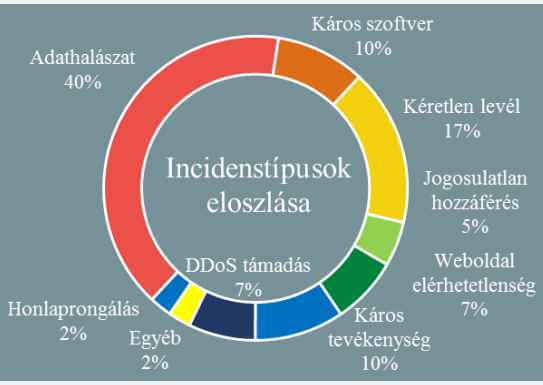
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2022. 14. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2022.04.01. - 2022.04.07.



Kövessen minket weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

A Dragos összegezte az európai kritikus infrastruktúrák kiberfenyegetettségét

(securityweek.com)

Folyamatosan nő az ipari vezérlőrendszerek (Industrial Control System - ICS) és általában az OT (Operation Technology - gyártási technológia) hálózatok ellen támadásokat indító fenyegetési csoportok száma, mégsem ez jelenti a fő kiberfenyegetést a kritikus szektorokra nézve ─ állítja a Dragos új jelentésében. **Bővebben...**

WhatsApp nevében küldött értesítésekkel terjesztenek káros kódokat az adathalászok

(bleepingcomputer.com)

Új adathalász kampányt fedeztek fel az Armorblox kutatói, ez idáig több mint 27 655 e-mail címre került kiküldésre az a WhatsApp hangüzenet-értesítő, aminek segítségével a támadók információlopó kártevőt terjesztenek, kihasználva, hogy a WhatsApp múlt héten adta ki a hangüzenetküldő funkciójának újításait. Az e-mail látszólag a WhatsApptól érkező hangüzenet-értesítő, ami egy beágyazott „Lejátszás” gombot is tartalmaz. **Bővebben...**

Megszavazták a kriptovaluták átláthatóságára vonatkozó jogszabálytervezetet

(bleepingcomputer.com)

Az új követelmények értelmében, minden kripto-tranzakciónak tartalmaznia kell a tőke forrására és kedvezményezettjére vonatkozó információkat, amelyeket rendelkezésre kell bocsátani az illetékes hatóságok számára is – áll a parlament közleményében. **Bővebben...**

Kínai hackerek a VLC Media Playert használták kiberkémkedés során

(bleepingcomputer.com)

Biztonsági kutatók egy régóta tartó kiberkémkedési műveletről közöltek információkat, amely a Cicada (más néven: menuPass, Stone Panda, Potassium, APT10, Red Apollo), kínai állami támogatású APT csoporthoz köthető. A támadási kampány körülbelül 2021 közepén indulhatott, és feltehetőleg még most is zajlik. **Bővebben...**

Feltörték a Mailchimpet, kriptovaluta tulajdonosok elleni támadásra használták

(securityaffairs.co)

Az elmúlt hétvége során több Trezor felhasználó kapott olyan értesítést, miszerint súlyos adatszivárgás érte a céget, ezért sürgősen meg kell változtatniuk a PIN kódjukat, amit az üzenetben szereplő linkről letölthető alkalmazással tudnak megtenni (lásd: 1. ábra). *(A Trezor az egyik, ha nem a legnépszerűbb hardveres kriptovaluta pénztárcákat kínáló szolgáltatás.)* **Bővebben...**

A VMware több termékben is javítja a Spring4Shell RCE hibáját

(bleepingcomputer.com)

A VMware biztonsági frissítéseket tett közzé a Spring4Shell néven ismert kritikus távoli kódfuttatási (RCE) sebezhetőséghez. A Spring4Shell által érintett VMware termékek listája a vállalat közleményében olvasható. Ahol nem áll rendelkezésre javítás, ott a VMware ideiglenes megoldásként egy megkerülő megoldást (workaround) adott ki. Kritikusan fontos a biztonsági közleményben szereplő tanácsok követése, mivel jelenleg a Spring4Shell egy aktívan kihasználható sebezhetőség. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán az androidos alkalmazás-engedélyekkel kapcsolatban talál gondolatébresztő információkat.