NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 13. hét

HÍREK

- 19 millió egyszerű szöveges jelszó került nyilvánosságra a rosszul konfigurált Firebase példányok miatt
- Ne dőljünk be a csalóknak, továbbra sincs poggyász kiárusítás a reptéren!
- A CISA három sérülékenységet vett fel a KEV-be
- A WINELOADER backdoor kihasználásával támad az APT29-es csoport
- A Sign1 malware kampány során több mint 39 ezer WordPress oldal fertőződött meg

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

További érdekességekért, látogasson el **weboldalunkra**!

NEWS

IT biztonsági

HÍREK

19 millió egyszerű szöveges jelszó került nyilvánosságra a rosszul konfigurált Firebase példányok miatt

(bleepingcomputer.com)

Három kiberbiztonsági kutató közel 19 millió egyszerű szöveges jelszót talált a weben a Firebase (Google által támogatott alkalmazásfejlesztési platform) rosszul konfigurált példányai miatt.**Bővebben...**

Ne dőljünk be a csalóknak, továbbra sincs poggyász kiárusítás a reptéren!

Intézetünkhöz bejelentés érkezett egy hamis Facebook oldal kapcsán, amely a Budapest Liszt Ferenc Nemzetközi Repülőtér (Budapest Airport – BUD) nevével visszaélve csaló posztokat és hirdetéseket jelenít meg, amelyek adatlopást végző (adathalász) weboldalakra vezetik a gyanútlanul kattintókat. **Bővebben...**

A WINELOADER backdoor kihasználásával támad az APT29-es csoport

(securityaffairs.com)

Az APT 29 a WINELOADER backdoor egy új változatát használja fel német politikai pártok ellen. A Mandiant szerint ez az első alkalom, melyben arra figyeltek fel, hogy a csoport politikai pártokat célzott meg. **Bővebben...**

A Sign1 malware kampány során több mint 39 ezer WordPress oldal fertőződött meg

(securityaffairs.com)

A Sucuri biztonsági kutatói által felfedezett, Sign1 néven nyomon követhető malware kampány az elmúlt hat hónapban már több, mint 39 ezer WordPress oldalt veszélyeztetett. **Bővebben...**

A CISA három sérülékenységet vett fel a KEV-be

(securityaffairs.com)

Az amerikai CISA felvett három sebezhetőségeket a KEV katalógusába. A sebezhetőségeket jelenleg aktívan kihasználják támadásokban.

CVE-2023-48788
CVE-2021-44529
CVE-2019-7256

Bővebben...

Aktuális tartalmak

A kriptovaluták veszélyei

CTI jelentés

Manapság igen népszerűvé váltak a különböző kriptovaluták. Rengeteg történet kering róluk a médiában, az interneten, néhányan a gyors meggazdagodást látják benne, néhányan a jövő pénztechnológiájának gondolják, és persze ki ne hallott volna a férfiról, aki 2010-ben 2 darab pizzát rendelt 10 000 Bitcoinból, ami mai árfolyamon körülbelül 150 milliárd forintot érne.

A **KiberPajzs együttműködés** keretében a tipikus csalási módok bemutatásában partnerünk volt az **Országos Rendőr-főkapitányság Bűnügyi Főigazgatóság Bűnügyi Főosztálya**.

A legjobb védekezés a tájékozódás, így ezt a CTI jelentést ajánljuk minden olvasónknak, aki kriptovalutákkal bármilyen módon tevékenykedni tervez vagy csak szeretne egy kicsit elmélyülni a témában.

Elolvasom

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

LinkedIn

Instagram

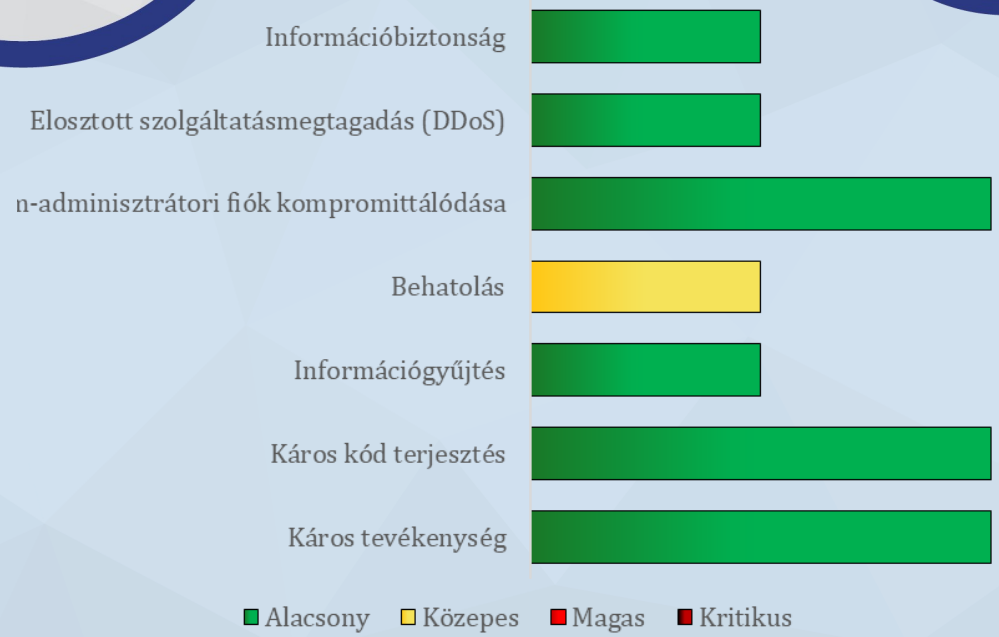
Facebook

Statisztikai Adatok

2024.03.22.-2024.03.27.

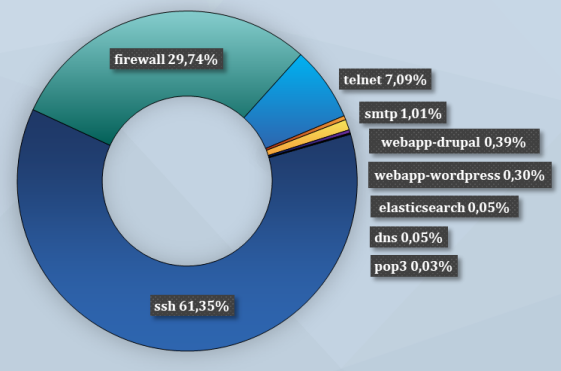
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

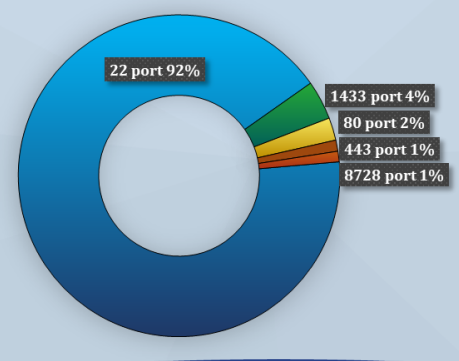
Fenyegetettségi szint: közepes



Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!