NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 39. hét

HÍREK

- Typosquatting technika – egy karakternyi eltérés is számít a weboldalak címében
- Több, mint 800 amerikai iskolát ért kibertámadás a MOVEit Transfer nulladik napi sebezhetőségét kihasználva
- Már aktívan használják a deepfake technikát a kibertámadások során
- Akcióban egy új APT csoport
- A BBTok trójai több mint 40 latin-amerikai bankot vett célba

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

Typosquatting technika – egy karakternyi eltérés is számít a weboldalak címében

(bleepingcomputer.com)

Egy új jelszólopó káros programot fedeztek fel, amelynek terjesztéséhez a kiberbűnözők a népszerű nyílt-forráskódú jelszókezelő, a Bitwarden népszerűségét igyekeztek kihasználni. **Bővebben...**

Több, mint 800 amerikai iskolát ért kibertámadás a MOVEit Transfer nulladik napi sebezhetőségét kihasználva

(bleepingcomputer.com)

Az amerikai oktatási nonprofit szervezet, a National Student Clearinghouse (NSC) nyilvánosságra hozta, hogy 890, a szolgáltatásait használó iskolát érintő adatszivárgás történt az Egyesült Államokban. **Bővebben...**

Akcióban egy új APT csoport

(bleepingcomputer.com)

A Gelsemium egy 2014 óta működő kiberkémkedésre specializálódott csoport, amely Kelet-Ázsia és a Közel-Kelet kormányzati, oktatási és elektronikai gyártóit veszi célba. **Bővebben...**

A BBTok trójai több mint 40 latin-amerikai bankot vett célba

(thehackernews.com)

A Kubernetes-ben felfedezett három magas kockázati besorolású sérülékenység (CVE-2023-3676, CVE-2023-3893, CVE-2023-3955, CVSS 8,8) kihasználásával az egy klaszteren belüli Windows végpontokon emelt jogosultságokkal történő távoli kódfuttatás (RCE) érhető el. **Bővebben...**

Számos alkalmazást érint a Chrome hibának „indult" libwebp sebezhetőség

(arstechnica.com)

A Google két hete javította a CVE-2023-4863 azonosítón jegyzett sebezhetőséget, amelyről biztonsági kutatók később megállapították, hogy annak eredője valójában a széleskörben alkalmazott **libwebp** nyílt forráskódú programkönyvtár, ami a WebP képformátum kezelésére szolgál. A libwebp könyvtár számos projekt, operációs rendszer és alkalmazás használja, köztük a Signal, a 1Password, a Mozilla Firefox, a Microsoft Edge, az Apple Safari, valamint az Electron nevű keretrendszer, amire Microsoft termékek épülnek (Teams, Visual Studio Code), illetve olyan szoftverekben is megtalálható, mint például a 1Password, a Bitwarden, a GitHub Desktop, vagy a Twitch. **Bővebben...**

További hírekért, látogasson el **weboldalunkra**!

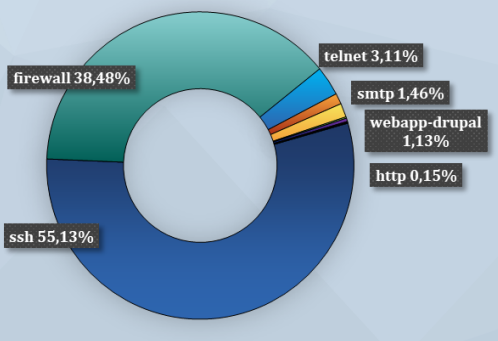
Statisztikai adatok

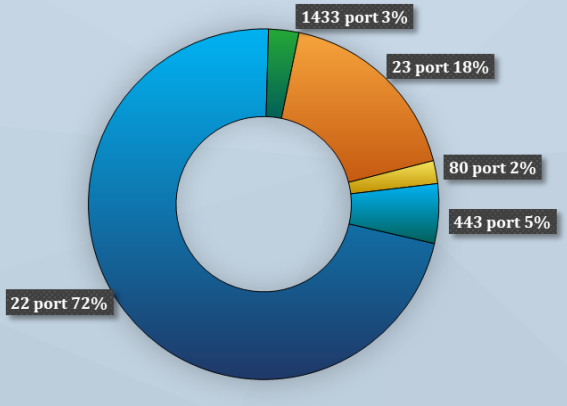
2023.09.22.-2023.09.28.

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**!