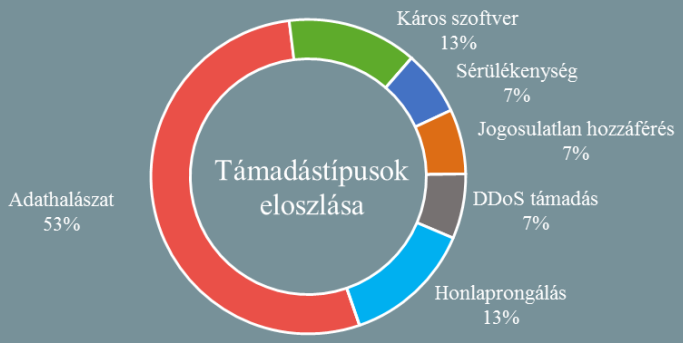
NEMZETI KIBERVÉDELMI INTÉZET

# Nemzetközi IT-biztonsági sajtószemle

2019. 29. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.07.12. - 2019.07.18.


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

## Súlyos adatlopás történt Bulgáriában

**(zdnet.com)**

Egy hacker (vagy hacker csoport) több millió bolgár állampolgár személyes adatát lopta el, majd az adatokra mutató linkeket elküldte helyi újságoknak. Az adatok forrásának a bolgár adóhatóságot, a National Revenue Agency-t (NRA) tartják. Az NRA weboldalán elismerte az incidenst, és közölte, hogy a belügyminisztériummal, valamint az Állami Nemzetbiztonsági Ügynökséggel (State Agency for National Security – SANS) együttműködve vizsgálják az incidenst, amely jelenleg az adatok hitelességének ellenőrzésénél tart. Az esetről értesülő média orgánumok szerint a támadást magára vállaló hacker azt állítja, hogy az adatlopásban a hétmilliós ország mintegy öt millió állampolgára érintett. Az adatok összesen körülbelül 21 GB-ot tesznek ki, amelynek első körben csak a felét tette elérhetővé, a maradékot a következő napok során tervezi közreadni. A kompromittálódott személyes információk között szerepelnek a polgárok nevei, személyi számai, címei és keresetei, azonban ezek többnyire nem friss, hanem még 2007-es információk.

## Visszafejthetők a GrandCrab zsarolóvírus által titkosított fájlok

**(darkreading.com)**

A GandCrab ransomware (zsarolóvírus ) készítői június elején bejelentették, hogy 18 hónapnyi működés ─ és állításuk szerint összesen több, mint 150 millió dollárnyi bevétel ─ után beszüntetik a zsarolóvírus hálózat (Ransomware-as-a-service) működtetését. Az FBI pedig július 15-én arról adott hírt, hogy elérhetővé teszik a visszafejtő kulcsokat a káros kód aktuális verzióihoz (4-5.2). A titkosított állományok visszafejtését lehetővé tévő dekriptor szoftver a No More Ransom projekt weboldalán (nomoreransom.org) érhető el. Jó hír ez a vírus eddigi áldozatainak, azonban a jövőben új verziók megjelenésére lehet számítani.

## Linuxos felhasználókat fenyeget az EvilGnome kémprogram

**(thehackernews.com)**

Biztonsági kutatók felfedeztek egy kiterjedt képességekkel rendelkező új linuxos kémprogramot (EvilGnome), amelyet az antivírus szoftverek jelenleg nem képesek azonosítani. Linux rendszerekre – a Windowshoz képest – alapvetően kevés kártevő készül, ami egyrészt az architektúra jellegéből adódik, másrészt abból, hogy ezt az operációs rendszert jóval kevesebben használják. A linuxos malware-ek jelentős részére inkább az a jellemző, hogy a fertőzött eszközökön kriptovaluta bányászatot végeznek, vagy azokat DDoS botnet hálózatba kapcsolják. **Bővebben...**

## Az Emberi Jogok Európai Bírósága előtt a svéd és angol megfigyelési programok

**(zdnet.com)**

Az Emberi Jogok Európai Bírósága (European Convention on Human Rights – ECHR) Svédország és az Egyesült Királyság tömeges megfigyelési programja kapcsán tartott meghallgatást a múlt hét során. A jogvédő szervezetek által kezdeményezett jogi eljárások már évek óta tartanak, és most értek a bíróság legfelső testületéhez, a Nagykamarához (Grand Chamber). Mindkét esetben hasonló vádak hangzottak el, miszerint a hírszerzési műveleteket a kormányzatok megfelelő felügyelet és ellensúlyok hiányában végezték. Svédország esetében ─ miután a 2008 óta tartó pereskedés során már több alkalommal módosították a törvényt, különböző biztosítékok beépítésével ─ az ECHR végül az állam mellett döntött tavaly, az eljárást kezdeményező svéd helyi alapítvány (Centrum för rättvisa) azonban ezt nem fogadta el. **Bővebben...**

## Bármelyik Instagram fiók feltörhető volt

(securityaffairs.co)

