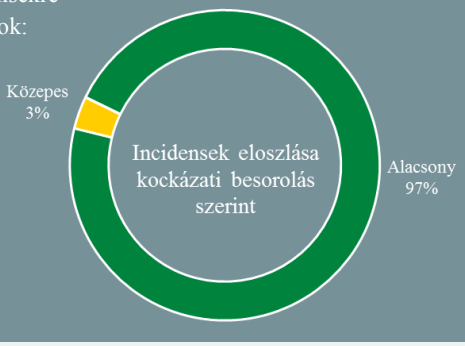
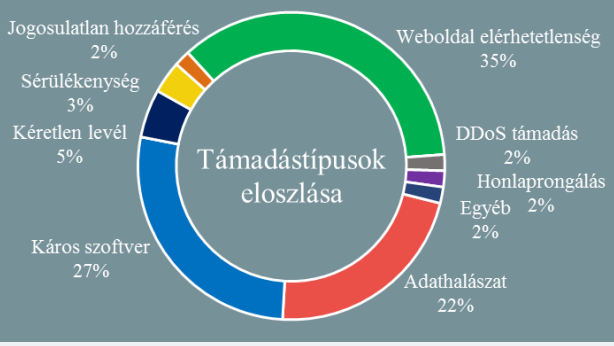
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 27. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.06.26. - 2020.07.02.





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

Kritikus Palo Alto sérülékenység kihasználását célzó támadásokra figyelmeztet az amerikai kiberparancsnokság

(securityweek.com)

A napokban derült fény Palo Alto tűzfalak operációs rendszerének (PAN-OS) kritikus sérülékenységére, amelynek kapcsán az Amerikai Egyesült Államok haderejének kiberparancsnoksága (USCYBERCOM) lehetséges kihasználó támadásokra hívja fel a figyelmet. A sérülékenység javítására elérhető gyártói hibajavítás, amelynek telepítése mielőbb javasolt.

Facebook hitelesítő adatokat lopó appokat törölt a Google

(zdnet.com)

A Google eltávolított 25 olyan káros alkalmazást a Play Store-ból, amelyek Facebook hitelesítő adatokat gyűjtöttek. Az alkalmazások, bár különböző legitim funkciókkal álcázták magukat — lépésszámláló, képszerkesztő, videószerkesztő, háttérkép alkalmazás, zseblámpa, fájlkezelő, mobil játék — működésük szempontjából azonosak voltak: figyelték, hogy a felhasználó milyen appokat indít el, és amennyiben ez a Facebook alkalmazás volt, egy hamis login oldalt generálva elfedték a valós bejelentkezési oldalt. Törlésük előtt a káros appokat több, mint 2,34 millióan töltötték le. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arról, hogy Windows 10-ben, miként állíthatók vissza a véletlenül törölt fájlok.

Kínai malware-eket is használtak ausztrál szervezetek elleni kibertámadások során

(securityaffairs.co)

Scott Morrison ausztrál miniszterelnök nemrég bejelentette, hogy egy több ágazatot érintő, intenzív kibertámadási kampány zajlik ausztrál szervezetek ellen, amelynek hátterében egy idegen államhatalmat sejtenek. Az ausztrál kiberközpont (ACSC) a támadások kivizsgálásának eredményéről most közölt részletes információkat. Eszerint a támadók többek között sérülékeny Telerik UI, Microsoft SharePoint, valamint Citrix sérülékenységeket használtak ki, az alkalmazott káros kódok között pedig kínai APT-khez köthető malware-ek (mint például a Korplug, vagy a PlugX) is megtalálhatóak.

A HTTPS forgalom ellenőrzése nélkül a legtöbb malware nem detektálható

(helpnetsecurity.com)

2020 első félévében a legtöbb azonosított malware titkosított HTTPS kapcsolaton keresztül fertőzött, 72%-uk pedig zero day-nek minősült, amelyeket a hagyományos szignatúra-alapú antivírus megoldások nem lettek volna képesek detektálni — írja jelentésében a WatchGuard. Mindez arra világít rá, hogy fejlett viselkedésalapú detektáló megoldások, valamint a HTTPS forgalom ellenőrzésének hiányában a szervezeteket érintő fenyegetések mintegy kétharmada azonosíthatatlan maradhat.

Netgear router tulajok figyelem: fontos biztonsági frissítések érkeznek

(securityweek.com)

A Netgear elkezdte elérhetővé tenni a közel 80 termékét érintő sérülékenységek hibajavításait. Eddig 28 eszköz számára készült biztonsági hibajavítás, azonban mivel egyes termékek már a támogatási életciklusuk végéhez értek, minden valószínűség szerint az összes érintett típus nem részesül majd javításban. A gyártói közlemény innen érhető el.