NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023.21. hét

HÍREK

- .ZIP, .MOV? Nem, nem fájlkiterjesztések, hanem új Top Level Domainek!
- Adatlopó malware-t találtak egyes NPM csomagokban
- Veszélyben lehet a KeePass jelszószéf tartalma!
- Frissítsen: Ismert módon kihasznált zero-day sérülékenységet javítottak Apple termékekben
- Samsung eszközöket használhattak kémkedésre

Heti IT biztonsági tipp

Az online piacteres csalások évek óta jelen vannak, ám a pandémia óta új módszerek is megjelentek. Mint mindig, ha tájékozottak vagyunk, könnyebben kikerülhetjük a csapdákat, e heti tippünkben ehhez szeretnénk segítséget nyújtani.

STATISZTIKAI ADATOK

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

CTI ELEMZÉS

Adathalász csalások, visszaélések a bankok nevében

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

NEWS

IT biztonsági
HÍREK

.ZIP, .MOV? Nem, nem fájlkiterjesztések, hanem új Top Level Domainek!

(wired.com)

A Google bejelentette nyolc új TLD kiadását (mint például a „.dad” és a „.nexus”), amelyek között akad olyan, amit nem fogadott egyöntetűen pozitívan az IT-biztonsági közösség. Egyesek szerint a „.zip” és „.mov” végződésű domainek alkalmasak lehetnek adathalászatra és más típusú online csalásokra. **Bővebben...**

Adatlopó malware-t találtak egyes NPM csomagokban

(securityaffairs.com)

A ReversingLabs két rosszindulatú csomagot (nodejs-encrypt-agent és nodejs-cookie-proxy-agent) fedezett fel az npm repositoryjában, amelyek **TurkoRatet** tartalmaznak. **Bővebben...**

Veszélyben lehet a KeePass jelszószéf tartalma!

(securityaffairs.com)

Egy biztonsági kutató PoC eszközt adott közre “KeePass 2.X Master Password Dumper” néven, amely lehetővé teszi a KeePass mesterjelszó lekérdezését. Az eszköz a KeePass eddig még nem javított, CVE-2023-32784 néven nyomon követett sebezhetőségét használja ki arra, hogy a KeePass 2.x verziók esetén a memóriájából kinyerje a mesterjelszót. **Bővebben...**

Frissítsen: Ismert módon kihasznált zero-day sérülékenységet javítottak Apple termékekben

(bleepingcomputer.com)

Az Apple többek között három nulladik napi sérülékenységhez adott ki biztonsági hibajavítást. A sebezhetőségeket a gyártói biztonsági közlemény szerint fenyegetési szereplők feltételezhetően aktívan kihasználják. **Bővebben...**

IT biztonsági
TIPP

Samsung eszközöket használhattak kémkedésre

(thehackernews.com)

A CISA egy közepes súlyosságú, Samsung készülékeket érintő biztonsági hiba aktív kihasználására figyelmeztetett. A CVE-2023-21492 a 11-es, 12-es és 13-as Android verziót futtató egyes Samsung készülékekre nézve jelent biztonsági kockázatot. A Samsung a problémát információfeltárási hibaként írta le, amelyet kihasználva egy privilegizált támadó megkerülheti az ASLR védelmet. **Bővebben...**

IT biztonsági Tipp

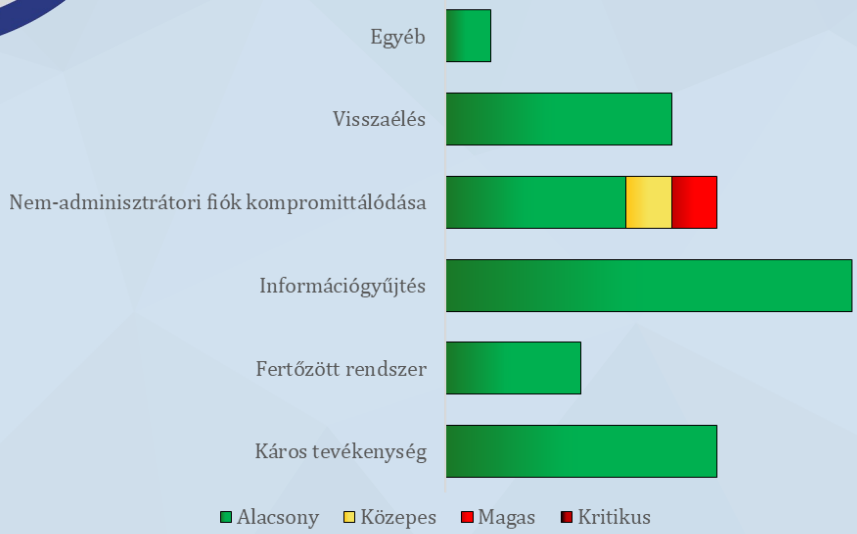
Az NBSZ NKI weboldalán a tipikus online piacteres csalásokkal szembeni védekezésről olvashat bővebben.

Statisztikai adatok

2023.05.19-2023.05.25.

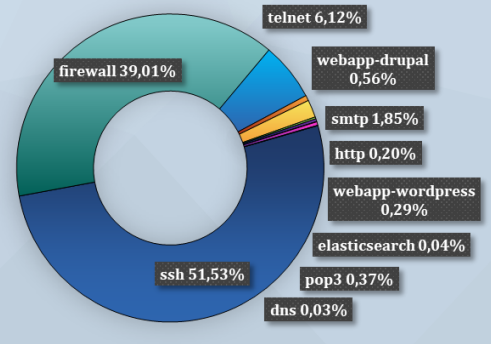
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

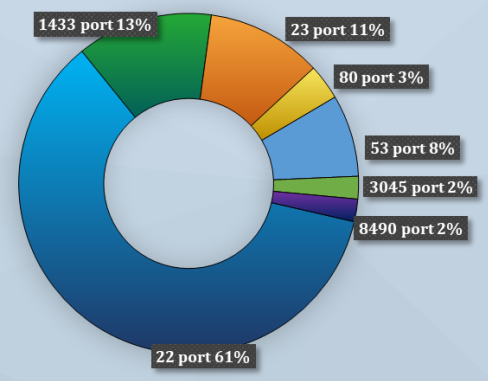
Fenyegetettségi szint: magas



Incidensek eloszlása típus és kockázati besorolás szerint

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





További információkért, látogasson el **weboldalunkra**!

Aktuális tartalmak

KIBERTÁMADÁS!
PODCAST

Adathalász csalások, visszaélések a bankok nevében

CTI jelentés

Az adathalász támadások célja, hogy a kiberbűnözők az áldozatoktól bizalmas adatokat tulajdonítsanak el. Jelen kiberbiztonsági elemzésünkben a leggyakoribb pénzügyi adathalász technikákat és az ellenük való védekezési javaslatokat mutatjuk be.

Elolvasom

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu