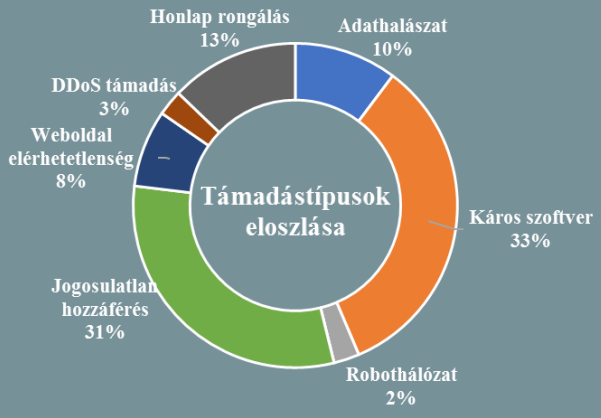
**Incidens adatok:**
2017.06.28. — 2017.07.04.


## Mi lehetett a NotPetya zsarolóvírus támadás valós célja?

**(www.healthcareinfosecurity.com)**

Több elemző egybehangzó véleménye szerint a múlt hét kedden kirobbant világszintű zsarolóvírus támadás célja valójában nem a profitszerzés volt. Matt Suiche, a dubai székhelyű Comae Technologies ügyvezető igazgatója úgy gondolja, a zsarolóvírus csak egy álca volt és a káros kód lényegében egy ún. 'wiper', egy olyan típusú malware, amelynek a célja a szándékos károkozás. Leginkább a tevékenysége az, ami erre utalhat: kezdetben ugyan az áldozat adatait enkriptálja, később azonban az operációs rendszer olyan összetevőivel is ezt teszi (Master Boot Record, majd a Master File Table), amelyek kritikusak a rendszer működése szempontjából. Oleh Derevianko, egy ukrán biztonsági cég munkatársa hozzáteszi, a pusztítás mellett cél lehetett korábbi támadások nyomainak eltűntetése is. **Bővebben...**

## Lehetséges katonai válasz a kibertámadásokra

**(www.tech.firstpost.com)**

A NATO kibervédelmi központja közleményben tudatta, hogy a több, mint 60 országot érintő 'NotPetya' zsarolóvírus támadás hátterében minden valószínűség szerint egy állami jóváhagyással rendelkező hacker csoport állhatott. A nyilatkozat azt is említi, hogy amennyiben egy kibertámadás által okozott kár mértéke egy katonai támadáshoz mérhető, a szövetséges nemzeteknek lehetőségük van azt háborús cselekményként értelmezni és ennek megfelelően, valamint – az Észak-atlanti Szerződés 5. cikkelye alapján – kollektívan eljárni. Hozzáteszik azonban azt is, hogy a mostani esetre ez nem vonatkozik. **Bővebben...**

## Az európai CSIRT hálózat ismét bizonyított

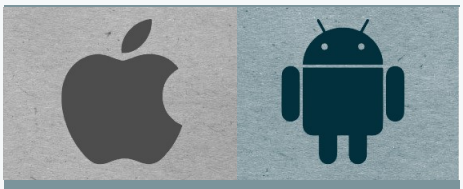
**(www.enisa.europa.eu)**

Sikeres volt a tagállamok incidens kezelő csoportjai (EU MS CSIRTs) közötti együttműködés a 'NotPetya' zsarolóvírus kampány kapcsán – áll az ENISA közleményében. A CSIRT-ek időben tudtak reagálni az eseményekre és a jól kialakított kommunikációs csatornáknak köszönhetően a határokon átívelő információáramlás nagyban hozzájárult a fenyegetés gyors megértéséhez, az elhárítási megoldások kidolgozásához és a nemzeti szintű incidenskezeléshez. A májusi 'Wannacry' mellett a mostani kampány is jó alkalom volt az MS CSIRT-ek közötti bizalom és operatív együttműködés építéséhez. **Bővebben...**

## Amerika vs. Kaspersky Lab

**(www.ibtimes.co.uk)**

Egy új törvényjavaslat szerint az Egyesült Államok Védelmi Minisztériumának rendszereiből kitiltanák a Kaspersky Lab szoftvereit, abból a gyanúból kiindulva, hogy a cég az orosz kormány befolyása alatt állhat és termékeiket kiberkémkedésre használhatta. Egy nappal korábban az FBI a cég amerikai munkatársait otthonukban kikérdezte, azonban eddig bizonyítékokkal nem jelentkeztek. A gyanú először májusban röppent fel, amikor a cégvezető Eugene Kaspersky határozottan tagadta, hogy bármilyen kormányzat befolyása alatt állnának és jelezte, kész a védelmi szoftverek forráskódját is elemzésre bocsátani. Egyes tisztségviselőknek ugyanakkor éppen vele szemben van fenntartásuk, például a KGB-hátterű Institute of Cryptography, Telecommunications, and Computer Science-ben végzett tanulmányai miatt. **Bővebben...**



## Biztonságosabb ujjlenyomat azonosítás

**(www.infosecurity-magazine.com)**

A 2017-es Mobile World Congress -en jelentette be a Qualcomm az új generációs ujjlenyomat olvasó szenzorát. A legnagyobb újdonság, hogy a szenzor a kijelzőpanelbe integrálható, de akár üvegbe, fémbe is beépíthető, illetve víz alatt is működni fog. Az új ultrahang alapú technológia emellett a felhasználó szívverését is képes észlelni, ezzel fokozott védelmet nyújtva például a lenyomatlopásos támadásokkal szemben. **Bővebben...**

## Arcfelismerés az Apple-ben

**(www.bloomberg.com)**

Ujjlenyomat olvasó helyett egy új 3D-s arcfelismerő funkción dolgozik az Apple, mely biztonságosabbá teszi a biometrikus azonosítást a 'Touch ID' ujjlenyomat szkennernél, mivel az új megoldás több adatpontot rögzít. A Samsung írisz olvasó hibájából tanulva a 3D-s mélységérzékelővel a tervek szerint nem lehet majd fényképpel kijátszani a rendszert. A hírek szerint a 3D szenzor vélhetően a következő iPhone modellben válik először elérhetővé. **Bővebben...**

## IT biztonsági Tanács

Az internetes vásárlás előnye a kényelem, azonban komoly veszélyeket is hordozhat magában.

Ezért soha ne adja ki bankkártya adatait e-mailben és részesítse előnyben azokat az online shopokat, melyeket ismer. Mindig olvassa el a szerződési feltételeket, valamint őrizze meg vásárlással kapcsolatos dokumentumokat (mentse le).

## Elfogadták Kanada új nemzetbiztonsági törvényét

**(www.tripwire.com)**

A C-59-es törvény egyik fő célja szerint ki szeretné terjeszteni a terrorista-elhárítási feladatokkal, valamint a megfigyelésekkel és kiberhadviseléssel kapcsolatos állami felügyeletet és kontrollt. Utóbbi kapcsán a 'Five Eyes' államok és a NATO intézkedéseivel összhangban hoz lényeges szabályzási lépéseket. Eszerint a nemzeti védelmi feladatokat a kanadai védelmi minisztérium (DND) és a SIGINT műveletekért felelős Kommunikációs Biztonsági Szervezet (CSE) feladatkörébe utalja és új tevékenységekként definiálja a védekező, valamint a megelőző kibertámadásokat. Egy széles körben implementált – jellemzően a civil szférára hatást gyakoroló – kategória, az ún. 'Defenzív Kiberműveletek - Válaszintézkedések' (DCO-RA) azonban teljesen hiányzik. **Bővebben...**

## Adatvédelmi hatásvizsgálat (DPIA)

**(www.itgovernance.co.uk)**

A GDPR által meghatározott eljárások egyikeként a szervezeteknek fel kell mérniük, hogy egy tervezett vagy már meglévő művelet milyen kockázatot jelent az egyének jogaira nézve. A DPIA segíti a vállalatokat, hogy egy projekt korai szakaszában felmérjék és kiküszöböljék a fennálló kockázatokat. 2017. július 19-én Londonban a szervezeteknek lehetőségük van részt venni egy DPIA Workshop-on, melynek célja, hogy a delegáltak számára gyakorlati ismereteket biztosítson a hatékony DPIA-k megvalósításához. **Bővebben...**

## Együttműködés nélkül nem megy

**(www.sfgate.com)**

Meng Hongwei a keddi biztonsági kongresszuson szoros együttműködésre szólította fel a nemzeteket és a bűnüldöző hatóságokat, utalva a 'WannaCry' támadássorozatra. Az online szolgáltatások exponenciális növekedése folyamatos, ennek következtében a támadások esetében sem számíthatunk másra. A fenyegetésekre most már jellemző, hogy nemzetközi méretűek, emiatt az államoknak nem lesz lehetőségük egyedül szembenézni ezekkel a kihívásokkal. **Bővebben...**

## Megelőző biztonsági intézkedések a G20 csúcs miatt

**(www.venturebeat.com)**

Németországban komoly az aggodalom, hogy a 2017. július 7-8 között esedékes G20-as csúcstalálkozót kibertámadás érheti. A német Szövetségi Információbiztonsági Hivatal (BSI) szerint a hatóságok védekezésképp létrehoztak egy 24/7-es parancsnoki központot és habár jelenleg tervezett akcióról nincs tudomásuk, az ügynökség sérülékenység vizsgálatok során mérte fel a kockázatokat. A szeptemberi választások kapcsán pedig poltikai pártokkal és törvényhozókkal együttműködve megkezdték az alkalmazottak biztonságtudatosságának erősítését. **Bővebben...**

## Rekordösszegű büntetés

**(www.bbc.com)**

A Google-t 2.42 milliárd euróra büntette az Európai Biztottság, amiért a Google Shopping nevű termék-összehasonlító szolgáltatását tisztességtelen piaci előnyhöz juttatta azáltal, hogy a keresési találatok tetején jelenítette meg. Eddig ez a legmagasabb összegű bírság, amit piactorzítás vádjával szabott ki az EU és amennyiben a keresőóriás nem hagy fel a gyakorlattal 90 napon belül, további szankciókra is számíthat. A Google az esettel kapcsolatban jelezte, hogy elutasítja a vádakat és fellebbezést fontolgat. **Bővebben...**