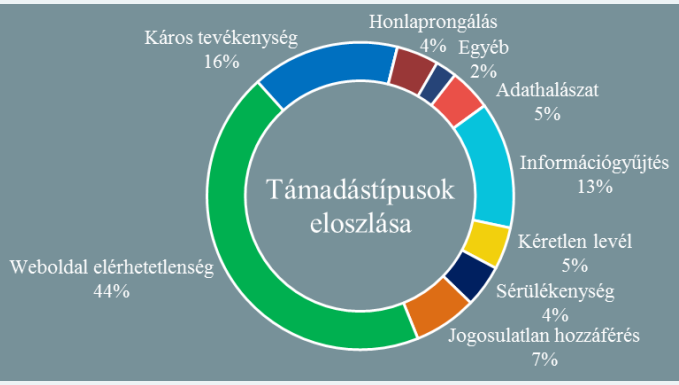
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 36. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.08.28. - 2020.09.03.



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

Az ipari vezérlőrendszerek rendkívül kitettek a hálózati támadásoknak

(securityweek.com)

Nyugtalanító felfedezést tett a Claroty nevű kiberbiztonsági cég: az idén eddig nyilvánosságra hozott ipari vezérlőrendszereket érintő sérülékenységek több, mint 70%-a távolról kihasználható volt. A cég közel 400 sérülékenységet vizsgált meg, amelyek összesen 53 terméket érintettek. Közel felük (41%) esetében kódfuttatás, majd ugyanennyi esetében (39%) szolgáltatás megtagadás, 37% esetében pedig a biztonsági mechanizmusok megkerülése volt lehetséges távolról. Ezek a termékek ráadásul többnyire népszerű, világszerte alkalmazott eszközök, csupán 7%-ra igaz az, hogy kifejezetten az Egyesült Államokban lenne jellemző a használatuk. **Bővebben...**

Hirdetési csaló appokat törölt a Google

(securityaffairs.co)

A White Ops kutatói több olyan androidos appot azonosítottak a Google Play Store-on, amelyek a "Terracotta" malware-t tartalmaztak. A threat intel cég 2019 óta követi figyelemmel a Terracotta botnetet, amely 2020 júniusában egyetlen hét alatt több, mint 2 milliárd hamis reklám kattintást generált, körülbelül 65 000 fertőzött eszköz segítségével. A káros alkalmazások általában valamilyen ingyenes termék (kuponok, jegyek, cipők, stb.) ígéretével csábították telepítésre az áldozatokat. A csaló ígéret szerint a választott termék két hét múlva érkezik, ám valójában sosem kerül kiszállításra. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a Windows Print Spooler elleni támadásokkal szembeni védekezésről.

Káros kódot tartalmazó szoftvert hagyott jóvá az Apple automatizált alkalmazás-hitelesítője

(bleepingcomputer.com)

2020 februárjától minden, a hivatalos Mac App Store-on kívül forgalmazott mac-es szoftver esetén a fejlesztőknek először be kell küldeniük az Apple-höz ellenőrzésre az alkalmazásokat, ahhoz, hogy azok macOS-en ─ Catalina vagy ennél újabb verzión ─ fussanak. Amennyiben egy alkalmazás sikeresen átmegy a káros komponensek után kutató automatizált ellenőrzésen, azt a macOS biztonsági mechanizmusa (Gatekeeper) engedi futni a rendszeren, ellenkező esetben blokkolja azt. A cég büszkén állítja, hogy a hitelesítő rendszer megbízhatóvá teszi a Mac App Store-on kívüli szoftvereket, azonban a rendszer nem csalhatatlan, ugyanis egyes alkalmazásokban a Shlayer adware mintáit fedezték fel. **Bővebben...**

Kibertámadás érte a norvég parlamentet

(securityweek.com)

Hackerek hozzáfértek több norvég országgyűlési képviselő e-mail fiókjához – tudatta a norvég parlament, a Storting keddi közleményében. A támadásról nem közöltek bővebb információt, mindössze annyi ismert, hogy a hackerek különböző mértékben töltöttek le adatokat az érintett fiókokból.

Figyelem: új EMOTET támadási kampány indult

(securityaffairs.co)

2020 februárjától a hírhedt Emotet botnet szünetet tartott, azonban július óta ismét aktív. A támadók legújabban COVID-19 témájú Word dokumentumokkal, hamis számlákkal, szállítási üzenetekkel igyekeznek rávenni az áldozatokat az e-mailben érkező, káros kódot tartalmazó csatolmányok megnyitására. Az augusztus közepén indult új kampány során a malware terjesztői új sablont kezdtek alkalmazni, amelyet a vörös színű fejléc miatt a felfedező Joseph Roosen "Red Dawnnak", azaz "Vörös hajnalnak" (lásd: borítókép) nevezett el. **Bővebben...**