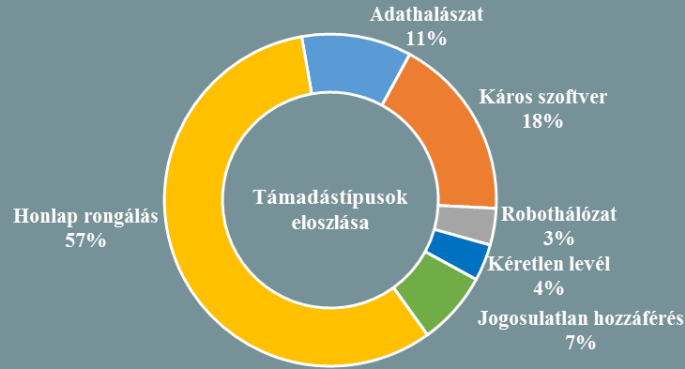


Incidens adatok:
2018.04.20. - 2018.04.26.



Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta olvashatja legújabb híreinket!

Lekapcsolták a legnagyobb DDoS bérlő szolgáltatást (www.bleepingcomputer.com)

Az Európai Rendőrségi Hivatal sikeresen elérhetetlenné tette a WebStresser-t, ahol havidíjas konstrukcióban már akár 15 euróért elosztott szolgáltatásmegtagadást okozó támadást lehetett vásárolni. A 2015 óta működő weboldalnak a lekapcsoláskor több, mint 136 000 regisztrált felhasználója volt, ezzel a legnagyobb ilyen jellegű site-nak számított és az elmúlt évek során mintegy 4 millió támadásért volt felelős. A készítőik nagy jelentőséget tulajdonítottak a reputációjuknak, Facebook oldalukon folyamatos kapcsolatot tartottak fenn az ügyfelekkel, akik ajánlásait havidíjas kedvezményekkel honorálták. Kényelmi szolgáltatásként elérhetővé tettek egy mobil applikációt, amelyen keresztül a kliens távolról is támadást indíthatott, emellett rendszeresen tájékoztatták az ügyfeleket a tervezett leállításokról és karbantartásokról. Az oldal népszerűségére jellemző, hogy a Google első találatként jelenítette meg a „DDoS booter” és „DDoS stresser” kulcsszavakra. A hivatalos közlemény szerint a Hollandiában, az Egyesült Államokban és Németországban található gépi infrastruktúra leállítása mellett az oldal adminisztrátorait is letartóztatták, illetve a hatóságok a legtöbb támadást indított felhasználók ellen is intézkedtek. **Bővebben...**

Komoly adatvédelmi aggályok a Google-nél (www.bleepingcomputer.com)

A Google új „Chat” nevű üzenetküldő szolgáltatásáról Joe Westby, az Amnesty International Technology and Human Rights kutatója fogalmazott meg éles kritikát, miszerint a Google „teljes mértékben háttér fordít az ügyfelek privát szférájának védelmének”. A legtöbb üzenetküldő alkalmazással ellentétben ugyanis – amelyek a végponttól végpontig terjedő titkosítással garantálják a felhasználók kommunikációjának bizalmasságát – a Chat-en történő üzenetváltás nem titkosított csatornán zajlik, amit a Google szóvivője is megerősített. Mindemellett nem ez az egyetlen Google termék, aminek adatkezelésével kapcsolatban az utóbbi időben kérdések merültek fel, a Google Assistant részeként működő „Android Auto” alkalmazás például bizonyítottan információt gyűjt a jármű működéséről (sebesség, a hűtőfolyadék, motor és olaj hőmérséklete, a motor fordulatszám, stb.), amelyeket valós időben továbbít a cégnek. **Bővebben...**

Hatékony segítséget kapnak a hatóságok az online zaklatók felderítéséhez (www.bleepingcomputer.com)

Amerikai kutatók kidolgoztak egy új algoritmust, amely képes felismerni a szexuális ragadozókat az online csevegő felületeken – írja a Bleeping Computer. Várhatóan az év végére el is készülhet az ezen alapuló eszköz, a Chat Analysis Triage Tool (CATT), amely támogathatja a bűnüldöző hatóságok munkáját a szexuális bűnözők utáni nyomozások során. Az algoritmus létrehozásához 107 online beszélgetésből több, mint 4 300 üzenet dolgoztak fel, melyek résztvevői elítélt zaklatók voltak. Ezek elemzését követően képesek voltak az általuk használt szavak között ismétlődéseket azonosítani, emellett olyan jellemző módszereket is feltártak, mint az „önfeltárulkozás”, melynek során az áldozat bizalmát valamilyen negatív személyes történet megosztásával igyekeznek elnyerni. Az eszköz emellett képes megbecsülni, hogy a támadó milyen valószínűséggel próbál meg fizikai kapcsolatba lépni áldozatával, valamint az általa használt nyelvezet segítségével a személy korát is képes lehet megállapítani. **Bővebben...**





Megjelent az Opera Touch

(www.techcrunch.com)

Az Opera bemutatta új mobil böngészőjét, az Opera Touch-ot Android-ra, és hamarosan az iOS-es verzió is megjelenik. Az alkalmazás az Opera asztali verziójából (Neon) kölcsönzött jó néhány ötletet, így található benne hirdetésblokkoló, valamint kriptobányászat elleni védelmi megoldásokkal is rendelkezik. Az alkalmazást úgy alakították ki, hogy a böngésző kulcsfontosságú funkciói (például a lapok közötti váltás és a könyvjelzők kezelése) legalul, a hüvelykujj segítségével érhetőek el, ezáltal egy kézzel is könnyen használható az applikáció, ami a Safari felhasználóknak ismerős lehet. Az Opera Touch emellett egy új funkciót is bevezet (Flow), amelynek segítségével az asztali és a mobil verzió között bejelentkezés nélkül, egyszerűen megoszthatók az információk, az asztali böngésző QR-kódjának leolvasásával. **Bővebben...**

IT biztonsági Tanács



A fejlett, perzisztens fenyegetések (APT) mára állandó veszélyeztető tényezővé váltak. Ezeket a szofisztikált informatikai támadásokat, **nagyon nehéz azonosítani**, a következő jelek azonban **utalhatnak ilyen tevékenységre**:

- **Célzott adathalászati e-mailek megjelenése**
- **Növekszik a munkaidőn kívüli naplóbejegyzések száma**
- **Backdoor trójai programok megszorodott száma**
- **Indokolatlan belső adatáramlások**
- **Váratlan helyeken megjelenő, nagyméretű adatfájlok**

IoT rendszerekre szabott titkosítási algoritmusok létrehozását kapacitálja a NIST

(www.infosecurity-magazine.com)

Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) felhívást intézett az IoT eszközök magasabb szintű biztosítására szolgáló, új titkosítási szabványok létrehozása érdekében, az okos eszközök biztonságával kapcsolatban ugyanis komoly korlátozást jelent, hogy a titkosítási rendszereket jellemzően a nagyobb számítási kapacitással rendelkező környezetek (asztali számítógépek, szerverek) számára tervezték. A NIST által most közzétett "Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process" című tervezetben ismertetik a kriptográfiai eljárások könnyűsúlyú változatára vonatkozó javasolt követelményeket, amellyel kapcsolatban 45 napig várják az iparági szereplők visszajelzéseit. **Bővebben...**

Trump első évében rekordszámú megfigyelési kérelmet utasított el a FISC

(www.zdnet.com)

Donald Trump amerikai elnök első hivatali évében több megfigyelési kérelem fölött gyakorolt vétót a Külföldi Felderítő és Megfigyelő Bíróság (FISC, vagy FISA Court), mint a bíróság 40 éves történetében bármikor. A FISC által nemrégiben kiadott éves jelentés szerint a bíróság 26 kérést teljes egészében, 50-et pedig részben utasított el. A bíróság megalakulása óta (1978) egészen Barack Obama elnökségének utolsó évéig (2016) összesen 21 kérelem került megtagadásra, így a visszautasítási arány – a 2017-es évet is figyelembe véve – immár 0.11%-ossá vált. A tavalyi évben 1 614 db, többnyire telefon és e-mail lehallgatásra vonatkozó kérelmet nyújtott be az NSA és az FBI, amiből 1 147 kérelem azonnal, 39 pedig azok módosításával került elfogadásra. **Bővebben...**

Kiberháborús stratégiát fogalmaztak meg az USA-ban

(www.cyberscoop.com)

Az Egyesült Államok elnöke kiberháborús stratégiát terjesztett az amerikai Kongresszus elé, mivel a 2018-as National Defense Authorization Act (NDAA) értelmében választ kell adnia arra vonatkozóan, hogy kormánya miképpen tervezi kezelni a kritikus infrastruktúrákat érő támadásokat, beleértve azt is, hogy ez esetben milyen offenzív intézkedéseket foganatosítana. A tervezet részleteit nem hozták nyilvánosságra. Eközben a Belbiztonsági Minisztérium (DHS) saját keretrendszert készít a kritikus hálózatok védelméhez, ami a tervek szerint egyaránt segítséget nyújt a szövetségi, állami, illetve a lokális szintű kormányzati szervezeteknek és a rendszerek üzemeltetőinek. **Bővebben...**

Új taggal bővült a NATO kibervédelmi központja

(www.ccdcoe.org)

Merle Maigre, a CCDCOE igazgatója üdvözölte Portugáliát, mint a NATO Kibervédelmi Kiválósági Központ (CCDCOE) új tagját. Az észtországi Tallinban található, 2008-ban alapított nemzetközi katonai szervezet feladata a NATO tagországok kibervédelmi képességeinek fejlesztése, kutatások, tréningek és gyakorlatok lebonyolításán keresztül. A központ szervezi többek között a világ legnagyobb szabású és legkomplexebb kibergyakorlatát, a Locked Shields-et, valamint a minden tavasszal – idén május 30 és június 1 között – megrendezésre kerülő CyCon konferenciát is, amelyen a globális kibervédelmi közösség kulcsszereplői, szakértők és döntéshozók találkozhatnak. **Bővebben...**