NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2022.31. hét

HÍREK

- Zsarolóvírus támadás ért egy európai energia-szolgáltatót
- Twitter API kulcsokat szivárogtat több mint 3200 alkalmazás
- Már az adathalászok is visszaszámlálóval sürgetik áldozataikat
- Windows, Adobe nulladik napi hibákat használ ki egy új kiberbűnözői csoport
- Rosszindulatú android alkalmazásokat hirdetnek a Facebookon, érdemes vigyázni!

Heti IT biztonsági tipp

- Az adományozási csalások egy másik formája – rövid esettanulmány

STATISZTIKAI ADATOK

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

CTI ELEMZÉS

Malware-ek típusai

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

NEWS

IT biztonsági
HÍREK

Zsarolóvírus támadás ért egy európai energiaszolgáltatót

(bleepingcomputer.com)

Az ALPHV — vagy ismertebb nevén BlackCat — zsarolóvírus csoport vállalta magára a luxemburgi Creos elleni kibertámadást. A cég öt európai államban van jelen földgáz vezeték és villamosenergia hálózatüzemeltetőként, utóbbi kapcsán kis mértékben (kb. 15%) termelő is. **Bővebben...**

Twitter API kulcsokat szivárogtat több mint 3200 alkalmazás

(techcommunity.microsoft.com)

A CloudSEK kiberbiztonsági kutatói 3207 olyan mobilalkalmazást fedeztek fel, amelyeken keresztül Twitter API kulcsok szivárognak, és a hiba kihasználásával egy támadó potenciálisan átveheti a felhasználók Twitter fiókjai feletti irányítást. **Bővebben...**

Már az adathalászok is visszaszámlálóval sürgetik áldozataikat

(infosecurity-magazine.com)

A Cofense által nemrég felfedezett „gyanús bejelentkezésről" szóló adathalász kampány során – a zsarolóvírus támadásokhoz hasonlóan – egy pánikkeltő visszaszámláló hajszolja rossz döntésekbe a felhasználókat. **Bővebben...**

Windows, Adobe nulladik napi hibákat használ ki egy új kiberbűnözői csoport

(darkreading.com)

A Microsoft jelentése szerint a világ különböző országaiban működő ügyvédi irodák, bankok és tanácsadó cégek elleni számos kémprogram támadás mögött egy „Knotweed" nevű kiberbűnözői csoport áll. **Bővebben...**

IT biztonsági
TIPP

Rosszindulatú android alkalmazásokat hirdetnek a Facebookon, érdemes vigyázni!

(bleepingcomputer.com)

Facebook hirdetésekkel népszerűsítik a McAfee által felfedezett adware kampány alkalmazásait, amelyek androidos rendszertisztító- és optimalizáló alkalmazásnak adják ki magukat a Play Store-on. A kampányban részvevő alkalmazásokból hiányzik az összes ígért funkció, helyettük reklámokat jelenítenek meg, és igyekeznek minél tovább rejtve maradni a felhasználók elől. **Bővebben...**