Kritikus biztonsági hibát fedeztek fel a Facebook tulajdonában álló fotómegosztó alkalmazásban, az Instagramban. A biztonsági rés lehetővé tette a támadók számára, hogy felhasználói interakció nélkül teljesen átvegyék az irányítást egy adott fiók felett. Egy indiai biztonsági szakértő, Laxman Muthiyah jelentette a biztonsági rést, ami a szolgáltatás mobil verziójának jelszó visszaállítási implementációját érintette. A jelszavak visszaállítása során a felhasználók e-mailben vagy SMS-ben kapnak egy tíz percig aktív, hat számjegyből álló kódot, amellyel megerősíthetik a műveletet. Amennyiben hozzáférést szeretnének szerezni egy fiókhoz, a támadóknak ez idő alatt kell a lehetséges egy millió kódkombinációt kipróbálniuk. A szakértő ezzel kapcsolatban azonban egy súlyos hiányosságot fedezett fel, miszerint a jelszó visszaállítási folyamat kapcsán nincs megfelelően szabályozva, hogy az érvényességi időn belül a rendszer hány jelszó próbálgatási kérést fogad el. Bővebben...

### IT biztonsági Tanács

Amennyiben az Amerikai Egyesült Államokba készülünk a nyaralás alatt, jó, ha tudjuk, hogy az amerikai határőrség, U.S. Customs and Border Protection (CBP), számára engedélyezett az utazók elektronikus eszközeinek tartalmának megismerése az országba történő be - és kilépéskor, külön végzés nélkül.

A digitális jogok érvényesítéséért küzdő Electronic Frontier Foundation (EFF) ajánlása szerint javasolt néhány megelőző intézkedést tennünk, amelyekről itt olvashat bővebb információkat.

## Manipulálhatók az Android üzenetküldő alkalmazásokban küldött médiafájlok

(www.theverge.com)

A Symantec új jelentést adott közre az üzenetküldő alkalmazások biztonságára vonatkozóan, amelyből kiderül, hogy míg a szöveges üzenetek titkosításra kerülnek a végpontok közötti áthaladás során, addig az alkalmazásokon keresztül küldött médiafájlok könnyedén módosíthatóak egy rosszindulatú harmadik fél számára. Androidos eszközök esetén az alkalmazásokon belül továbbított kép és hangfájlok belső vagy külső tárhelyen is tárolódhatnak. A WhatsApp esetében például a külső adathordozó az alapértelmezett, a Telegramnál viszont ez csak a „Mentés a galériába” funkció engedélyezése esetén érhetők el. A problémát ezzel kapcsolatban az jelenti, hogy a külső adattárolóhoz számos más alkalmazás is hozzáférhet. **Bővebben...**

## Adathalász elleni automatikus védelmi funkcióval bővül a Microsoft Forms

(bleepingcomputer.com)

A Microsoft 365 szolgáltatásának részét képező, online kvízek és felmérések készítését lehetővé tévő Microsoft Forms egy új biztonsági funkcióval egészül ki (Automatic Phishing Detection), amely lehetővé teszi az adathalász tartalmak automatikus észlelését. A Forms ezután gépi segítséggel detektálni fogja a jelszavak és egyéb szenzitív adatok gyűjtését, a tervek szerint ezáltal megakadályozva, hogy rosszindulatú felhasználók adathalászatot végezzenek a szolgáltatás segítségével. Mindazonáltal a gyanúsnak vélt tartalmak kézi bejelentésére is van lehetőség, a felhasználók ezeket az űrlap alján található „Visszaélés bejelentése” gombra kattintva is jelezhetik. Az intézkedés indokolt, ugyanis az elmúlt években jelentősen nőtt a Microsoft Forms felhasználásával készített adathalász oldalak száma. **Bővebben...**

## A kazah kormány elkezdte megfigyelni a teljes HTTPS forgalmat

(zdnet.com)

Július 17-től kezdődően a kazah kormányzat elkezdte megfigyelni az országon belüli teljes HTTPS ─ azaz titkosított ─ webes forgalmat. Mindez technikailag úgy kerül kivitelezésre, hogy a felhasználóknak telepíteniük kell egy webes gyökértanúsítványt (root certificate) minden asztali és mobil eszközön. A tanúsítvány lehetőséget biztosít a kormányzati ügynökségek számára, hogy a felhasználók titkosított webes forgalmába ékelődve a teljes hálózati forgalmat kibontsák, majd a kommunikáció tartalmának megismerése után újra titkosítsák és továbbítsák a címzett felé. **Bővebben...**

## Több ország is vizsgálatot indít a FaceApp adatkezelésével kapcsolatos vádak miatt

(securityweek.com)

A Google Playen már két éve elérhető az „arcöregítő” funkcióval bíró FaceApp, azonban népszerűsége csak az utóbbi időben nőtt meg ugrásszerűen, jelenleg azonban már listavezető az ingyenesen letölthető alkalmazások között, több, mint 100 millió letöltéssel. Az appot fejlesztő cég, a (Wireless Lab) vezetője, Yaroslav Goncharov a Washington Postnak nyilatkozva hiába igyekezett eloszlatni a vádakat ─ miszerint az alkalmazás felhasználja a felhasználók képeit, valamint, hogy az orosz hatóságok hozzáféréssel bírnak a felhasználók adataihoz ─ már több ország is jelezte, hogy vizsgálatot kíván indítani a FaceApp adatkezelésével kapcsolatban. **Bővebben...**