NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2022.24. hét

HÍREK

- Zsarolóvírus támadások várhatóak a „Follina” sérülékenység kihasználásával
- Javíthatatlan biztonsági hibát találtak az Apple M1 processzorokban
- Egy új rendszer lehetővé teszi az IoT eszközök által gyűjtött adatok minimalizálását
- Nemzeti kiberbiztonsági tesztközpontot tervez Svájc
- Már 2 millió áldozata van a legújabb androidos malware kampánynak

Heti IT biztonsági tipp

- Így tehető biztonságosabbá az Ügyfélkapus bejelentkezés

STATISZTIKAI ADATOK

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

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK,

- Riasztás Emotet malware kampánnyal összefüggésben
- Riasztás Microsoft termékeket érintő sérülékenységekről – 2022. június
- Tájékoztatás Adobe szoftverek sérülékenységeiről – 2022. június

CTI ELEMZÉS

Mobilfenyegetettségek
– Mobil Security Threats

NEWS

IT biztonsági
HÍREK

Zsarolóvírus támadások várhatóak a „Follina” sérülékenység kihasználásával
(therecord.media)

A néhány hete felfedezett, és hivatalosan továbbra sem javított windows-os nulladik napi hibáját (Follina) kiberbűnözők már olyan káros programok terjesztésére is kihasználják, ami csupán egy lépésre van a zsarolóvírusok terjesztésétől. **Bővebben...**

Javíthatatlan biztonsági hibát találtak az Apple M1 processzorokban
(thehackernews.com)

Az MIT kutatói „PACMAN” névre keresztelték az általuk felfedezett, Apple M1 processzorok chipsetjei elleni hardvertámadást, amely tetszőleges kódfuttatást eredményezhet a macOS rendszereken. **Bővebben...**

Egy új rendszer lehetővé teszi az IoT eszközök által gyűjtött adatok minimalizálását
(thehackernews.com)

A Carnegie Mellon Egyetem kutatói hozták létre a „Peekaboo” névre keresztel rendszert, amelynek célja, hogy minimalizálja az IoT eszközök által gyűjtött adatokat, mielőtt azokat feltöltené egy külső felhőszerverre. **Bővebben...**

Nemzeti kiberbiztonsági tesztközpontot tervez Svájc
(heise.de)

A tervek szerint 2025-ban nyitják meg a „Crypto Valley”-ként is ismert Zug városában Svájc új nemzeti kiberbiztonsági tesztközpontját. A 2020 óta egyesületként működő svájci Nemzeti Kiberbiztonsági Tesztintézet jelentős beruházásokkal nyitja meg a központot, ahol elsősorban a kritikus infrastruktúrákhoz tartozó hálózatba köthető eszközök, valamint a digitális alkalmazások biztonságát, sebezhetőségét vizsgálják majd. **Bővebben...**

IT biztonsági
TIPP

Már 2 millió áldozata van a legújabb androidos malware kampánynak
(bleepingcomputer.com)

Kiberbiztonsági kutatók a múlt hónapban több reklám és információlopó szoftvert fedeztek fel a Google Play áruházban, amelyek közül legalább 5 továbbra is elérhető az alkalmazásboltban. A Dr. Web mobilvírusok aktivitásáról szóló jelentése szerint 2022 májusában a reklám és információlopó trójai programok jelentették a legnagyobb fenyegetést az Android eszközök esetében. Ebbe beletartoznak azok a spyware alkalmazások is, amelyek képesek elfogni a kétfaktoros (2FA) azonosításhoz kapott egyszer használatos biztonsági kódokat (OTP). **Bővebben...**

IT biztonsági Tipp

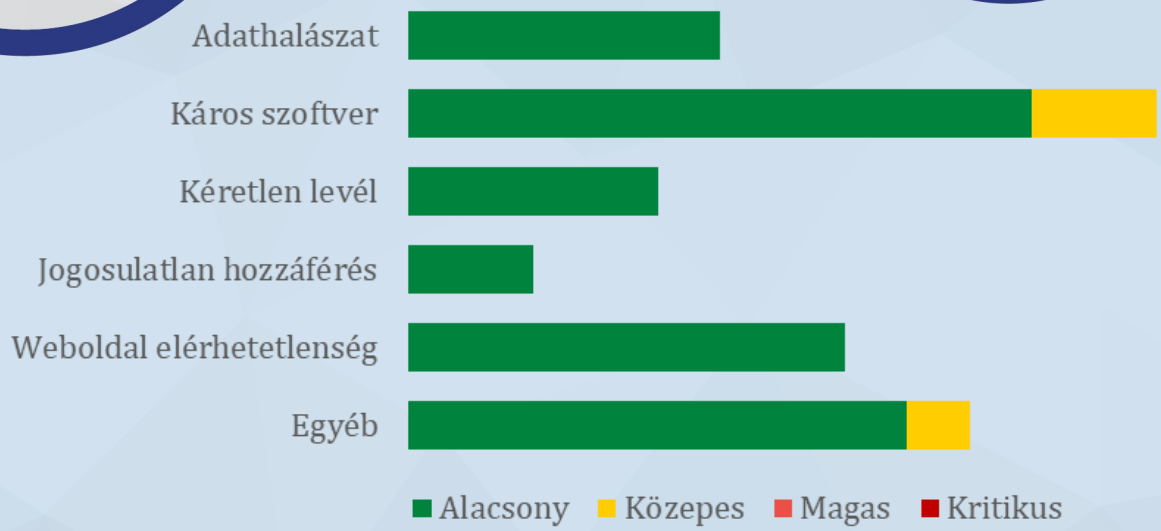
Az NBSZ NKI weboldalán többet tudhat meg az Ügyfélkapu új kétfaktoros bejelentkezési módjáról.

