NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 14. hét

HÍREK

- Valós az Oracle Cloud elleni adatszivárgás
- A Microsoft válasza a CrowdStrike incidensre
- Ez a szurikáta éberen figyeli a DNS MX rekordokat
- Kritikus sebezhetőség Canon nyomtató illesztőprogramokban
- Crocodilus: célkeresztben az Android-felhasználók

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

Valós az Oracle Cloud elleni adatszivárgás

(cloudsek.com – part-1)
(cloudsek.com – part-2)

A 2025. március 21-én a CloudSEK XVigil kutatói felfedezték, hogy egy “rose87168” nevű felhasználó 6 millió, állítólag az Oracle Cloud rendszeréből kiszivárgott rekordot árul egy darkweb fórumon. Az adatbázis tartalmai közé tartoznak JKS fájlok, LDAP, titkosított SSO jelszavak. **Bővebben...**

A Microsoft válasza a CrowdStrike incidensre

(bleepingcomputer.com)

A Microsoft nemrégiben bejelentett egy új Windows 11 funkciót, a Quick Machine Recovery-t, amely a rendszerindítási hibák és problémás illesztőprogramok gyors, távoli javítását teszi majd lehetővé. A Quick Machine Recovery a Windows Resiliency Initiative részeként jött létre. **Bővebben...**

Ez a szurikáta éberen figyeli a DNS MX rekordokat

(infoblox.com)

A Morphing Meerkat egy kifinomult phishing-as-a-service (PhaaS) platform, amely a DNS-over-HTTPS (DoH) protokollt alkalmazza a hagyományos biztonsági megoldások megkerülésére és az adathalász tevékenységek hatékonyságának növelésére. A DoH lényege, hogy a DNS lekérdezéseket titkosított HTTPS forgalomba ágyazza. **Bővebben...**

Crocodilus: célkeresztben az Android-felhasználók!

(bleepingcomputer.com)

Egy nemrég felfedezett rosszindulatú program, a Crocodilus, arra készteti az Android felhasználókat, hogy adják meg a kriptotárcájukhoz tartozó seed phrase-t (a kriptotárca biztonsági helyreállító kulcsát). A Crocodilus képes teljes hozzáférést szerezni az eszközhöz. **Bővebben...**

Kritikus sebezhetőség Canon nyomtató-illesztőprogramokban

(gbhackers.com)

A Canon nyomtató-illesztőprogramokat érintő, súlyos biztonsági sebezhetőségről tett közzé 2025. március 31-én cikket a GBHackers. A CVE-2025-1268 azonosítójú biztonsági rés tetszőleges kódfuttatást tehet lehetővé.
Bővebben...

Aktuális tartalmak

Fióklopások: érzelmi ragadozók SANS OUCH!

Megjelent a **SANS** és a **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** közös kiadványának **2025. áprilisi száma**, melyben bemutatjuk, hogy a csalók hogyan élhetnek vissza a **feltört közösségi média fiókjainkkal**, mitől lesznek ezek a csalások ennyire veszélyesek, illetve azt is, hogyan védhetjük meg magunkat tőlük.

Elolvasom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!

Linked in

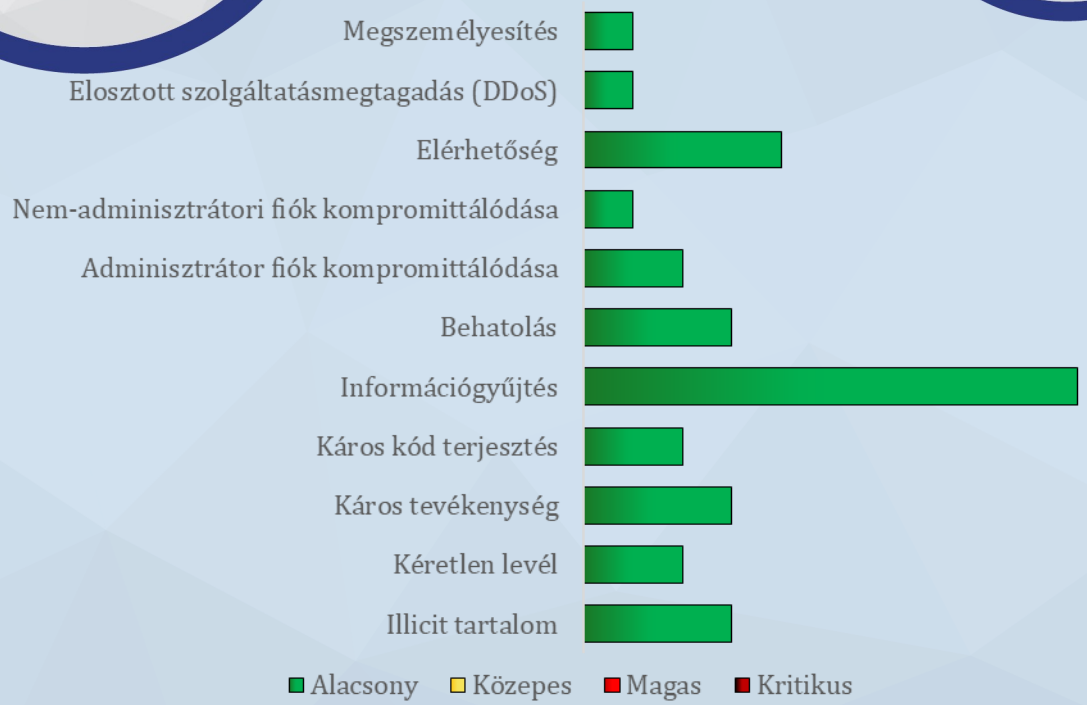
További érdekességekért, látogasson el **weboldalunkra**!

Statisztikai Adatok

2025.03.28.-2025.04.03.

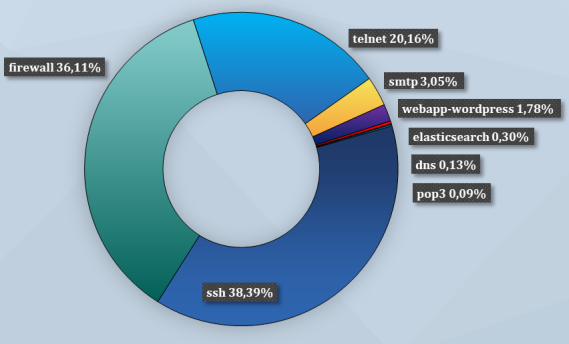
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

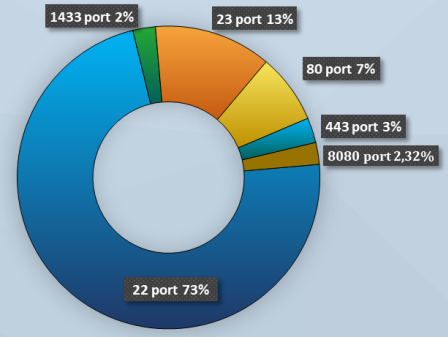
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

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





További hírekért, látogasson el **weboldalunkra**!