Fenyegetettségi szint: közepes



Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!