NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2022.22. hét

HÍREK

- Veszélyes MS Office zero-day sérülékenységet fedeztek fel, de van rá megkerülő megoldás
- Helyzetkép: a kiberbűnözés 57%-át a scamek tették ki tavaly
- Kaspersky: egyre több a mobilos trójai program
- Több millió androidos eszközt érintő sebezhetőségeket talált a Microsoft
- Ne használja a Tails OS-t, amíg a Tor böngésző hibája javításra nem kerül!

Heti IT biztonsági tipp

- Lehet biztonságos a jelszavunk megosztása?

STATISZTIKAI ADATOK

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

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK,

Rendkívüli tájékoztatás Microsoft Windows Support Diagnostic Tool (MSDT) zero-day sérülékenység kapcsán

PODCAST

Kriptográfia már nem is olyan régen [örökzöld]

CTI ELEMZÉS

Adathalászat
- a leghatékonyabb kiberfegyver

További érdekességekért, látogasson el **weboldalunkra**!

NEWS

IT biztonsági HÍREK

Veszélyes MS Office zero-day sérülékenységet fedeztek fel, de van rá m megkerülő megoldás

(securityweek.com)

Kiberbiztonsági szakértők egy nulladik napi hibára (CVE-2022-30190) figyelmeztetnek a Microsoft Office-ban, amelynek aktív kihasználtsága is ismert, és az MS dokumentumok makrók elleni védett nézete (protected view) sem nyújt vele szemben védelmet. **Bővebben...**

Helyzetkép: a kiberbűnözés 57%-át a scamek tették ki tavaly

(helpnetsecurity.com)

Az internethasználók száma 2021-re meghaladta a 4,62 milliárdot, azonban a digitalizáció előrelendülésével együtt az online csalások száma is jelentősen megnőtt. **Bővebben...**

Kaspersky: egyre több a mobilos trójai program

(bleepingcomputer.com)

A Kaspersky negyedéves jelentése szerint a rosszindulatú programok mennyiségének általános csökkenése ellenére a trójai típusú káros kódok terjesztése kiugró értéket mutat. **Bővebben...**

Ne használja a Tails OS-t, amíg a Tor böngésző hibája javításra nem kerül!

(securityaffairs.co)

Az anonimitást szem előtt tartó, Linux-alapú Tails operációs rendszer üzemeltetője, a The Amnesic Incognito Live System arra figyelmezteti a szoftver használóit, hogy a Tor böngésző aktuális verziója jelenleg nem biztonságos szenzitív adatok – például jelszavak – biztonságos küldésére, ezért a hibajavításig nem javasolt annak használata. **Bővebben...**

IT biztonsági TIPP

Több millió androidos eszközt érintő sebezhetőségeket talált a Microsoft

(thehackernews.com)

A Microsoft négy magas kockázati besorolású biztonsági hibát azonosított egy olyan alkalmazás-keretrendszerben (mce framework), amelyet számos androidos rendszeralkalmazás használ, ily módon több millió androidos eszköz sebezhetőségére derült fény.

A sebezhetőségek (CVE-2021-42598, CVE-2021-42599, CVE-2021-42600, CVE-2021-42601) lokális és távoli kihasználást is lehetővé tettek, azonban a Microsoft szerint a hibajavítást már minden érintett gyártó implementálta. **Bővebben...**

IT biztonsági Tipp

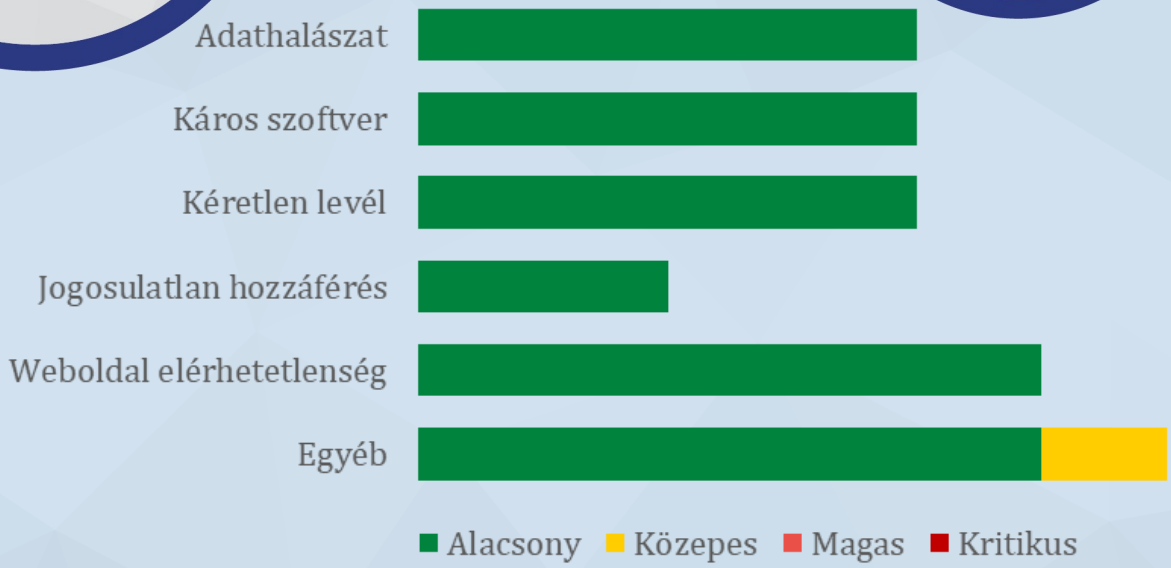
Az NBSZ NKI weboldalán bővebben olvashat arról, hogy lehet-e biztonságos a jelszavunk megosztása.

Statisztikai adatok

2022.05.27-2022.06.02.

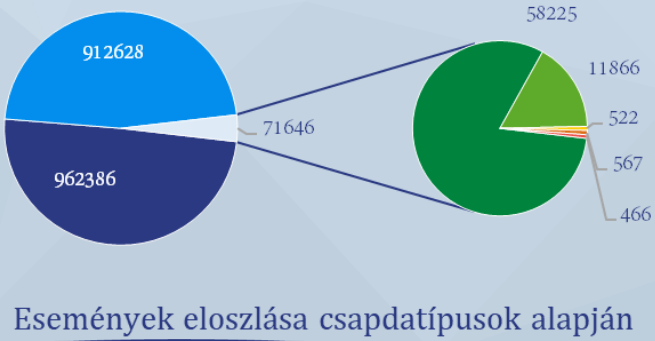
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes

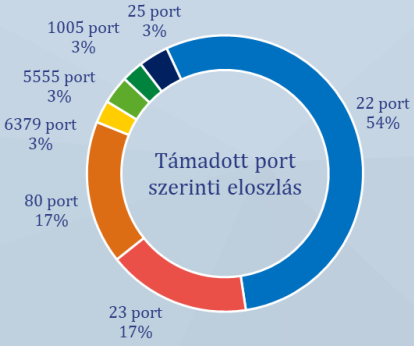


Incidensek eloszlása típus és kockázati besorolás szerint

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



Események eloszlása csapdatípusok alapján



További információkért, látogasson el **weboldalunkra**!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Rendkívüli tájékoztatás Microsoft Windows Support Diagnostic Tool (MSDT) zero-day sérülékenység kapcsán

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **tájékoztatást** ad ki a Microsoft Windows Support Diagnostic Toolt (MSDT) érintő, **Follina** néven hivatkozott **kritikus nulladik napi** sérülékenység kapcsán, amelynek **aktív kihasználtsága** is ismert.

A sérülékenység a CVE-2022-30190 számon került a nyilvántartásba. Sikeres kihasználás esetén a támadó egy **speciálisan szerkesztett MS Office dokumentum segítségével** az érintett rendszeren tetszőleges kódot futtathat, programokat telepíthet, adatokat tekinthet meg, módosíthatja vagy törölheti azokat, illetve új fiókokat hozhat létre az érintett felhasználó jogosultsági szintjének megfelelően.

Érintett verziók:

- **Office 2013**
- **Office 2016**
- **Office 2019**
- **Office 2021**
- **valamint a Professional Plus kiadások**

A sérülékenységgel kapcsolatban gyártói hibajavítás még nem érhető el, azonban a Microsoft közzétett egy tájékoztatót, amely tartalmazza a sérülékenység kihasználásának megelőzésére szolgáló lépéseket.

Az NBSZ NKI fokozott óvatosságot javasol az e-mailek csatolmányaként érkező MS dokumentumok kapcsán!

A tájékoztató szövege letölthető pdf formátumban.

Aktuális tartalmak

KIBERTÁMADÁS! PODCAST

Kriptográfia már nem is olyan régen [örökzöld]

Elérkezett #kriptotöri kurzusunk soron következő adása, amelyben az 1800-as évek közepétől a második világháborús Enigmáig bezárólag beszéljük át, hogy hogyan fejlődött a titkosítási technológia. Ezúttal is izgalmas sztorikra számíthattok feketeöves kriptomesterünk, Dani jóvoltából.

Meghallgatom

Online játék biztonságosan

Megjelent a SANS és a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet közös kiadványfolyamának 2022. júniusi száma, amely az online videójátékok kapcsán ad néhány hasznos tanácsot.

Elolvasom

Adathalászat - a leghatékonyabb kiberfegyver

CTI jelentés

Napjaink legkomolyabb információbiztonsági fenyegetései közé tartozik az adathalász (phishing) tevékenység. Még a legszofisztikáltabb, legösszetettebb kibertámadás – ami informatikai rendszerek, hálózatok összeomlásához, vagy a szervezetek legféltettebb belső információinak kiszivárgásához vezethet – is a legtöbb esetben **egyetlen e-maillel kezdődik**.

Kijelenthetjük, hogy kiberbiztonság sem szervezeti, sem személyes szinten nem létezik anélkül, hogy az adathalászat veszélyeit ne értenénk meg, és ezzel szemben ne hoznánk védekezési lépéseket. **Bővebben...**