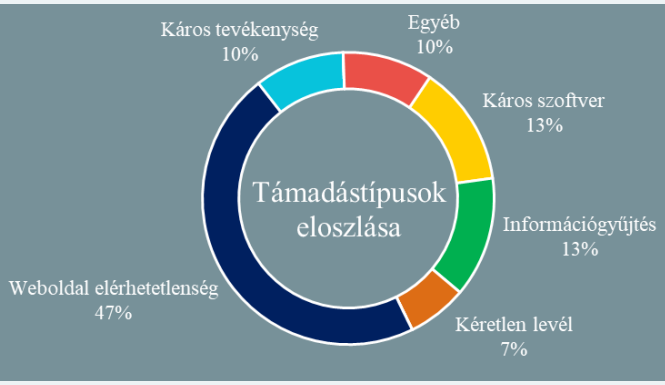
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 44. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.10.22. - 2020.10.29.



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

A Maze ransomware nyugdíjba vonul, felemelkedőben az Egregor

(bleepingcomputer.com)

A Maze kiberbűnözői kollektíva 2019 májusában kezdte meg működését, tavaly novemberre pedig már az egyik legjelentősebb fenyegetési szereplővé nőtte ki magát. Ez a csoport kezdte alkalmazni azt a mára célzott ransomware támadások esetén alapvetőnek számító taktikát, hogy az áldozatot nem csupán a fájlok titkosításával zsarolják, hanem azzal is, hogy a titkosítás előtt ellopott adatokat nyilvánosságra hozzák. (Az első ilyen áldozat az Allied Universal volt.) **Bővebben...**

Adatvédelmi indokra hivatkozva törölt legitim appokat a Google a Play Store-ból

(engadget.com)

A Google három, gyermekeknek készített legitim alkalmazást távolított el alkalmazásboltjából, arra hivatkozva, hogy megsértették a cég adatgyűjtésre vonatkozó irányelveit. A probléma oka a szóban forgó appok (Princess Salon, Number Coloring és a Cats & Cosplay) fejlesztéséhez használt keretrendszerekben keresendő. Az alkalmazásokhoz ugyanis az Unity, az Appodeal és az Umeng szoftverfejlesztői készletek (SDK) verzióit használták fel, amelyek Android ID-t és Android Advertising ID-t (AAID) is gyűjtenek. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a Tos;DR weboldaláról, amely az online szolgáltatások általános szerződési feltételeinek értékelésében nyújthat segítséget.

Vigyázat: ismét új megtévesztést alkalmaz az Emotet!

(bleepingcomputer.com)

Újabban Microsoft Office frissítésnek álcázott üzenettel próbálják meg a támadók rávenni áldozataikat az Emotet káros program telepítésére. Az e-mail üzenetekkel terjedő, káros makrókat tartalmazó Microsoft Word dokumentumok megnyitása során a felhasználók egy olyan üzenettel találják szemben magukat, amely arról tájékoztatja őket, hogy frissíteniük kell a Microsoft Word programot (lásd: borítókép). A szerkesztés engedélyezésével (Enable Content) azonban az Emotet települ az áldozat rendszere. A káros kód veszélyessége abból adódik, hogy gyakran további káros programokat ─ nem ritkán zsarolóvírust ─ telepít az áldozat eszközére.

Új keretrendszert adtak ki a gépi tanuláson alapuló rendszerek védelmére

(thehackernews.com)

Microsoft, MITER, IBM, NVIDIA és Bosch közösen kiadott egy új nyíltan elérhető keretrendszert, ami segítheti a gépi tanuláson (ML- machine learning) alapuló rendszerek ellen irányuló kontradiktórius támadások észlelését, kezelését és megoldását. A mesterséges intelligencia (MI) és a gépi tanuláson alapuló rendszerek számos új területen jelen vannak, amelyekkel a fenyegetési szereplők is visszaélhetnek, akár a rosszindulatú programok működtetésével, vagy a félrevezető adathalmazok becsatolásával, aminek következtében rossz döntési eredmények születnek. **Bővebben...**

Egy frissítés telepítésével az Adobe Flash már most törölhető a Windows-ból

(bleepingcomputer.com)

A **KB4577586** számú frissítéssel a Microsoft kizárja az Adobe Flash-t a Windows 10 és Windows Server minden verziójából. A frissítés jelenleg kizárólag a Microsoft Update katalógusból érhető el, ám a tech óriás tervei szerint 2021 elején WSUS-on és Windows Update-en keresztül is telepíthető lesz, amint a Flash a támogatási életciklusának végéhez ért. **Bővebben...**