NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2022.36. hét

HÍREK

- Pályázati lehetőség – szakértőként most Ön is az ENISA tanácsadói csoport tagjává válhat
- Most Kína vádolja kibertámadással az Amerikai Egyesült Államokat
- Súlyos sérülékenység érint egyes Cisco routereket, javítás azonban nem várható
- Kibertámadás érte a The North Face weboldalát, vásárlói adatok is veszélybe kerültek
- Visszatért a SharkBot a Google Play-re

Heti IT biztonsági tipp

- Jön az iOS 16, így frissítsünk biztonságosan

STATISZTIKAI ADATOK

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

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK,

Tájékoztatás hamis vírusirtó alkalmazásokkal kapcsolatban

PODCAST

Az Internet sötét oldala

[örökzöld]

További érdekességekért, látogasson el **weboldalunkra**!

NEWS

IT biztonsági HÍREK

Pályázati lehetőség – szakértőként most Ön is az ENISA tanácsadói csoport tagjává válhat

(enisa.europa.eu)

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) szakértők számára pályázati felhívást tett közzé, hogy részt vehessenek a tanácsadó csoport (ENISA Advisory Group) munkájában. **Bővebben...**

Most Kína vádolja kibertámadással az Amerikai Egyesült Államokat

(securityaffairs.co)

A Kínai Nemzeti Számítógépes Vírus-Vészhelyzeti Központ (CVERC), illetve a Qihoo 360 nevű kiberbiztonsági cég közös jelentése szerint az NSA több tízezer kibertámadást indított kínai számítógépes hálózatok ellen az elmúlt évek során. **Bővebben...**

Súlyos sérülékenység érint egyes Cisco routereket, javítás azonban nem várható

(bleepingcomputer.com)

Több kisvállalat is érintett lehet egyes VPN routerek egy nemrég felfedezett zero day sérülékenységében (CVE-2022-20923), ami egy hibás jelszóellenőrzési algoritmusból ered. **Bővebben...**

Kibertámadás érte a The North Face weboldalát, vásárlói adatok is veszélybe kerültek

(bleepingcomputer.com)

2022. július 26-án vette kezdetét a The North Face ruházati áruházlánc weboldala elleni kibertámadás, amelynek során a hackereknek közel 200 000 felhasználói fiókot sikerült kompromittálniuk. **Bővebben...**

IT biztonsági TIPP

Visszatért a SharkBot a Google Play-re

(bleepingcomputer.com)

Ez idáig két androidos alkalmazásban fedezték fel a SharkBot káros program egy újabb verzióját, aminek célja továbbra is a banki bejelentkezési adatok megszerzése. Az NCC group-hoz tartozó Fox IT blogbejegyzése szerint a szóban forgó két alkalmazás a **Mister Phone Cleaner** és a **Kylhavy Mobile**. Ezek az alkalmazás-boltban még nem tartalmazták a káros kódot, az csupán egy későbbi frissítéssel került az appokba, így kerülve meg a Google Play Store védelmét. **Bővebben...**

IT biztonsági Tipp

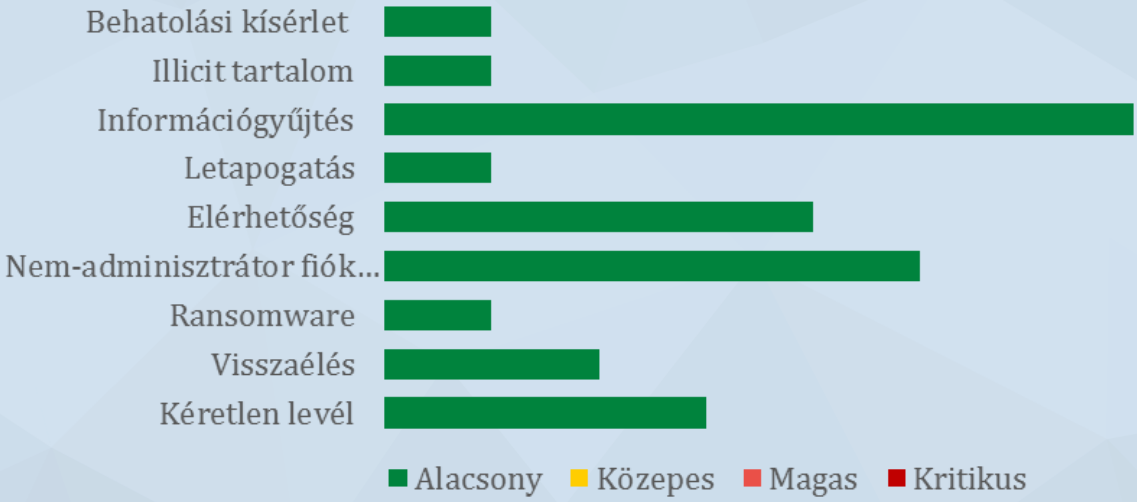
Az NBSZ NKI weboldalán összegyűjtöttük azokat az intézkedéseket, amelyeket érdemes egy iOS verziófrissítés előtt elvégezni.

Statisztikai adatok

2022.09.02.-2022.09.08.

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

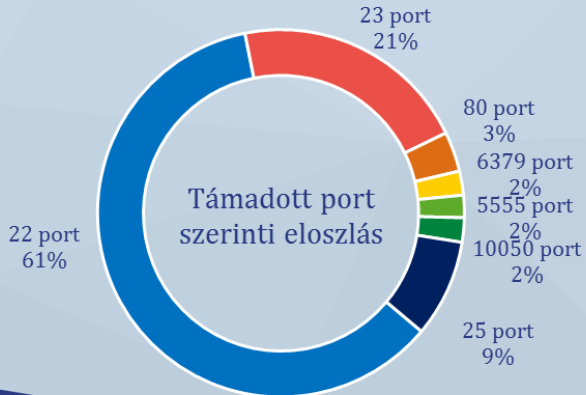
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

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

Események eloszlása csapdatípusok alapján



További információkért, látogasson el **weboldalunkra**!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Aktuális tartalmak

Tájékoztatás hamis vírusirtó alkalmazásokkal kapcsolatban

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **tájékoztatót** ad ki **hamis vírusirtó alkalmazásokkal kapcsolatban.**

A **Sharkbot** egy androidos készülékekre készített „újgenerációs” trójai program, amely elsősorban kompromittált eszközökről **pénzátutalások kezdeményezésére** szakosodott, azáltal, hogy **képes automatikusan kitölteni** a fertőzött eszközre telepített **legális banki alkalmazások mezőit,** illetve akár **teljes távoli hozzáférést** biztosíthat a fertőzött eszközön a támadó számára.

A káros kód számos káros funkcióval rendelkezik, képes például **billentyűnaplózásra, SMS üzenetek** elfogására, legutóbbi verziója pedig az internetes „sütikhez” is hozzáférhet. (Utóbbi azért veszélyes, mivel azok olyan szoftver- és helymeghatározási paramétereket tartalmazhatnak, amelyek segíthetnek megkerülni az ujjlenyomat-ellenőrzéseket, vagy bizonyos esetekben a felhasználói hitelesítéshez szükséges tokent is.)

Elolvasom

Az Internet sötét oldala [örökzöld]

podcast

A hírekben gyakran hallunk a darkwebről, mint az Internet sötét bugyráról. A mai adásból kiderül mi is ez pontosan, kik és mire használják, illetve, hogy milyen veszélyeket rejt magában.

Meghallgatom

További érdekességekért, látogasson el Facebook oldalunkra!