NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 16. hét

HÍREK

- Támadás alatt a mobilfizetési rendszerek
- Hackerek a volán mögött: így vették át az irányítást egy Nissan Leaf felett
- A Defender mostantól lekapcsolja a nem felügyelt végpontokat
- A Tycoon2FA adathalász készlet új módszerekkel célozza a Microsoft 365-öt
- MI által generált hibás kódfüggőségek – új ellátásilánc-kockázat

IT BIZTONSÁGI TIPP

- KiberKedd: Ne higgy a hihetetlenül vonzó ajánlatoknak!

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

Támadás alatt a mobilfizetési rendszerek
(gbhackers.com)

A pénzügyi csalások evolúciója napjainkra új szintre lépett. A kiberbűnözők egyre kifinomultabb módszerekkel használják ki az olyan mobilfizetési rendszereket, mint például az Apple Pay és a Google Wallet. A korábban mágnescsíkos kártyák másolására épülő csalások mára kezdik elveszíteni jelentőségüket. **Bővebben...**

Hackerek a volán mögött: így vették át az irányítást egy Nissan Leaf felett
(securityweek.com)

A PCAutomotive biztonsági kutatói a Black Hat Asia 2025 konferencián mutatták be, miként tudták távolról átvenni egy 2020-as gyártású, második generációs Nissan Leaf elektromos jármű teljes szoftveres és részben fizikai irányítását. **Bővebben...**

A Defender mostantól lekapcsolja a nem felügyelt végpontokat
(bleepingcomputer.com)

A Microsoft Defender for Endpoint új funkciója lehetővé teszi a még fel nem fedezett vagy a rendszerbe be nem csatlakoztatott eszközök automatikus hálózati elszigetelését, hogy megakadályozza a támadók oldalirányú mozgását és a támadások terjedését. **Bővebben...**

MI által generált hibás kódfüggőségek – új ellátásilánc-kockázat
(bleepingcomputer.com)

Azáltal, hogy a generatív AI eszközöket egyre többen használják programozásra, valamint azáltal, hogy a modellek az általuk generált kódban gyakran nem létező csomagnevekre hivatkoznak, megjelent egy új típusú ellátásilánc-támadási forma, a slopsquatting. **Bővebben...**

A Tycoon2FA adathalász készlet új módszerekkel célozza a Microsoft 365-öt
(bleepingcomputer.com)

A Tycoon2FA phishing-as-a-service (PhaaS) platform — amely arról ismert, hogy képes megkerülni a többfaktoros hitelesítést (MFA) a Microsoft 365 és Gmail fiókok esetében — olyan frissítéseket kapott, amelyek megnehezítik, hogy a biztonsági rendszerek felfedezzék a jelenlétét. **Bővebben...**

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

KiberPajzs
Védelem a pénzügyekben

KiberKedd: Ne higgy a hihetetlenül vonzó ajánlatoknak!

Manapság számtalan **hamis hirdetéssel találkozhatunk** a közösségi média különböző felületein, amelyek vonzó, nagy profitot ígérő kriptovaluta kereskedelmi oldalakat népszerűsítenek. **Ne legyünk naívak**: az ilyen ellenállhatatlan ajánlatok mögött általában csaló, rosszindulatú szándék áll.

E havi **KiberKedd** tippünkben szeretnénk **felhívni a figyelmet** néhány intő jelre, amivel **felismerhetjük** ezeket **a hamis weboldalakat és alkalmazásokat**.

Elolvasom

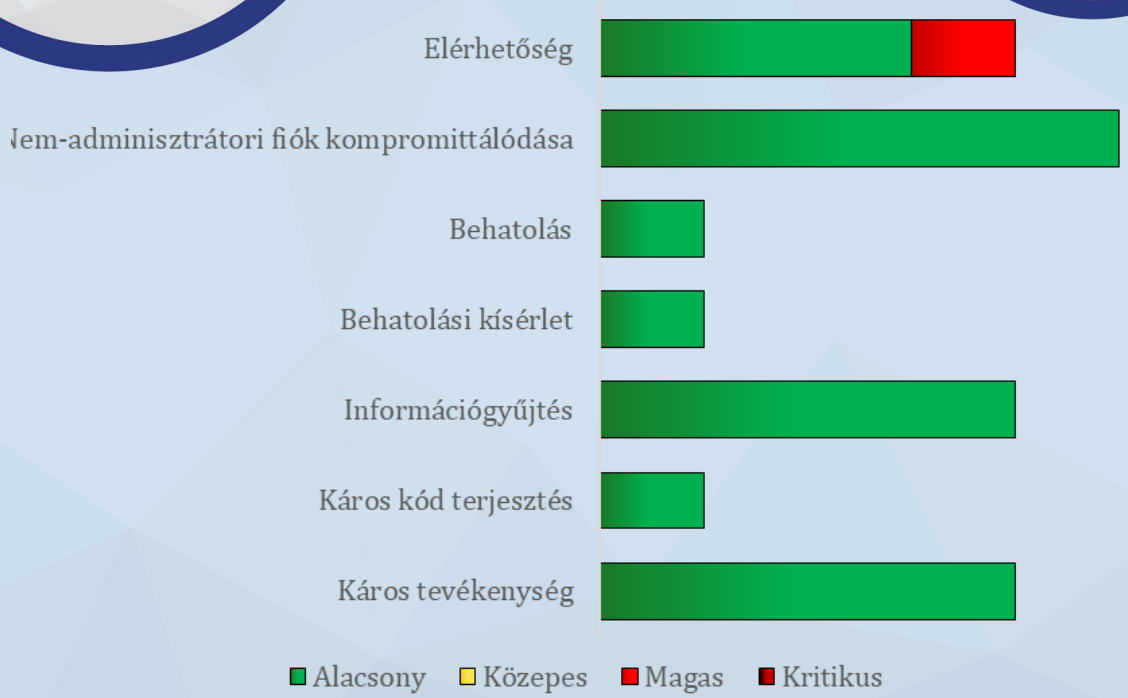
További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!

Statisztikai Adatok

2025.04.11.-2025.04.16.

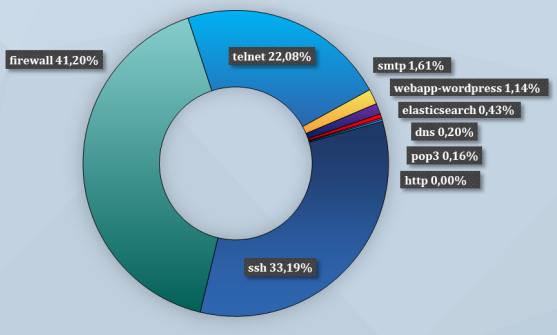
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

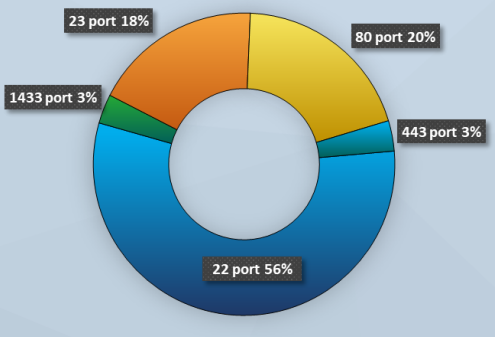
Fenyegetettségi szint: magas



Incidensek eloszlása típus és kockázati besorolás szerint

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





További hírekért, látogasson el **weboldalunkra**!