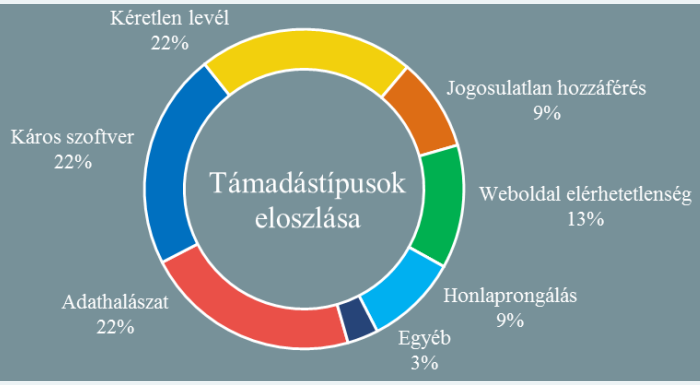
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 06. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.01.31. - 2020.02.06.



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

30. alkalommal tart csoporttalálkozót az ENISA az európai telekommunikációs szektor biztonsági kérdéseiről

(enisa.europa.eu)

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) az európai telekommunikációs szektor hatóságaival már tíz éve dolgozik szoros együttműködésben az EU-n belüli elektronikus kommunikációt szabályozó keretrendszer 13a pontjának implementálásán, olyan kérdésköröket érintve, mint például az incidens bejelentés és a telekommunikációs szolgáltatókra vonatkozó követelmények. **Bővebben...**

Vigyázat: androidos banki trójait terjesztő üzenetek érkezhetnek

(bleepingcomputer.com)

A Confense nevű IT biztonsági cég egy olyan adathalász kampányt azonosított, amelynek során a támadók az Anubis nevű banki trójai programot juttatják célba és mintegy 250 androidos banki és webshop alkalmazásból igyekeznek pénzügyi adatokat szerezni. Az áldozatoknak küldött e-mailben arra kérik a felhasználókat, hogy engedélyezzék a Google Play Protect szolgáltatást, valójában azonban éppen hogy letiltásra kerül annak működése, ezt követően pedig az Anubis települ az eszközre. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arról, hogy miként lehet adathalász leveleket bejelenteni a Gmail levelező rendszerben.

Részt vehet a Huawei az európai 5G hálózat kiépítési projektekben

(theverge.com)

Megjelentek az Európai Unió iránymutatásai az 5G hálózatok biztonsági kockázatainak kezeléséhez. Az EU az Egyesült Királysághoz hasonló döntést hozott a magas biztonsági kockázatú cégek ─ mint például a Huawei ─ részvételéről. Eszerint azon cégek is kaphatnak megbízást, amelyek ilyen minősítést kapnak a kockázatelemzés során, ugyanakkor bizonyos kritikus fontosságú rendszerelemeknél korlátozni kell a részvételüket. **Bővebben...**

Ezzel a szoftverrel ellenőrizhetjük, hogy fertőződött-e a gépünk EMOTET trójaival

(bleepingcomputer.com)

Az EMOTET trójai aktuálisan a legtöbb fertőzést okozó káros kód, amely kéretlen levelek csatolmányában szereplő Word dokumentumok útján terjed. Fertőzés esetén az áldozat munkaállomása spamelő robothálózatba (botnet) kapcsolódhat, hozzájárulva a káros kód terjesztéséhez. Ezen túl további káros kódok letöltődésére is számítani lehet, mint például a Trickbot, vagy a Ryuk ransomware. A japán CERT (JPCERTCC) készített egy EmoCheck névre keresztelt programot, amellyel Windows platformon detektálható a fertőzés. **Bővebben...**

Zsarolóvírus támadás sújtotta a wisconsini Raciene város rendszereit

(securiyaffairs.co)

Zsarolóvírus támadás érte az amerikai Wisconsin államban található Racine város számítógépes rendszereit 2020. január 31-én pénteken, amelynek következtében a város több informatikai szolgáltatása elérhetetlenné vált. A fertőzés nem érintette az adóbeszedési rendszert, a 911-et, valamint a közbiztonsági rendszereket, ugyanakkor a város weboldala, levelezése, továbbá az online díjbefizető rendszer még a cikk megjelenésének pillanatában is offline volt, a rendőrség pedig per pillanat nem képes rendőrségi vagy baleseti jelentésekről másolatot kiállítani. **Bővebben...**