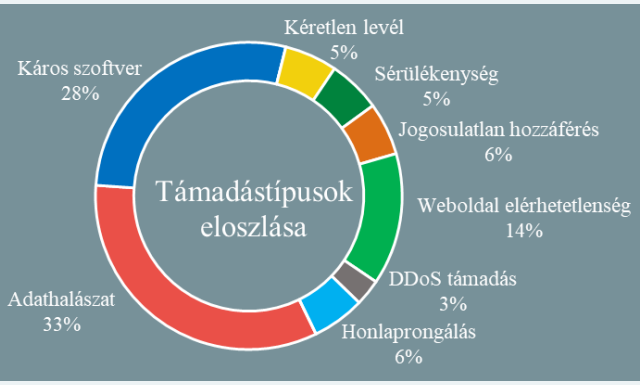
Nemzetközi IT-biztonsági sajtószemle

2020. 19. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.05.01. - 2020.05.07.



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

Hamis frissítési üzenetek – lehetséges támadási vektor VPN szoftverekkel szemben

(securityweek.com)

A VPN szoftverek elemzésével foglalkozó VPNpro vizsgálat alá vonta a 20 legnépszerűbb VPN-t, amelynek során arra voltak kíváncsiak, hogy lehetséges-e frissítésnek álcázott üzenetekkel káros kódot juttatni a szoftvereket használók gépére. Ennek során azt találták, hogy a TorGuard, a CyberGhost, a PrivateVPN, valamint a Betternet VPN lehetőséget adtak arra, hogy harmadik fél a kommunikációba ékelődjön, azonban hamis frissítések letöltésére csupán az utóbbi két program esetében volt mód, a PrivateVPN-nél ráadásul a letöltött fájl automatikusan futtatásra is került. A két érintett cég február közepén értesítésre került, a sérülékenységeket befoltozó hibajavítások pedig a gyártók szerint megszüntetik a sebezhetőségeket.

Androidos pénzügyi alkalmazásokat céloz az EventBot malware

(securityweek.com)

Európai és észak-amerikai androidos banki alkalmazásokat igyekszik kompromittálni az EventBot elnevezésű káros program. A Cybereason Nocturnus biztonsági kutatói szerint a jelenleg is fejlesztés alatt álló banki trójai program a megszerzett jogosultságokkal hozzáférhet a pénzügyi alkalmazások által tárolt érzékeny adatokhoz, az SMS üzenetek elfogásával pedig lehetővé teheti a kétfaktoros hitelesítés megkerülését. A szakértők arra is felhívják a figyelmet, hogy szervezeti pénzügyi információk is veszélyben lehetnek. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a CISA által kiadott ajánlásról, amely a Microsoft Office 365 leglényegesebb IT biztonsági kockázataira, és azok lehetséges kezelésére hívja fel a figyelmet.

A kalóz filmek most különösen nagy kockázatot jelentenek

(bleepingcomputer.com)

A Microsoft felhívja a figyelmet arra, hogy a kalóz streaming szolgáltatások és torrent weboldalak forgalmának megemelkedését a kiberbűnözők is aktívan kihasználják káros kódok terjesztésére. Erre jó példa egy kriptovalutát bányászó, rosszindulatú program terjesztése, amellyel elsősorban spanyol és dél-amerikai felhasználókat céloznak. E konkrét támadáshoz a kiberbűnözők a John Wick filmsorozat harmadik epizódját használták fel csaliként, olyan fájlneveket használva, mint a "John_Wick_3_Parabellum", a "contagio-1080p,", illetve "Punales_por_la_espalda_BluRay_1080p", "La_hija_de_un_ladron", vagy a "Lo-dejo-cuando-quiera". Az ilyen támadások elkerüléséhez kerüljük a nem jogtiszta tartalmak letöltését!

Kaiji: új IoT malware a láthatáron

(securityaffairs.co)

Biztonsági szakemberek egy új DDoS botnetet azonosítottak, amely Linux szervereket és IoT eszközöket céloz. A MalwareMustDie elemzése szerint a Kaiji egyedi fejlesztésű és Go programozási nyelven készült. Működését tekintve nem sérülékenységek kihasználásával fertőz, hanem SSH portokon elérhető eszközök root fiókjaihoz próbál brute force technikával hozzáférni. Sikeres fertőzés után DDoS (*ipspoof és synack)* támadások indítására használhatja fel a fertőzött rendszert, emellett helyi SSH hitelesítő kulcsok után is kutat a továbbterjeszkedéshez. **Bővebben...**

Cisco Webex felhasználók veszélyben: tanúsítvány lejáratra hivatkozva csalnak ki hitelesítő adatokat

(bleepingcomputer.com)

A Cisco Webex VTC platformot is elérte az utóbbi hónapokban tapasztalható nagy ütemű felhasználói bázis bővülés, ezzel együtt azonban a szofisztikált adathalász támadások is megjelentek. Az e-mail biztonsággal foglalkozó Abnormal Security szerint már legalább 5 000 Webex felhasználót ért támadás, amelynek során olyan, a Cisco Webex Team-et megszemélyesítő e-mail üzenetek érkeznek, amelyek arculatilag szinte teljesen azonosak az eredeti üzenetekkel. **Bővebben...**