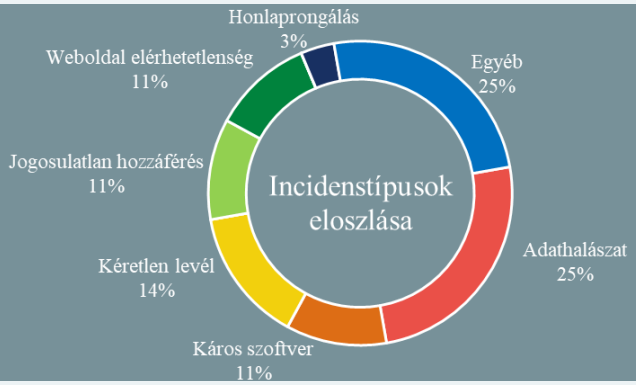
Nemzetközi IT-biztonsági sajtószemle

2022. 21. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2022.05.20. - 2022.05.26.



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

PDF dokumentumba rejtett docx fájlokkal csempészik az áldozatok gépére a káros programot

(bleepingcomputer.com)

Szerencsére egyre több felhasználó kezeli kellő gyanakvással az e-mailek mellékleteként érkező docx és xls kiterjesztésű dokumentumokat, ezeket ugyanis gyakran rosszindulatú makrók és egyéb káros programok terjesztéséhez is felhasználhatják a támadók. Ennek köszönhetően azonban a kiberbűnözők egyre újabb módszereket dolgoznak ki a felhasználók megtévesztésére. A HP Wolf Security jelentésében ezúttal a pdf dokumentumokba ágyazott rosszindulatú makrókat tartalmazó docx fájlokra hívják fel a figyelmet. **Bővebben...**

Zero-day sebezhetőségek kihasználásával terjesztik a Predator kémprogramot Androidon

(bleepingcomputer.com)

A Google Fenyegetettségelemző Csapata (TAG) állami támogatottságú hackerekhez köti azokat a 2021 augusztusa és októbere közötti támadási kampányokat, amelyek során a támadók öt – Google Chrome és Anroid OS – nulladik napi sérülékenység kihasználásával telepítenek Predator kémprogram implementációkat naprakész Androidos eszközökre. **Bővebben...**

IT biztonsági Tanács

A közelgő Nemzetközi Gyereknap alkalmával az NBSZ NKI weboldalán a hasznos tanácsok mellett, egy ingyenes online magyar nyelvű kiberbiztonsági kalandjáték is bemutatásra kerül.

Bántalmazott áldozatoknak adják ki magukat randioldalakon a csalók

(bleepingcomputer.com)

A BleepingComputerhez több bejelentés is érkezett a Tinderen és a Grindr társkereső alkalmazáson megjelent új adathalász kampányról, amely során a csalók magukat áldozatként feltüntetve veszik rá a felhasználókat adataik megadására. A kegyetlen átverés során a támadók vonzó profil mögé bújva veszik fel a kapcsolatot, általában az LMBTQ közösség felhasználóival. A beszélgetések előrehaladtával a csalóról „kiderül", hogy korábbi randipartnere bántalmazta, ezért arra kéri csevegőpartnerét, hogy töltsön ki egy űrlapot, amivel bizonyítani tudja, hogy nem szerepel a bántalmazók nyilvántartási listájában. **Bővebben...**

Minden eddiginél gyakoribb támadási forma a telefonos csalás

(helpnetsecurity.com)

Az Agari és a PhishLabs negyedéves fenyegetési trendeket összefoglaló jelentése szerint a telefonos adathalász támadások (vishing) száma közel 550%-kal nőtt az elmúlt egy évben, ezzel megelőzve az üzleti e-mailekkel történő visszaéléses (Business Email Compromise – BEC) támadásokat. Az elemzők szerint a standard vishing helyett ─ azaz amikor a támadó közvetlenül hívja az áldozatot ─ egyre inkább az a jellemző „forgatókönyv", hogy a támadók először egy megtévesztő e-mailt küldenek az áldozatnak, amiben arra próbálják rávenni, hogy hívja fel a mellékelt számot. **Bővebben...**

Ne lepődjünk meg, ha egy adathalász oldalon ránk köszön egy chatbot

(bleepingcomputer.com)

A kiberbűnözők egyre szofisztikáltabb támadásokat hajtanak végre, vagyis egyre jobban figyelnek a nyelvhelyességre, az adathalász oldalak dizájnjára, és egyre gyakrabban használnak olyan mechanizmusokat a megtévesztés fokozása érdekében, amelyeket valódi cégek használnak. Mindez azt eredményezi, hogy egyre figyelmesebbeknek kell lenniünk ahhoz, hogy ki tudjuk szűrni az ilyen jellegű támadásokat. **Bővebben...**