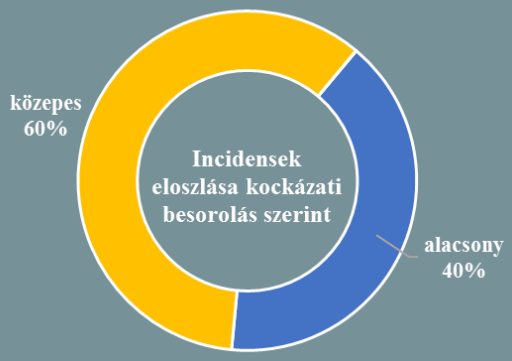
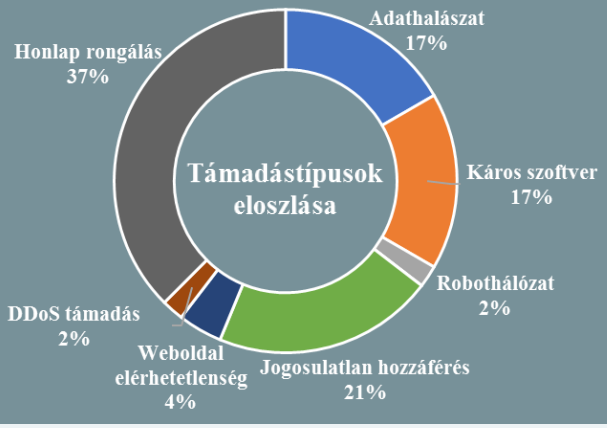
Incidens adatok:
2017.07.26. — 2017.08.01.





Nagyszabású kiberbiztonsági gyakorlatot tart az EU

(www.euractiv.com)

2017. szeptember 1. és október 11. között kiberbiztonsági gyakorlaton vesznek részt az Európai Unió tagállamai, amihez EU-n kívüli NATO-tagországok is csatlakozhatnak. A cél felmérni, hogyan reagálnak az egyes nemzetek a kiberbiztonsági támadásokra és fenyegetésekre, valamint fejleszteni a résztvevők technikai képességeit. A forgatókönyvek a lehető legvalósághűbb módon igyekeznek szimulálni a fenyegetéseket, ennek megfelelően az egyik ismert scenario egy EU tagállamok kritikus infrastruktúrája ellen intézett kiterjedt támadást ír le, míg egy másik – terrorista hátterű fenyegetés – az energetikai és a katonai szektort célozza majd. Egy átfogó intézkedési terv részeként az Európai Bizottság a gyakorlat idején tervezi nyilvánosságra hozni – többek között – az új kiberbiztonsági törvényjavaslatát és a frissített EU-s kiberbiztonsági stratégiát. **Bővebben...**

Hackertámadás érhette a FireEye kutatócsapatát

(www.cio.economictimes.indiatimes.com)

A támadók közzétettek egy tömörített fájlt, ami körülbelül 370 megabájtnyi személyes és szakmai anyagot tartalmaz, ami a FireEye kriminalisztikai tanácsadó egységének (Mandiant) egy alkalmazottjához köthető. Ezen kívül hozzáférést szereztek a személy LinkedIn fiókjához is, ahol nem oda illő tartalmat helyeztek el. A FireEye hétfőn megerősítette, hogy egy kiberbiztonsági kutatójuk online adatai szivárogtak ki, azonban azt tagadták, hogy a vállalat rendszerei kompromittálódtak volna. A cég szóvivője elmondta, az esettel kapcsolatban vizsgálatot kezdeményeztek, és lépéseket tettek a későbbi hasonló problémák megelőzésére. **Bővebben...**

Google felmérés a zsarolóvírusok által termelt profitról

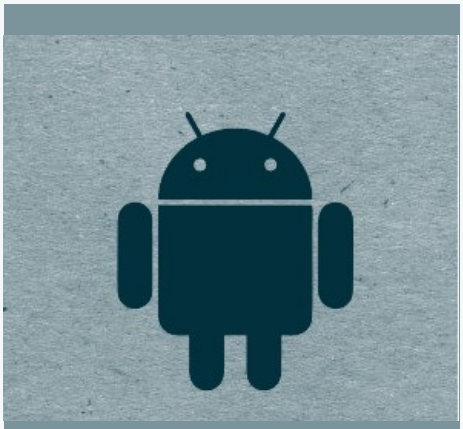
(www.threatpost.com)

A 2017-es Black Hat konferencián megjelent tanulmányban több nagyvállalat adatai alapján mérték fel a zsarolóvírusok által okozott károkat és az általuk szerzett bevételek mértékét. Az eredmények szerint az elmúlt két év során összesen 35 egyedi ransomware variáns segítségével a kiberbűnözők összesen mintegy 25 millió dollárt kerestek. A legsikeresebb törzsnek a 'Locky' bizonyult, ez a malware család az összbevétel 28%-áért (7,8 millió dollár) felelős. A Google kutatói arra figyelmeztetnek, hogy az év hátralévő részében a 'ransomware-as-a-service'-nek (RaaS) köszönhetően a zsarolóvírusok okozta fenyegetés nőni fog, csakúgy, mint a pusztító célú malware (wiper) támadások száma. **Bővebben...**

Észak-Korea pénzt gyűjt

(www.firstpost.com)

A Dél-Koreai South's Financial Security Institute (FSI) jelentése szerint az Észak-Korea által indított kibertámadások motivációjában az utóbbi években változás figyelhető meg. A korábbi főbb célpontok – a katonai és kormányzati szektor – mellett egyre gyakoribbak a pénzügyi szervezetek elleni támadások, amelynek hátterében a külföldi valutaszerzés áll. Az eddigi incidenseket elsősorban a 'Lazarus' csoporthoz kötötték, de azóta már több, eltérő profillal rendelkező alcsoportot is azonosítottak, ilyen például a 'Bluenoroff' és az 'Anderiel'. Utóbbi legalább 2016 májusa óta lehet aktív és tevékenysége elsősorban a dél-koreai üzleti és kormányzati szférára irányul. **Bővebben...**



Új szereplő vált ismertté a kémszoftver piacon

(www.motherboard.vice.com)

A Google biztonsági kutatói felfedeztek egy új Android platformra készült kémprogramot, amely képes a felhasználó e-mailjeinek, SMS-einek, beszélgetéseinek lehallgatására. Elemzések során megállapították, hogy az egy eddig relatíve ismeretlen izraeli cég, az Equus Technologies-hez köthető. A magánkézben lévő vállalat testreszabott megoldásokat fejleszt bűnüldöző hatóságok és hírszerző ügynökségek számára. Egy, a céget közelebbről ismerő forrás a Motherboard-nak elmondta, az Equus Technologies már évek óta a piacon van, és iOS alapú szoftvereket is gyártanak. **Bővebben…**

IT biztonsági Tanács

A kémprogramok működésük során igyekeznek észrevétlenek maradni, ennek ellenére magunk is felfedezhetjük a főbb intő jeleket, például:

- gyorsabban merül a telefon
- megnövekedett adatforgalom
- szokatlan működés, rendszeres leállás
- rendellenes háttérzaj hívás közben
- furcsa szöveges bejövő üzenetek

Ezeket tapasztalva, érdemes egy kémprogram kereső és eltávolító szoftver alkalmazása.

Alakul az indiai nemzeti tűzfal koncepciója

(www.cio.economictimes.indiatimes.com)

Az elmúlt időszakban történt globális kibertámadások (lásd: Wannacry, NotPetya) és a világszerte jellemző nemzeti kibervédelmi intézkedések hatására az indiai kormány egy országos tűzfal létrehozását tervezi, amely – legalábbis kezdetben – a kormányzati szektor védelmét látná el. A zsarolóvírus és botnet támadások megnövekedett száma mellett Indiát is érte már feltételezhetően állami hátterű kibertámadás, például egy Kínához köthető hacker csoport 2015-ben képes volt betörni két prominens indiai IT vállalat rendszerébe. Szakértők véleménye szerint a multinacionális vállalatok és egyéb nem állami szervezetek számára legalább ennyire fontos a tervezett többrétegű védelmi rendszer, de ezzel kapcsolatban még nem született megállapodás. A konkrét tervek kidolgozásához júniusban már meg is történt az első ülés, amelyen kormányzati és IT biztonsági szereplők vettek részt. **Bővebben...**

Mennyire használnak virtuális fizetőeszközöket a terroristák

(www.deepdotweb.com)

Az Európai Bizottság tanulmányt készített a terrorizmus finanszírozás (TF), valamint a pénzmosás (ML) európai pénzügyi piaccal való kapcsolatairól. Eszerint számba vették a főbb pénzügyi szolgáltatásokat, termékeket és ezekre vonatkoztatva határozták meg a fókuszban lévő tevékenységekből fakadó kockázatokat, illetve az okozott hatásokat. Kiemelten vizsgálták a kripto-fizetőeszközök részvételét a bűnszervezetek műveleteiben, amelynek kapcsán arra a következtetésre jutottak, hogy terrorizmussal és pénzmosással összefüggésben jellemzően nem használnak kripto-valutákat (például: Bitcoin, Monero, Litecoin), amelynek elsősorban az az oka, hogy – habár igény egyértelműen volna rá – a bűnözők részéről hiányzik a megfelelő szintű technikai tudás. Így a fenyegetési szintet ennek kapcsán mindkét vizsgálati szempontból „közepesen jelentősnek” (level 2) értékelték. **Bővebben...**

A Facebook szerint kontraproduktív a kripto backdoor koncepció

(www.theregister.co.uk)

Sheryl Sandberg, a Facebook vezérigazgatója úgy véli, nem segíti a terrorizmus visszaszorítását az üzenetküldő alkalmazások titkosításának gyengítése, sőt véleménye szerint ezáltal még kevesebb információ kerül majd a kormányok birtokába, mint korábban. A tech cég ugyanis – legalábbis a nem titkosított metaadatok szintjén – eddig is igyekezett megfelelni a kormányzati információigényeknek. A szigorító intézkedések miatt azonban a bűnözők valószínűleg más platformok után néznek majd, amelyeken nem feltétlenül érvényesül majd bármilyen kormányzati befolyás. Sandberg kiemelte, hogy a Facebook jelenleg is működtet egy 4 500 fős csapatot a terrorizmussal összefüggésbe hozható tartalmak és a gyűlöletbeszéd szűrésére és ezen a területen további 3 000 fős bővítést terveznek. **Bővebben...**

IoT szerverek veszélyben

(www.zdnet.com)

Lucas Lundgren biztonsági tanácsadó figyelmét egy kevésbé hivatkozott, ellenben igen széles körben használt és sajnos gyakran rosszul implementált üzenetküldő protokoll (MQTT) keltette fel. Ennek során a világ szinte minden pontján talált sérülékeny kiszolgáló szervereket (körülbelül 87 000 darab), amelyek hibás konfigurálás miatt támadás kivitelezésére nyújthatnak lehetőséget, amellyel szélsőséges esetben akár vonatkatasztrófát is okozhatnak. **Bővebben...**