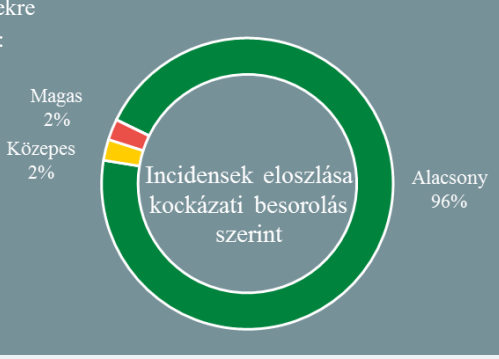
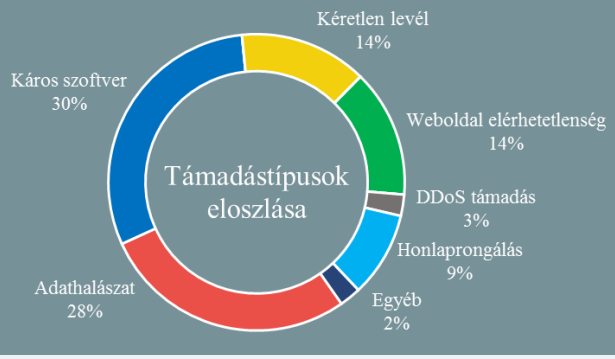
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 16. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.04.09. - 2020.04.16.





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

Katonai dokumentumok szivárogtak ki egy ransomware támadás után

(heise.de)

Az amerikai Visser Precision ipari beszállító ellen folytatott sikeres ransomware támadás után a támadók bizalmas dokumentumokat tettek közzé az interneten, mivel a Visser Precision nem volt hajlandó eleget tenni a zsarolók követeléseinek. A támadást a Windows-os környezetekre specializálódott DoppelPaymer ransomware mögött álló kollektíva végezte. A Visser Precision precíziós alkatrészeket gyárt az repülőgép- és űripar számára, valamint műszaki szolgáltatásokat nyújt. **Bővebben...**

Ha ezt a VPN-t használja Androidon, minél előbb törölje le

(ehackingnews.com)

A Google több, mint száz millió Android felhasználót figyelmeztetett egy VPN alkalmazás, a SuperVPN használata ellen. Ennek oka, hogy kutatók több súlyos sérülékenységet is azonosítottak az applikáció kapcsán: nem titkosított HTTP kommunikációt, beégetett titkosító kulcsokat, valamint az EAP hitelesítő adatok titkosítatlan forgalomban való továbbítását. Ezek a sérülékenységek lehetővé tehették ún. közbeékelődéses támadások (MitM) végrehajtását, amelyek során illetéktelenek hozzáférhetnek az appot használók teljes webes kommunikációjához, beleértve a weboldalakon beírt jelszavakat, videó hívásokat, letöltött programokat, stb. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a Windows 10 Insider Programban tesztelhető új tárterület-kezelő funkcióról.

Linksys router használók veszélyben

(securityweek.com)

A hackerek lopott hitelesítő adatokkal igyekeznek hozzáférést szerezni a Linksys routereihez. A gyártó ezért jelszócserét kényszerít ki a Linksys Smart Wi-Fi-t használó ügyfeleitől. A támadók sikeres hozzáférés után az útválasztók DNS beállításait úgy módosítják, hogy a felhasználókat egy letöltő oldalra irányítják, ahonnan látszólag egy COVID-19 témájú applikációt tölthetnek le, azonban a program valójában káros kódokat tartalmaz. A Bitdefender volt az első, amely késő márciusban beszámolt ezekről a támadásokról, amelyek főképp Linksys routerek ellen irányultak. A cég március végén figyelmeztette ügyfeleit, hogy a következő bejelentkezéskor kizárásra kerülnek Linksys Smart Wi-Fi fiókjukból, és csak új jelszó megadásával tudnak a jövőben bejelentkezni. **Bővebben...**

BIOS-védelmi biztonsági szoftvert ad ki a DEll ügyfeleinek

(thehackernews.com)

A Dell egy biztonsági szoftvert tesz elérhetővé ügyfeleinek, amelynek segítségével detektálhatóak a BIOS kompromittálására tett kísérletek. A SafeBIOS Events & Indicators of Attack (IoA) névre hallgató végpontvédelmi program automaikusan riasztást generál, amint a munkaállomás BIOS-ának beállításain gyanús módosítás történik. A BIOS védelme kritikus fontosságú, mert ennek kompromittálásával egy támadó irányítása alá képes vonni a teljes rendszert. SafeBIOS azonban képes időben figyelmeztetni, így lehetővé válik a fertőzött gép korai izolálása, ezzel csökkentve annak esélyét, hogy a fertőzés tovább terjedjen a hálózaton.

Új IoT botnet felemelkedőben

(securityaffairs.co)

Új IoT botnetet fedezett fel a Bitdefender. A Dark Nexus különböző típusú okoseszközöket – Dasan Zhone, Dlink és ASUS routereket, video rögzítő brendezéseket és hőkamerákat – kapcsol botnet hálózatba, hogy azután az eszközöket elosztott szolgáltatás megtagadást okozó támadások (DDoS) indítására használja fel. Jelenleg minimum 1 372 fertőzött eszközből áll a hálózat, amelyek elsősorban Kína, Dél-Korea, Thaiföld, Brazília és Oroszország területén találhatóak. **Bővebben...**