NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 31. hét

HÍREK

- Szakértők a bankszektor elleni OSS SCA támadásokra figyelmeztetnek
- Újabb aktívan kihasznált sérülékenységről közölt információt az Ivanti
- Kibertámadás érhette Izrael legnagyobb olajfinomítóját
- 800 000 WordPress weboldal vált sebezhetővé a Ninja Forms Plugin miatt
- Optikai karakterfelismeréssel lop érzékeny adatokat a CherryBlos malware

STATISZTIKAI ADATOK

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

CTI ELEMZÉS

APT csoportok

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági
HÍREK

Szakértők a bankszektor elleni OSS SCA támadásokra figyelmeztetnek

(securityaffairs.com)

2023 első felében a Checkmarx kutatói több, a bankszektort célzó, nyílt forráskódú szoftverek ellátási láncát (Open Source Software Supply Chain Attacks) érintő támadást észleltek, amelyek során a támadók a bankok által használt webes eszközök bizonyos komponenseit célozták meg. **Bővebben...**

Újabb aktívan kihasznált sérülékenységről közölt információt az Ivanti

(therecord.media)

Az Ivanti MDM termékének (EPMM) egy kritikus sebezhetőségét (CVE-2023-35078) fenyegetési szereplők kihasználták norvég államigazgatási szervek elleni támadások során. A tech cég néhány napja egy újabb sebezhetőségről (CVE-2023-35081) közölt információkat. **Bővebben...**

Kibertámadás érhette Izrael legnagyobb olajfinomítóját

(bleepingcomputer.com)

Izrael legnagyobb olajfinomító üzemeltetőjének, a BAZAN Groupnak a honlapja a világ legtöbb pontjáról elérhetetlen, mivel a fenyegetési aktorok azt állítják, hogy feltörték a csoport rendszereit. **Bővebben...**

Optikai karakterfelismeréssel lop érzékeny adatokat a CherryBlos malware

(thehackernews.com)

Veszélyes új malware technikára hívja fel a figyelmet a Trend Micro. Az új, CherryBlos nevű Android malware ún. optikai karakterfelismerő (Optical Character Recognition – OCR) technikát használ a képeken tárolt érzékeny adatok megszerzésére. **Bővebben...**

800 000 WordPress weboldal vált sebezhetővé a Ninja Forms Plugin miatt

(thehackernews.com)

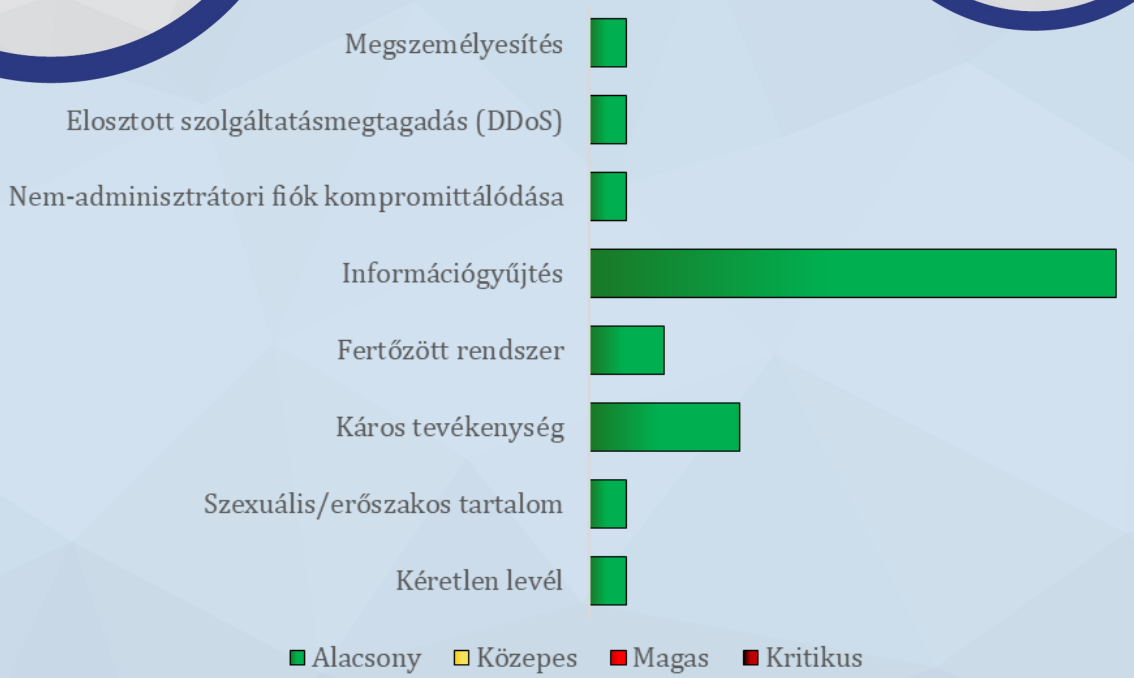
Több biztonsági rés is nyilvánosságra került a WordPress Ninja Forms pluginjában, amelyek kihasználása jogosultság-kiterjesztését és érzékeny adatok ellopását teheti lehetővé illetéktelen számára az érintett weboldalon. **Bővebben...**

Statisztikai adatok

2023.07.28.-2023.08.03.

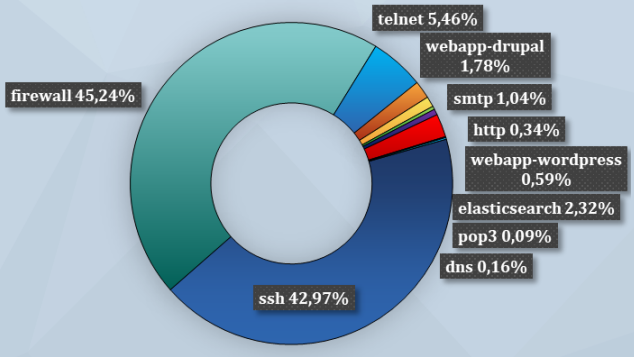
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

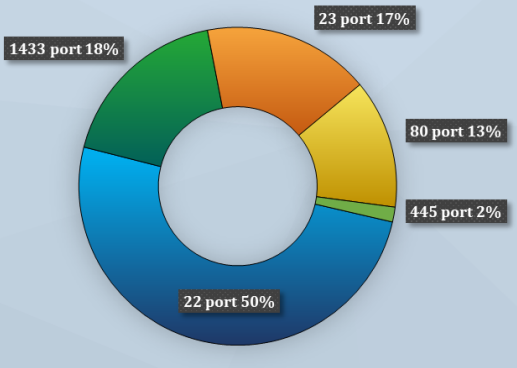
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

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





További információkért, látogasson el **weboldalunkra**!

Aktuális tartalmak

KIBERTÁMADÁS! PODCAST

APT csoportok

CTI jelentés

Jelen dokumentum célja, hogy bemutassa az APT csoportok legfőbb jellemzőit, támadásaik, eszközkészleteik jellegzetességeit, valamint a céljaik és motivációjuk sajátosságait.

A jelenlétük nem újdonság, az első ismert támadást az 1990-es évek végén dokumentálták.

TUDTAD?

Elolvasom

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu