NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 45. hét

HÍREK

- Tanulmány: A ChatGPT-4o hangvezérlési funkciója kihasználható pénzügyi csalások elkövetéséhez
- qBittorrent-használók évekig MitM támadásoknak voltak kitéve
- 5 hibás konfiguráció, ami jelentős károkat okozhat SaaS környezetekben
- Git repository-kat célzó masszív támadókampányt fedeztek fel
- A Google javított két nulladik napi Android sebezhetőséget

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

qBittorrent-használók évekig MitM támadásoknak voltak kitéve

(bleepingcomputer.com)

A qBittorrent — az egyik legismertebb torrent kliens — fejlesztői CVE regisztrálása és a felhasználók figyelmeztetése nélkül javítottak egy jelentős, távoli kódfuttatást lehetővé tevő (RCE) hibát. **Bővebben...**

5 hibás konfiguráció, ami jelentős károkat okozhat SaaS környezetekben

(thehackernews.com)

A bérelhető felhő alkalmazások (Software-as-a-Service – SaaS) számos kockázatot rejtenek magukban többek között a konfigurációs lehetőségek széles skálája miatt. **Bővebben...**

Git repository-kat célzó masszív támadókampányt fedeztek fel

(thehackernews.com)

A sysdig közölt információkat egy újabb kampányról, ami publikusan elérhető Git repo-kat célzott. A támadók klónozták az elérhető tárolókat, amivel további szolgáltatások hitelesítőadatait is meg tudták szerezni. **Bővebben...**

A Google javított két nulladik napi Android sebezhetőséget

(bleepingcomputer.com)

A Google a novemberi biztonsági frissítése során összesen 51 biztonsági hibát javított, köztük két aktívan kihasznált nulladik napi Android sebezhetőséget. **Bővebben...**

Tanulmány: A ChatGPT-4o hangvezérlési funkciója kihasználható pénzügyi csalások elkövetéséhez

(bleepingcomputer.com)

Kutatók egy új tanulmányban bizonyították, hogy vissza lehet élni az OpenAI valós idejű hangalapú API-jával pénzügyi csalások elkövetéséhez. A tanulmány különféle lehetséges csalástípusra terjedt ki, mint például a banki csalások, az ajándékutalványokkal való visszaélések, a kripto csalások, valamint a közösségi média- vagy a Gmail-fiókok hitelesítő adatainak ellopása.

Bővebben...

Aktuális tartalmak

Ne hagyjuk, hogy a kiberbűnözők lenyúlják a megtakarításainkat – SANS OUCH! – 2024. november

Megjelent a **SANS** és a Nemzetbiztonsági Szakszolgálat **Nemzeti Kibervédelmi Intézet** közös kiadványának **2024. novemberi száma**, melyben azzal foglalkozunk, hogyan védhetjük meg a csalóktól online pénzügyi fiókjainkat.

Elolvasom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el közösségi oldalainkra!

LinkedIn

Instagram

Facebook

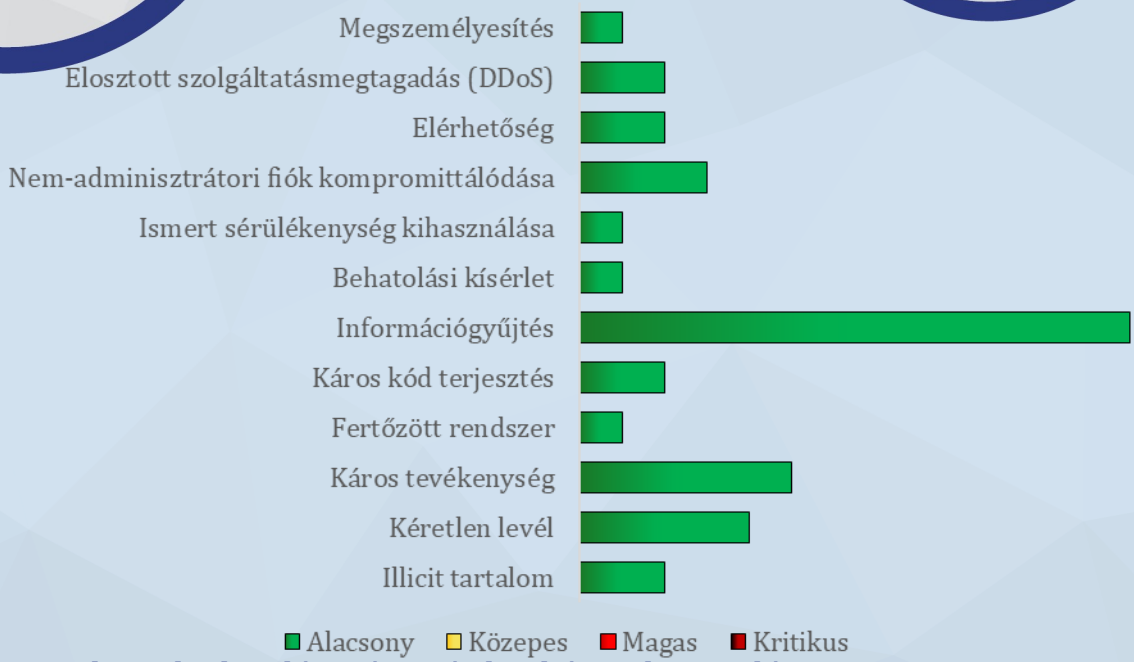
További hírekért, látogasson el **weboldalunkra**!

Statisztikai Adatok

2024.10.31.-2024.11.07.

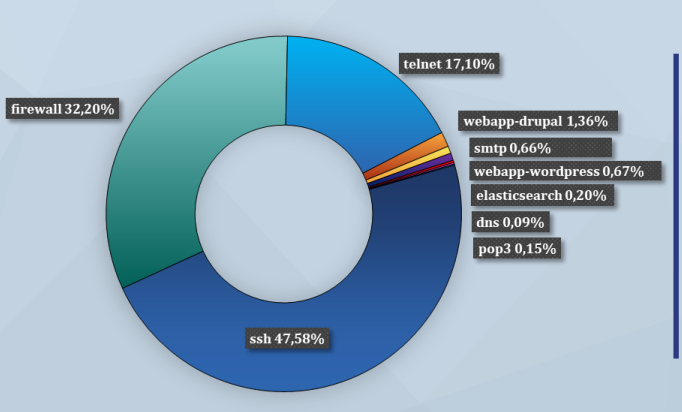
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

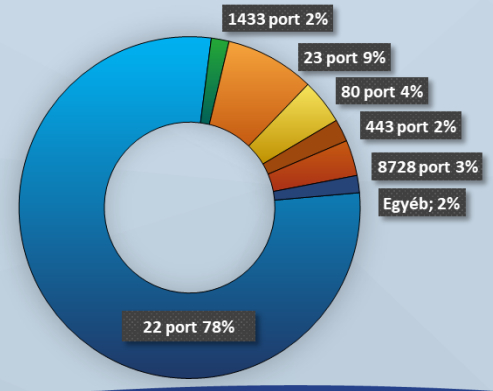
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!