Statisztikai adatok

2022.06.10.-2022.06.16.

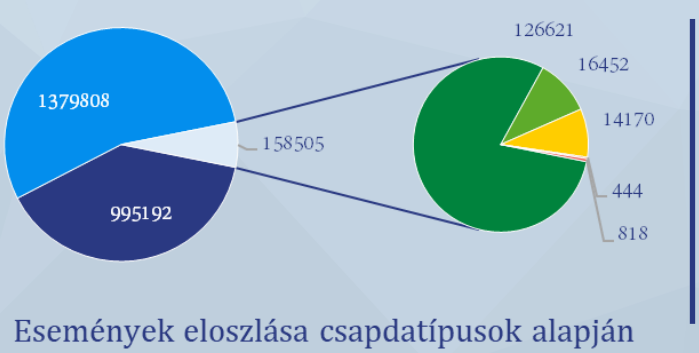
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes

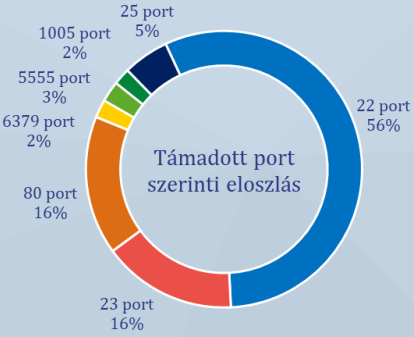


Incidensek eloszlása típus és kockázati besorolás szerint

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



Események eloszlása csapdatípusok alapján



További információkért, látogasson el **weboldalunkra**!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Riasztás Emotet malware kampánnyal összefüggésben

Az NBSZ NKI **riasztást** ad ki **Emotet malware terjedésével kapcsolatban**. A tapasztalatok alapján a malware terjesztésére irányuló e-mail tevékenység az elmúlt időszakban ugrásszerűen megemelkedett. Fontos tudni, hogy a **feladó** – Intézetünk tapasztalatai alapján – minden esetben **hamisított.** Elsősorban szenzitív adatok megszerzésére tesz kísérletet, mint például banki adatok, böngészőben mentett adatok, különböző azonosítók, emellett billentyűzetfigyelési funkcióval is rendelkezik, és **zsarolóvírus telepítésre** is alkalmas.

Részletek....

Riasztás Microsoft termékeket érintő sérülékenységekről – 2022. június

Az NBSZ NKI **riasztást** ad ki **Microsoft** szoftvereket érintő **kritikus kockázati besorolású sérülékenységek kapcsán**, azok súlyossága, kihasználhatósága, és a szoftverek széleskörű elterjedtsége miatt.

A Microsoft 2022. június havi biztonsági csomagjában összesen 55 különböző biztonsági hibát javított, amelyek között a **Follina néven hivatkozott nulladik napi (zero-day)** sebezhetőség (CVE-2022-30190,) is megtalálható.

Részletek...

Tájékoztatás Adobe szoftverek sérülékenységeiről – 2022. június

Az NBSZ NKI **tájékoztatót** ad ki az **Adobe** szoftverfejlesztő cég **termékeit érintő sérülékenységekkel kapcsolatban**, azok súlyossága, valamint az egyes biztonsági hibákat érintő aktív kihasználások miatt.

Összesen **47 db sérülékenység** került javításra, ebből – a gyártói besorolás szerint – **40 kritikus, 6 magas, 1** pedig **közepes** kockázati besorolású.

Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítésen keresztül, valamint manuálisan is letölthetőek a gyártói honlapokról. Bővebben...

Aktuális tartalmak

KIBERTÁMADÁS! PODCAST

Mobilfenyegetettségek – Mobil Security Threats

CTI jelentés

Az NBSZ NKI mobilfenyegetettségéről szóló jelentésének a célja, hogy ismertesse az olvasóval a mindennapos telefonhasználat veszélyeit és a különféle kockázatokat, amelyek a nem tudatos felhasználói magatartásból eredhetnek. Mivel a mai okostelefonok már miniszámítógépeknek minősülnek, és hasonló folyamatokat tudunk velük elvégezni (bankolás, e-mailezés, közösségi tevékenységek stb.) mint egy számítógépen (PC, laptop stb.), ezért sok hasonlóság van a két fajta eszköz között a ránk leselkedő biztonsági fenyegetéseket tekintve. Természetesen egy az egyben nem feleltethető meg az egyik eszköz a másiknak, de olyan információkkal gazdagodhat az olvasó, amelyeket számítógéphasználat közben is kamatoztathat.

Részletek...

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu