NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2022.47. hét

HÍREK

- A kiberbűnözők idén is (Black Friday) akcióba lendültek
- Vigyázat, megkerülhetők a Cisco Secure Email Gateway szűrői!
- Eggyel több ok sürgősen telepíteni a ProxyNotShell javítást
- A Google Cloud kutatói a Cobalt Strike 34 különböző feltört verzióját azonosították
- Sharkbot malware-rel fertőztek androidos fájlkezelő appok

Heti IT biztonsági tipp

- Idén is eljött az akciókkal és persze a veszélyekkel teli Black Friday

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint

CTI ELEMZÉS

Tudnivalók a biztonságos online vásárláshoz – II. rész

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK,

Riasztás AgentTesla malware kampánnyal

NEWS

IT biztonsági
HÍREK

A kiberbűnözők idén is (Black Friday) akcióba lendültek

(securityaffairs.co)

A kiberbűnözők minden évben kihasználják az online akciós időszakokat, hogy csaló ajánlatokkal próbáljanak megkárosítani bennünket. A Bitdefender Antispam Lab adatai alapján nincs ez másként idén sem. **Bővebben...**

Vigyázat, megkerülhetők a Cisco Secure Email Gateway szűrői!

(securityweek.com)

Egy névtelen kutató több olyan módszert is nyilvánosságra hozott, amelyekkel megkerülhető a Cisco Secure Email Gateway alkalmazás egyes szűrői, és speciálisan kialakított e-mailek segítségével rosszindulatú szoftvereket lehet eljuttatni az áldozat gépére. **Bővebben...**

Eggyel több ok sürgősen telepíteni a ProxyNotShell javítást

(bleepingcomputer.com)

ProxyNotShell kihasználási kód (proof-of-concept) került nyilvánosságra. Biztonsági hibajavítás a 2022. novemberi MS „patch kedd" részeként már elérhető, javasolt a frissítés mielőbbi telepítése! **Bővebben...**

A Google Cloud kutatói a Cobalt Strike 34 különböző feltört verzióját azonosították

(securityaffairs.co)

A Google Cloud kutatói bejelentették, hogy 34 különböző Cobalt Strike feltört verziót fedeztek fel, amelyekben összesen 275 egyedi JAR fájl található. A Cobalt Strike eredetileg egy fizetős penetrációs tesztelési termék, amely lehetővé teszi a támadó számára, hogy egy "Beacon" nevű agentet telepítsen a célgépre. **Bővebben...**

IT biztonsági
TIPP

Sharkbot malware-rel fertőztek androidos fájlkezelő appok

(thehackernews.com)

Nem az első alkalommal került a Sharkbot malware a Google Play áruházba. Ezúttal kiberbűnözők különböző fájlkezelő applikációba rejtve csempészték be a káros kódot a hivatalos androidos alkalmazásboltba. Az esetre a Bitdefender figyelt fel, akik a héten tették közzé elemzésüket. A Sharbot banki trójai elsődleges célja az, hogy a banki átutalásokat eltérítsék, az ún. Automatic Transfer System technika segítségével. **Bővebben...**

IT biztonsági tipp

Az NBSZ NKI weboldalán a Black Friday veszélyeiről, valamint az azok elkerülését segítő biztonságtudatos online vásárlási szokásokról olvashat bővebben.

Statisztikai adatok

2022.11.18.-2022.11.24.

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes

Incidensek eloszlása típus és kockázati besorolás szerint

További információkért, látogasson el **weboldalunkra**!

Aktuális tartalmak

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Tudnivalók a biztonságos online vásárláshoz II. rész

A „Tudnivalók a biztonságos online vásárláshoz – I. rész” című tájékoztató dokumentumban bemutattuk a felhasználókat fenyegető leggyakoribb támadástípusokat, módszereket és számos javaslattal éltünk, amelyek betartásával nagy mértékben csökkenthető annak a kockázata, hogy személyes adataink és vagyonunk rossz kezekbe kerüljön.

Az első részben a felhasználó oldaláról igyekeztünk bemutatni a legfőbb problémákat, jelen dokumentumban pedig mindezt az üzemeltetők, webshop tulajdonosok szemszögéből ismertetjük.

Elolvasom

Riasztás AgentTesla malware kampánnyal összefüggésben

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **riasztást** ad ki **AgentTesla malware** egyes variánsainak **terjedésével kapcsolatban**.

Elolvasom

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu