NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 23. hét

HÍREK

- Kalóz Microsoft Office csomaggal terjesztik a malwareket
- A Check Point frissítéseket publikált a VPN-eket érintő sérülékenységek javítására
- Az új V3B adathalász készlettel európai bankok ügyfeleit célozzák meg
- A Synnovis-t ért ransomware támadásban több londoni kórház is érintett
- Publikálták az Atlassian Confluence RCE sérülékenységének részleteit

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

Kalóz Microsoft Office csomaggal terjesztik a malwareket

(bleepingcomputer.com)

A kiberbűnözők a torrentoldalakon a Microsoft Office feltört verzióin keresztül terjesztenek rosszindulatú programokat. Ezt a jelenleg is futó kampányt az AhnLab Security Intelligence Center (ASEC) azonosította. **Bővebben...**

A Check Point frissítéseket publikált a VPN-eket érintő sérülékenységek javítására

(bleepingcomputer.com)

A Check Point javításokat publikált egy olyan VPN-eket érintő nulladik napi sérülékenységhez, amelyet a tűzfalakhoz való távoli hozzáférés megszerzésére irányuló támadásokban használnak ki. **Bővebben...**

Az új V3B adathalász készlettel európai bankok ügyfeleit célozzák meg

(bleepingcomputer.com)

A Resecurity kutatói fedezték fel az új "V3B" elnevezésű adathalász szolgáltatást (Phishing-as-a-Service – PhaaS), melyet a hackerek a Telegramon népszerűsítenek. Ezzel jelenleg 54 nagy pénzügyi intézet ügyfeleit célozzák szerte Európában. **Bővebben...**

A Synnovis-t ért ransomware támadásban több londoni kórház is érintett

(securityaffairs.com)

A Synnovis patológiai és diagnosztikai részlegét ért támadás számos londoni kórház működésében okozott komoly zavarokat. A támadás miatt az érintett kórházakban félbe kellett szakítani egészségügyi ellátásokat. **Bővebben...**

Publikálták az Atlassian Confluence RCE sérülékenységének részleteit

(securityweek.com)

A SonicWall megosztotta a nemrég felfedezett Confluence-ben lévő súlyos RCE hiba technikai részleteit. A **CVE-2024-21683** néven nyomon követett RCE hiba a függvény input validálási mechanizmusában rejlik – lehetővé teszi a felhasználók számára, hogy új kódblokk makró nyelvi definíciót adjanak hozzá.

Bővebben...

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

KIBERTÁMADÁS! PODCAST

Gyakori kriptovalutás csalások [örökzöld]

Te tudod mi a különbség kriptoponzik és a piramisjátékok között?

Gondolkodtál már azon, "vajon hány giga a Bitcoin?" vagy hogy mennyire megbízhatóak az interneten hirdetett automata kereskedő botok?

Kibertámadás!
adásunkban
Tamás és Olivér
beszélgetnek a kriptovalutákról és az azokat érintő leggyakoribb csalásokról. Olivér elmeséli saját tapasztalatait is, így megtudhatjuk mikre kell odafigyelni, hogy ne váljunk a kriptocsalások áldozataivá, és ezen felül a fentebb feltett kérdésekre is választ kaphatunk.

Meghallgatom

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

LinkedIn

Instagram

Facebook

Statisztikai Adatok

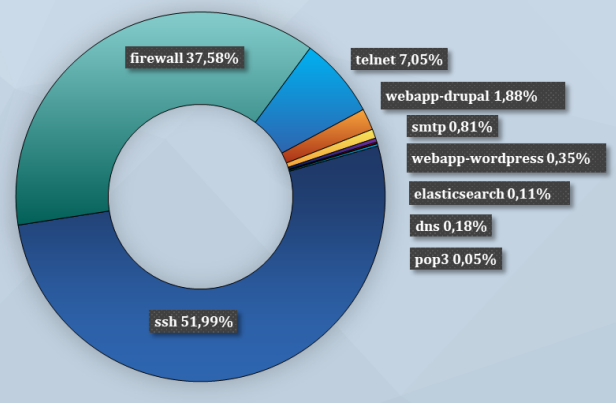
2024.05.31.-2024.06.06.

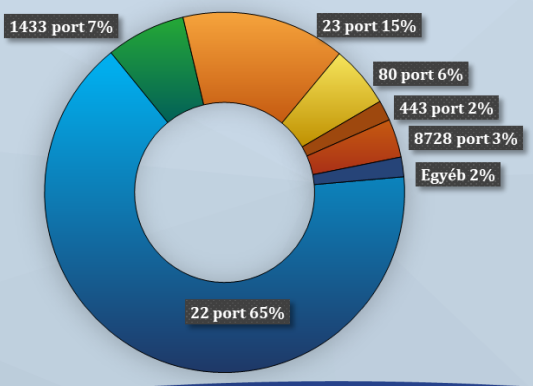
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes

Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!