NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 35. hét

HÍREK

- A 'sedexp' Linux malware éveken át észrevétlen maradt
- Kézikönyv készült a szervezetek eseménynaplózásának meghatározásához
- Letartóztatták a Telegram alapítóját
- A SonicWall javított egy kritikus tűzfal sérülékenységet
- Az NGate nevű új Android malware képes ellopni a bankkártya adatokat

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

A ’sedexp’ Linux malware éveken át észrevétlen maradt

(bleepingcomputer.com)

A ’sedexp’ névre hallgató kifejezetten jól rejtőzködő linux malware 2022 óta sikeresen kerüli el a felismerést egy olyan persistence módszer alkalmazásával, ami még nincs benne a MITTRE ATT@CK keretrendszerben. **Bővebben...**

Kézikönyv készült a szervezetek eseménynaplózásának meghatározásához

(securityweek.com)

A “Best Practices for Event Logging and Threat Detection” (PDF) címet viselő dokumentum az eseménynaplózásra és a fenyegetésészlelésre összpontosít, miközben részletezi azokat az úgynevezett “living-off-the-land” (LOTL) technikákat, amelyeket a támadók használnak, és kiemeli a biztonsági gyakorlatok fontosságát a fenyegetések megelőzése érdekében. **Bővebben...**

Letartóztatták a Telegram alapítóját

(securityaffairs.com)

Pavel Durovot, a Telegram alapítóját és vezérigazgatóját szombat este tartóztatták le a Párizs melletti Bourget repülőtéren. A helyi média szerint a letartóztatás egy franciaországi nyomozás miatt történt, amely a Telegram moderálásának hiányával kapcsolatos, ami a hatóságok szerint segíti bűnözést. **Bővebben...**

A SonicWall javított egy kritikus tűzfal sérülékenységet

(thehackernews.com)

A SonicWall biztonsági frissítést adott ki tűzfalai számára, amiben javítja a CVE-2024-40766 néven nyomon követett, 9.3-as CVSS ponttal értékelt kritikus sérülékenységet. **Bővebben...**

Az NGate nevű új Android malware képes ellopni a bankkártya adatokat

(bleepingcomputer.com)

A kampány kapcsolódik az ESET nemrégiben kiadott jelentéséhez, amely a progresszív webes alkalmazások (PWA-k) és fejlett WebAPK-k fokozott használatáról szól, amelyekkel banki hitelesítő adatokat lopnak el.
Bővebben...

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT Fortes fortuna adiuvat

A keresőmotorok működése

CTI jelentés

Jelen dokumentum célja, hogy bemutassa a keresőmotorok fejlődési útját, különböző mechanizmusait, illetve rávilágítson a lehetséges csalási formákra.

Elolvasom

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

LinkedIn

Instagram

Facebook

Statisztikai Adatok

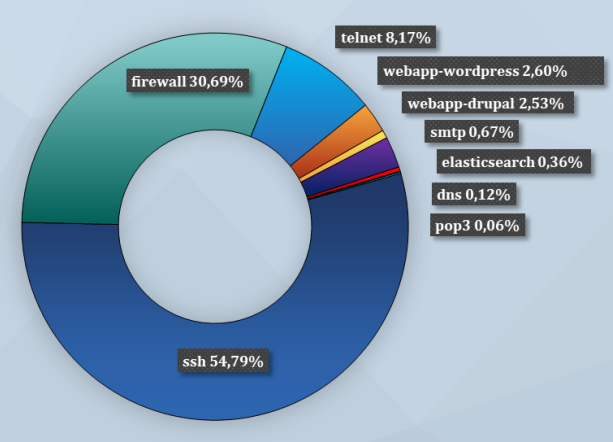
2024.08.23.-2024.08.29.

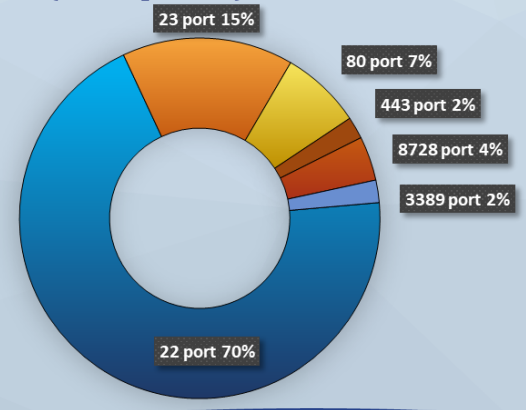
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony

Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!