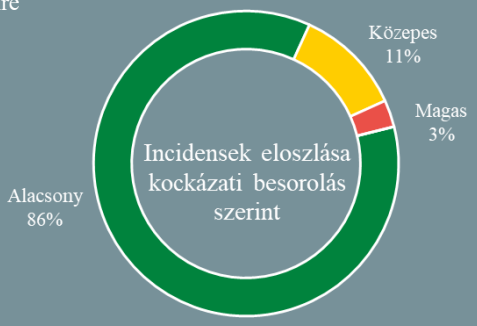
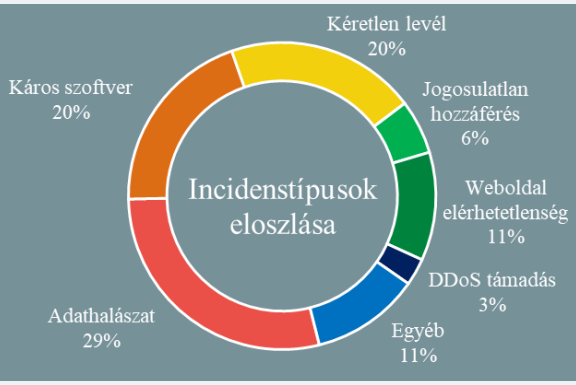
Nemzetközi IT-biztonsági sajtószemle

2022. 09. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2022.02.25. - 2022.03.03.





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

Vigyázat, egyre több az Ukrajnát névleg támogató, hamis adományozási mozgalom

(bleepingcomputer.com)

Ez idáig több mint 37 millió dollár értékű kriptovalutát sikerült összegyűjteni Ukrajna megsegítésére, azonban ennek hatására a kiberbűnözők is akcióba lendültek. A BleepingComputer számos „Segítse Ukrajnát!" témájú csaló e-mailt, adathalász oldalt és egyéb fórumot azonosított, amelyekkel a segítőkész felhasználók jóhiszeműség kihasználva igyekeznek pénzt szerezni a csalók. A hamis „Segítse Ukrajnát" mozgalom során a támadók olyan, jellemzően Bitcoin és Ethereum kriptovaluta adománygyűjtést hirdetnek, amely semmilyen kapcsolatban nem áll az ukrán kormányzattal. **Bővebben...**

Új képességekkel tért vissza a TeaBot androidos banki malware

(thehackernews.com)

Az Anatsa, más néven TeaBot rosszindulatú program először 2021 májusában jelent meg, akkoriban látszólag valódi PDF dokumentum- és QR kód olvasó alkalmazásként került a Play Store alkalmazásboltba, ezt követően pedig 2021 novemberében bukkant fel ismét különböző dropper alkalmazásokban. A mostani kampány során a TeaBot RAT több mint 400 — jellemzően Oroszország, Kína és az Egyesült Államok — banki és pénzügyi alkalmazásait célozza. **Bővebben...**

Európai szervezetek a kibertámadások célkeresztjében

(thehackernews.com)

Egy új államilag támogatott adathalász kampányra derült fény, amely európai kormányzati szervezetek ellen irányul, célja pedig, hogy információkat szerezzenek az Ukrajnából menekülők tartózkodási helyzetéről, illetve a régió utánpótlásainak útvonaláról. A Proofpoint biztonsági cég „***Asylum Ambuscade***"-nek nevezte el azokat a 2022. február 24-én észlelt rosszindulatú e-maileket és social engineering támadásokat, amelyekkel európai pénzügyi-, valamint a közlekedésért és népvándorlásért felelős kormányzati munkatársakat céloztak. **Bővebben...**

Óvatosan a Microsoft Store-os játékokkal, nehézsúlyú kártevő is járhat hozzájuk!

(thehackernews.com)

A Microsoft hivatalos alkalmazásboltján keresztül terjed egy nemrégiben azonosított kártevő program, amely átveheti az irányítást az áldozatok eszközei felett. Ezidáig több mint 5000 Windows-os gép érintett a fertőzésben, a legtöbb áldozatot eddig Svédországban, Bulgáriában, Oroszországban, Spanyolországban és a Bermuda szigeteken szedte a kártevő. A Check Point biztonsági cég „***Electron Bot***"-nak nevezte el a rosszindulatú programot, amely egy moduláris SEO túloptimalizálásra (SEO poisoning) alkalmas malware. **Bővebben...**

Fokozott iráni APT aktivitásról adott ki tájékoztatót a CISA

(cisa.gov)

Az Egyesült Államok Kiberbiztonsági és Infrastruktúra-biztonsági Ügynöksége (CISA), az FBI, az Amerikai Kiber Parancsnokság – Nemzeti Kiber Műveleti Egysége (U.S. Cyber Command Cyber National Mission Force – CNMF), valamint a brit kibervédelmi központ (NCSC-UK) közös figyelmeztetést adott ki az iráni állami hátterű **MuddyWater** APT csoport kormányzati és magánszektor ellen irányuló fokozott kiberműveleteiről. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán a potenciális fenyegetettségek elleni kiberbiztonsági intézkedésekről olvashat bővebben.