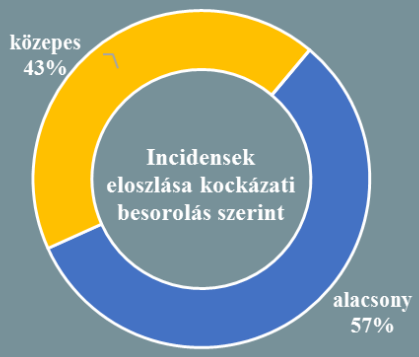
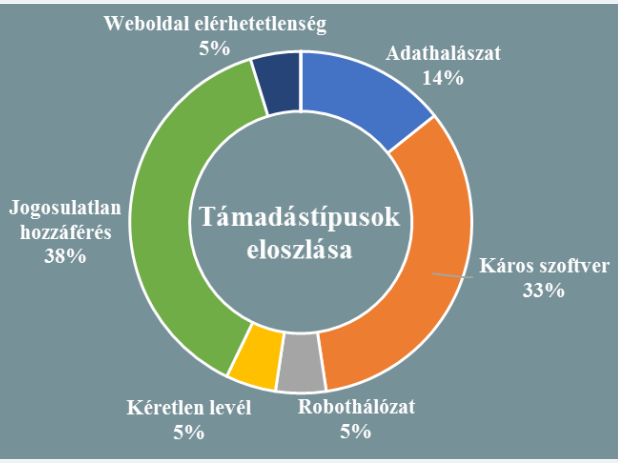
Incidens adatok:
2017.07.19. — 2017.07.25.





Microsoft vs. Fancy Bear

(www.thedailybeast.com)

A Microsoft beperelte a 'Fancy Bear' néven azonosított hacker csoportot, számítógépes behatolás és a Microsoft védjeggyel szemben elkövetett jogsértés vádjával. Ennek alapja, hogy az Oroszországhoz kötött csoport többnyire Windows rendszereket támad és Microsoft terméknevekre hasonlító domain neveket használ a tevékenysége során. A Microsoft kezdeményezésének célja támadást intézni a Fancy Bear infrastruktúrája ellen, a szerintük leggyengébb ponton, a vezérlőszervereken keresztül. A cég stratégiája szerint ahelyett, hogy fizikai hozzáférést szereznének a szerverekhez, inkább azon domain-ek felett igyekeznek felügyeletet szerezni, amelyeken keresztül a fertőzött munkaállomások kommunikálnak. Mivel azonban a hackerek folyamatosan új domaineket regisztrálnak, a techóriás terve, hogy az eddig megfigyelt domain foglalási mintázatok alapján olyan domain neveket is megszerezzen, amelyeket még nem regisztráltak, de a mintázatba illeszkednek. **Bővebben...**

Kína kémprogram telepítésére kötelezi a muszlim lakosságot

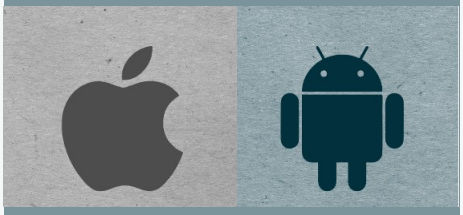
(www.news.softpedia.com)

A kínai kormány a terroristagyanús tartalmak kiszűrésére hivatkozva arra kényszerít egyes etnikai kisebbségeket, hogy mobil készülékükre egy olyan alkalmazást telepítsenek, amelynek segítségével a tevékenységük nyomonkövethető. Az intézkedés eddig csak Urumqi lakosságát érintette, amely többségében muszlim vallású. A helyiek egy népszerű kínai csevegő platformon, a 'WeChat'-en keresztül kaptak felszólítást a hatóságoktól a 'Jingwang' nevű Androidos alkalmazás telepítésére. Ez többek között képes rögzíteni egyes csevegő programokon folytatott beszélgetéseket, Wi-Fi bejelentkezési információkat, egyes készülékadatokat (IMEI szám, SIM kártya szám) illetve képes a készüléken tárolt médiafájlok begyűjtésére és egy kormányzati szerverre való továbbítására. A következő hetekben a lakosság szúrópróbaszerű ellenőrzésekre számíthat, és akinél nincs telepítve az alkalmazás, akár tíz nap elzárással is büntethető. **Bővebben...**

Svédország történetének legnagyobb adatszivárgása

(www.bleepingcomputer.com)

2015 szeptemberében történt, amikor a Svéd Közlekedési Ügynökség (STA) úgy döntött, hogy kiszervezi adatbázisának és egyéb informatikai szolgáltatásaink kezelését olyan vállalatokhoz, mint az IBM a Cseh Köztársaságban és az NCR Szerbiában. Az egész adatbázist feltöltötték a két céghez tartozó felhőszerverekre, és egyes alkalmazottak teljes hozzáférést kaptak az adatbázishoz, minthogy a svéd IT alkalmazottakat elbocsátották. A svéd titkosszolgálat csak 2016 márciusában szerzett tudomást a történtekről és kezdeményezett vizsgálatot. Egyes svéd újságok értesülései szerint a kiszivárgott adatbázisban érzékeny adatok szerepeltek – többek között – az összes svéd vezetői engedélyről, minden svéd állampolgárról (személyes és rendőrségi nyilvántartásban szereplő adatok), emellett kormányzati és katonai járművekről, pilótákról, illetve Svédország különleges katonai egységéről és közlekedési infrastruktúrájáról. **Bővebben...**



Trusted Contacts megjelent iOS rendszerre is

(www.engadget.com)

A Google iOS eszközökre is elérhetővé tette a Trusted Contacts nevű alkalmazását, ami a Facebook hozzáférés segítségével automatikusan képes megosztani állapotunkat a közeli barátainkkal és családtagjainkkal. **Bővebben…**

Play Protect, az Android új biztonsági rendszere

(blog.malwarebytes.com)

A Play Protect a Google alkalmazásboltjába történő integrálásával csökkenti a felhasználók által a készülékre telepített alkalmazások biztonsági kockázatainak mértékét. Az újonnan bevezetett biztonsági funkció segítségével a letöltés előtt, illetve a már korábban a készülékre telepített alkalmazásokat periódikusan ellenőrzi. **Bővebben...**

IT biztonsági Tanács

Napjaink egyik legjövedelmezőbb támadási formája az adathalászat.

Legyünk különösen elővigyázatosak a céges e-mail fiókra érkező üzenetekkel szemben (is), amelyekben pénzkifizetést kérnek tőlünk, még akkor is, ha az üzenet látszólag egy jogszerű fizetési igényre hivatkozik és ismert partnertől érkezett. Minden esetben ellenőrizzük a kérést!

Bíróság előtt a Deutsche Telekom-ot támadó hacker

(www.bleepingcomputer.com)

Egy 29-éves férfi bíróság előtt bűnösnek vallotta magát a Deutsche Telekom hálózatát ért 2016-os kibertámadás kivitelezésének vádjában, amely több mint 900 000 hálózati eszköz felé irányult és mintegy 1,25 millió felhasználó internet elérésében okozott fennakadást. A hacker a bíróságon elmondta, a routerek felett a 'Mirai' (IoT eszközöket támadó malware és egyben botnet hálózat) egy saját variánsával szerzett irányítást. Célja azonban nem az volt, hogy az eszközök működését ellehetetlenítse, hanem DDoS támadásokhoz szerette volna azokat felhasználni. Erre állítása szerint egy – eddig nem nevesített – libériai internet szolgáltató bérelte fel 10 000 dollárért. A több becenéven is (Spiderman, BestBuy, Popopret) ismert személyt más kiberbűnözői tevékenységhez is kötik, például a 'GovRAT' malware megalkotásáért és értékesítéséért is őt teszik felelőssé. **Bővebben...**

Újfajta módszer a kritikus infrastruktúrák ellen

(www.infosecurity-magazine.com)

Egyre több aggodalomra adnak okot a kimondottan a kritikus infrastruktúrák vezérlőrendszereit (ICS) érő támadások és az újabb és újabb szofisztikált módszerek, amelyek a hagyományos védelmi megoldásokkal nem, vagy csak nehezen detektálhatók. A legutóbbi, az Egyesült Államok energiaszektorát célzott adathalász támadások során alkalmazott technika például annyiban tér el a már jól ismert eljárástól, hogy a csatolmányban szereplő Word dokumentum nem káros kódot, csupán egy beágyazott külső hivatkozást tartalmazott. Amennyiben a felhasználó erre rákattintott, a támadók érzékeny, a felhasználói fiókra vonatkozó információkat voltak képesek megszerezni, valamint egy fertőzött Word sablon is letöltődhetett. **Bővebben...**

Kína a AI fejlesztés terén piacvezető szerepre tör

(www.infosecurity-magazine.com)

Az ország gazdasági növekedését támogatandó, Kína nagyarányú fejlesztéseket irányzott elő a mesterséges intelligencián (AI) alapuló feltörekvő iparágak tekintetében, mint például az intelligens hardware és szoftver fejlesztés, a robotika és az IoT alapú eszközök. A kínai kormányzat ennek érdekében három fő fázisra bontotta a terv kivitelezését, amelynek célja, hogy az ország 2030-ra az első számú AI központtá váljon nemzetközi szinten. A nagyszabású tervekkel összecseng a PwC múlt havi jelentése is, amely szerint a globális GDP 2030-ra 14%-kal fog nőni az AI technológiáknak köszönhetően és a legnagyobb arányú növekedést (26%) Kína produkálja majd. **Bővebben...**

Pusztító támadásokra figyelmeztet a Cisco

(www.securityweek.com)

A Cisco évközi kiberbiztonsági jelentésében számba veszi az aktuális fenyegetési trendeket, mint például a Business Email Compromise (BEC) típusú adathalász támadások előretörése, a növekvő spam aktivitás vagy az üzleti szféra számára jelenleg legnagyobb problémát jelentő, felhőbiztonsággal kapcsolatos kihívások. Mindezek mellett felhívják a figyelmet egy új támadási forma, az ún. destruction of service (DeOS) megjelenésére. Az ilyen típusú támadások általában arra irányulnak, hogy a célkeresztben lévő szervezet azon biztonsági funkcióit, amelyek a támadások utáni remediációban vennének részt (pl. biztonsági mentések) használhatatlanná tegyék, amire jó példa a közelmúltban történt 'NotPetya' támadáshullám. Az elemzők emellett aggasztónak tartják az IoT botnetek elmúlt időszakban tapasztalt magas aktivitását, amely arra is utalhat, hogy egyesek egy nagy volumenű támadást készíthetnek elő. **Bővebben...**