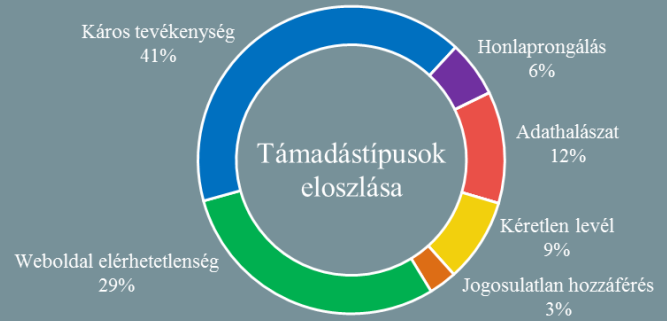


Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:  
2020.07.10. - 2020.07.16.



Kövessen minket megújult [weboldalunkon](#), ahol friss IT-biztonsági hírek kerülnek publikálásra!

## Megjelent a kiberfenyegetési csoportok enciklopédiája 2.0

([dropbox.com](#))

A ThaiCERT elkészítette a kiberfenyegetési csoportok enciklopédiájának (A Threat Actor Encyclopedia – TAE) második, bővített kiadását. A kiadvány kizárólag publikus forrásokra hagyatkozva igyekszik kompakt információval szolgálni a különböző kiberfenyegetési kollektívákról, bemutatva azok ismert aliasait, a vélhető földrajzi eredetüket, motivációikat, a támadott szektor(oka)t, az alkalmazott TTP-eket (Tactics, Techniques and Procedures – eszközök, taktikák, módszerek), illetve az adott csoport nevéhez köthető főbb műveleteket/kampányokat. **Bővebben...**



## Felhasználói után kémkedik a Welcome Chat

([bleepingcomputer.com](#))

Az ESET Android malware-  
elemzője, Lukas Stefanko [szerint](#) a biztonságos kommunikációt ígérő Welcome Chat androidos csevegőalkalmazás kémkedési funkcióval bír, és a felhasználói adatokat titkosítás nélkül, nyilvánosan elérhető módon tárolja. Az alkalmazás főleg azokat a közel-keleti országokban élő, arab nyelvű felhasználókat célozza, akik számára tiltott az ilyen típusú alkalmazások használata, azonban harmadik féltől származó alkalmazásboltokból töltenek le ilyen funkciójú appokat. **Bővebben...**

## Az eddigi legsúlyosabb Twitter hack

([theregister.com](#))

A népszerű közösségi platform történetének eddigi legsúlyosabb hacker támadását szenvedte el szerdán (2020.07.15-én), amelynek során a támadók több világszerte ismert közéleti személy (például: Bill Gates, Barack Obama, Joe Biden, Jeff Bezos, Elon Musk), valamint szervezet (pl. Apple, Uber) hivatalos Twitter fiókját felhasználva csaló üzenetekkel gyűjtöttek pénzt. A csalás abból állt, hogy az üzenetek a fiók tulajdonosának nevében azt állították, hogy aki a megadott Bitcoin számlára 1 000 dollárt utal, dupla ekkora összeget kap vissza. **Bővebben...**

## Mennyire biztonságos a TikTok?

([euronews.com](#))

Egyre több vizsgálat indul a TikTok adatkezelési gyakorlata feletti aggodalmak miatt, miszerint a pekingi bázisú alkalmazást a felhasználói adatok átadására kényszerítheti a kínai kormány. Az alkalmazás eddig konzekvensen tagadta, hogy bármilyen információt is szolgáltatna a kínai kormánynak, az Euronews azonban szakértők bevonásával arra kereste a választ, hogy mennyire lehet megbízni egy ilyen állításban. A sommás nemleges válasz hátterében több minden is megtalálható. A megkérdezettek többek közt kiemelik, hogy a lényegi kérdés nem csupán egy alkalmazás által gyűjtött adatok milyensége és mennyisége — ezek a legtöbb szolgáltatás esetében hasonlóak — hanem az is, hogy ezeket hogyan kezeli egy adott platform. **Bővebben...**

## Kritikus hibát javít a július havi Microsoft javítócsomag

([securityaffairs.co](#))

SigRed-nek nevezték el azt a kritikus kockázati besorolású biztonsági hibát ([CVE-2020-1350](#)), amely Windows DNS szerverekre nézve jelent fenyegetést. A hiba autentikáció nélkül, távolról kihasználható arra, hogy a támadó domain admin jogosultságot szerezzen a célzott rendszeren. A problémát súlyosbítja, hogy a sérülékenység lehetőséget ad rá, hogy a támadó egy adott infrastruktúrán további végpontokat fertőzzön meg felhasználói interakció nélkül, ezáltal teljes kontrollt nyerjen az adott infrastruktúrán. **Bővebben...**

## IT biztonsági Tanács



Az NBSZ NKI [weboldalán](#) hasznos információkat olvashat az utazási csalásokról és azok elkerülési módjáról.