IT biztonsági Tipp

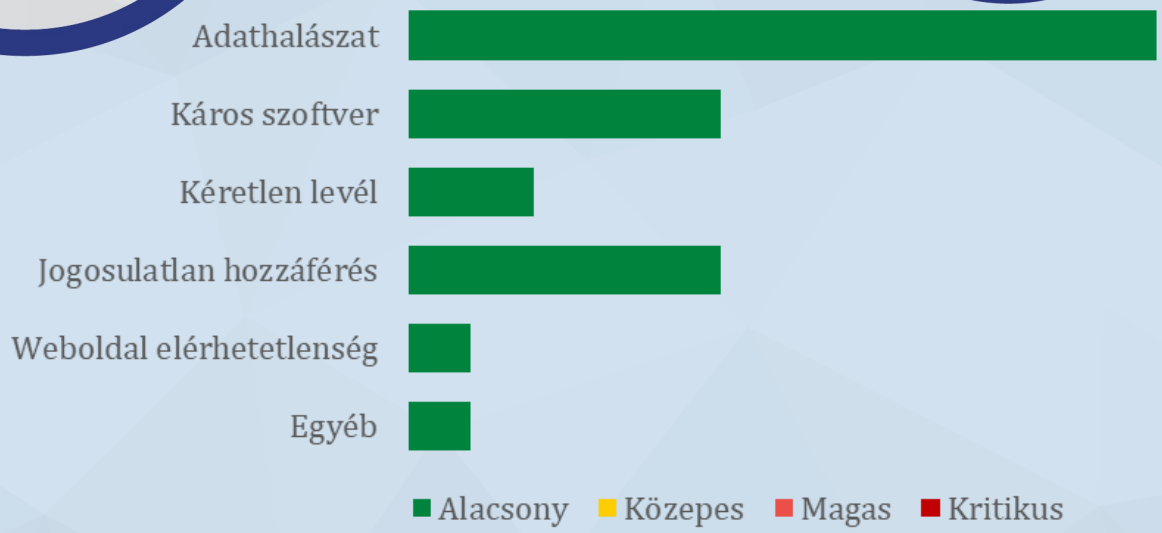
Az NBSZ NKI weboldalán egy rövid, átfogó esettanulmányt olvashat az adományozási csalások egy új formájáról.

Statisztikai adatok

2022.07.29.-2022.08.04.

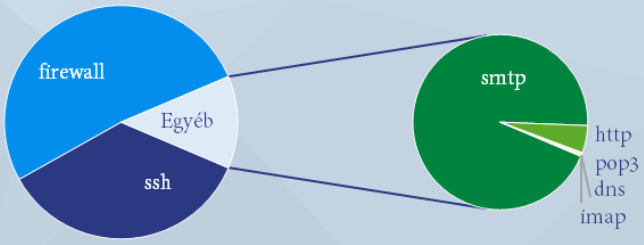
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes

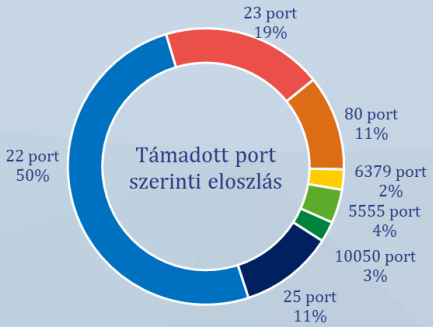


Incidensek eloszlása típus és kockázati besorolás szerint

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



Események eloszlása csapdatípusok alapján



További információkért, látogasson el **weboldalunkra**!

Aktuális tartalmak

KIBERTÁMADÁS! PODCAST

Ransomware as a Service (RaaS) – Zsarolóvírus-szolgáltatás

CTI jelentés

A zsarolóvírus vagy zsarolóprogram olyan szoftver, amely valamilyen módszer alapján zárol egy számítógépet vagy titkosítás útján **elérhetetlenné tesz egyes fájlokat a tulajdonosa számára**. A bűnözők ígéretei alapján ezeket csak a megadott **váltságdíj kifizetése után teszik újra elérhetővé**.

Az elmúlt évek tendenciái azt mutatják, hogy egyre sűrűbben támadnak nagyobb vállalatokat az egyes csoportok a nagyobb haszonszerzés reményében. Az **egyéni felhasználók sincsenek biztonságban** az ilyen fenyegetéssel szemben, azonban fontos tudni, hogy sokkal kecsegtetőbb célpontot nyújtegy olyan vállalat, amely (fiat-valutától függetlenül) több milliós vagy milliárdos bevétellel rendelkezik és olyan adatokat, információkat kezelnek és tárolnak, amelyek nyilvánosságra hozatala vagy elérhetetlenné tétele óriási anyagi és PR károkat okozna a vállalat számára.

A dokumentum célja, hogy bemutassa azt az üzleti modellt, amely során **zsarolóvírus készítői tovább értékesítik szoftverjeiket vagy szolgáltatásukat** olyan személyek, bűnbandák vagy államilag támogatott szervezetek számára, akik **célzott vagy tömeges támadásokat** indítanak magánszemélyek, cégek vagy kormányzati szervek ellen.

Elolvasom

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu