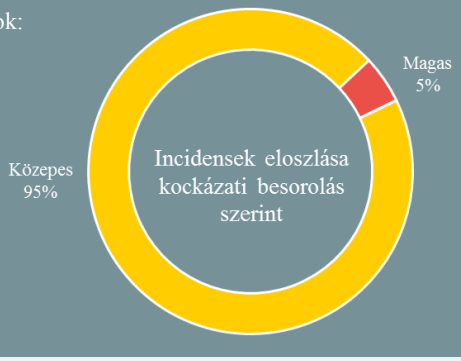
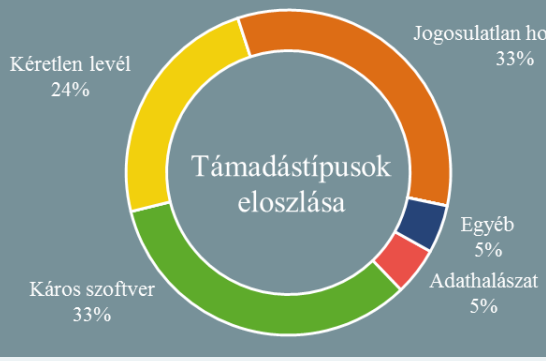
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 15. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.04.05. - 2019.04.11.





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

Lezajlott az EU-s választási kibergyakorlat

(enisa.europa.eu)

Múlt hét pénteken került megrendezésre az EU-s szervek, valamint az uniós tagállamok által közösen szervezett EU ELEx19, az Európai Parlamenti választások folyamatainak kiberbiztonsági ellenálló képességét felmérő döntéshozatali gyakorlat (Tabletop Excercise). Az esemény célja az volt, hogy átfogó képet adjon a tagállamok incidenskezelési gyakorlatainak, válságkezelési terveinek és képességeinek hatékonyságáról egy esetleges kiberbiztonsági incidens bekövetkezése esetén. Mindez a potenciális gyengeségek azonosítása mellett lehetőséget nyújtott a releváns szervek közötti nemzeti szintű, valamint határokon átívelő együttműködés javítására is.
(Szerk.: Az EU ELEx19 gyakorlat során Magyarország képviseletét a Nemzeti Választási Iroda, a Miniszterelnöki Kabinetiroda, valamint a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet látta el.)

Újabb információkra derült fény a hírhedt Stuxnetről

(securityweek.com)

A Stuxnetet a világ első ─ felfedezett ─ katonai célú kiberfegyvereként tarják számon. A káros kódot, amelyet vélhetően az Egyesült Államok és Izrael vetett be egy iráni urándúsító üzem ellen, az eddigi kutatások már három másik kiberfenyegetéssel is összefüggésbe hozták (a Duqu és a Flame nevű, valamint az NSA-féle Equation Group kártékony szoftvereivel). A Chronicle legfrissebb elemzése szerint azonban a Stuxnet egy moduljának ─ a vezérlőszerverekkel való kapcsolattartást időzítő Stuxshop ─ fejlesztésében a Flowershop nevű, 2002 és 2013 között aktív malware-t készítő kollektíva is részt vett. **Bővebben...**

Újabb Triton támadást azonosított a FireEye

(motherboard.vice.com)

A FireEye nyilvánosságra hozta, hogy Triton (más néven TriSIS) támadást észleltek egy eddig meg nem nevezett kritikus infrastruktúra ellen. Említett támadási formát a szakértők rendkívül veszélyesnek tartják, mivel céljuk a fizikai károkozás olyan rendszereken, amelyek meghibásodása emberéletek veszélyeztethet. 2017 nyarán ezt a malware-t vetették be a szaúdi Petro Rabigh olajvállalat ellen, amelynek során a támadók kifejezetten a létesítmény katasztrófa állapotok megelőzésére, elkerülésére szolgáló biztonsági rendszereit (Safety Instrumented System ─ SIS) támadták. **Bővebben...**

Hiába a patch, egyes MikroTik routerek továbbra is veszélyben lehetnek

(securityaffairs.co)

A MikroTik biztonsági frissítéseket adott ki a hálózati eszközein futó RouterOS firmware-hez. Ezek olyan, az IPv6 csomagok nem megfelelő kezeléséből fakadó sérülékenységeket javítanak, amelyek távoli kihasználásával kikényszeríthető az eszközök újraindulása (CVE-2018-19298), valamint RAM-kezelési problémák miatt azok túlterhelése (CVE -2018-19299). Úgy tűnik azonban, hogy a javítások ez utóbbi kapcsán nem minden MikroTik router számára nyújtanak védelmet, Marek Isalski biztonsági kutató ugyanis egy 64 MB RAM-mal rendelkező routeren tesztelve úgy találta, hogy a patch hatástalan. Isalski egyike volt azon kutatóknak, akik 2018 áprilisában elsőként jelentették a hibákat, emellett aktív támadásokról is közölt információkat. Javier Prieto MikroTik oktató szintén vizsgálódott az ügyben, ő úgy találta, hogy a rendszer egy névlegesen 256 MB RAM-mal rendelkező router esetében körülbelül 180 MiB-nyi (kb. 188 MB) memória „lopást” képes tolerálni, 200 MB esetén azonban az eszköz már újraindul. **Bővebben...**

A Google biztonsági kulccsá alakítja az Androidos telefonokat

(techcrunch.com)

A Google idei Cloud Next konferenciáján jelentette be, hogy kidolgozott egy Bluetooth-alapú protokollt, amely lehetővé teszi, hogy a korábbról ismert Bluetooth-os hardverkulcsok helyett a felhasználók androidos mobileszközüket használják a kétfaktoros azonosítás második lépcsőjeként. Manapság közkeletű, hogy a többfaktoros autentikáció az egyik legjobb módja online fiókjaink biztosításának, hiszen az már a technológiából adódóan is hatékony védelmet jelent az adathalász támadásokkal szemben. Mindez a legtöbbször egy, a hálózaton haladó üzenet formájában történik, amelynél azonban mindig fennáll az esélye annak, hogy illetéktelenek megszerzik az azonosításra szolgáló kódot. **Bővebben**

IT biztonsági Tanács

A Bitcoin Abuse Database olyan Bitcoin címeket tartalmaz, amelyeket rosszindulatú hackerek és számítógépes bűnözők használnak fel káros, zsaroló műveleteik során. Jó példa erre az évek óta jelenlévő ransomware-ek, vagy az utóbbi időben egyre gyakoribb, ún. „Sextortion" zsarolólevelek, amelyek a felhasználókról készült pikáns képanyagok közzétételével fenyegetik az áldozatokat. A bitcoinabuse.com célja, hogy nyilvánosan dokumentálja a bűnözéshez köthető bitcoin címeket, ami az oldal készítőinek reményei szerint a jövőben megnehezíti majd a támadók dolgát a kizsarolt összegek felhasználásakor.

Kibertámadás okozta a HOYA 3 napos leállását

(bleepingcomputer.com)

Február végén kibertámadás érte a japán HOYA vállalat thaiföldi üzemét, amely három napig részleges leállásokat okozott a gyártósoron. A vállalat közleménye szerint körülbelül 100 munkaállomás fertőződött meg hitelesítő adatokat gyűjtő káros kóddal, valamint a támadás második fázisában kriptobányász malware-rel. Helyi hírforrások szerint – a szokatlanul magas erőforrás-felhasználás miatt – utóbbi vezetett a támadás felfedezéséhez. Habár az üzletmenetre összességében alacsony befolyással bírt a támadás, és adatszivárgás sem történt, a termelésben keletkezett csúszás következményeivel a vállalat a mai napig küzd. **Bővebben...**

Visszafejthetők a „Planetary" zsarolóvírus által titkosított fájlok

(bleepingcomputer.com)

Az Emsisoft újabb dekriptor eszközt tett ingyenesen elérhetővé, ezúttal a „Planetary" zsarolóvírus család által titkosított fájlok váltak visszafejthetővé. A szóban forgó ransomware onnan ismert, hogy a titkosított fájlok kiterjesztéseként bolygó neveket alkalmaz, mint például a .Pluto vagy a .Neptune, de legutóbb például egy videojátékban szereplő fiktív bolygó nevét használták (.mira). A fájlok visszafejtéséhez szükség van a zsarolóvírus által létrehozott váltságdíj felszólítást tartalmazó üzenetre (ransom note), amely egy „!!!READ_IT!!!.txt" nevű fájl, és minden olyan könyvtárban megtalálható, amelyben a vírus fájlokat titkosított. A dekriptor és a hozzá tartozó felhasználói útmutató az Emsisoft weboldaláról ingyenesen beszerezhető.

Ausztria: Csak a „digitális álruhatiltás" segíthet

(heise.de)

Bécs elő kívánja írni, hogy csak egy mobiltelefonszám megadásával lehessen az interneten posztolni. Az intézkedés célja, hogy az írás készítője egyértelműen beazonosítható legyen. Az osztrák kormányzat egyértelműen eltökélt, hogy a közösségi oldalakon publikáló személyek a telefonszámuk révén identifikálhatóak legyenek, visszaszorítva ezzel az álnéven posztolás egyre növekvő jelenségét. Ennek érdekében már el is készült a vonatkozó törvénytervezet, ahogyan erről már az ottani sajtóorgánumok is beszámoltak. A hírek szerint nemcsak a legnagyobb közösségi oldalak lesznek ezen intézkedéssel érintve, hanem az egyes újságok fórumai is. Becslések szerint, a szóban forgó tervezet hatálybalépése a lapok közül legélesebben a Standard újságot érintené, amelyhez naponta esetenként 40 000 internetes kommentár is beérkezik.

Veszélyes megtévesztő technikát alkalmaz az új Emotet spam kampány

(zdnet.com)

Az Emotet az egyik legnagyobb botnet jelenleg, jelentőségére jellemző, hogy nagyobb kiberbiztonsági cégek (CrowdStrike, FireEye, Kryptos Logic, McAfee, IBM, Cybereason) elemzései alapján nagy szerepe van a Ryuk, a LockerGoga, valamint a BitPaymer zsarolóvírusok elterjedésében is. A Cofense szerint a botnetet működtető kollektíva most új taktikát kezdett alkalmazni: egy korábbi, alapozó kampány során begyűjtött valós e-mail üzenetekre válaszolva küldenek káros hivatkozást az áldozatnak. Ez a technika ─ amelyet a Palo Alto Networks Észak-Koreához köt ─ nagyon megtévesztő, hiszen a felhasználó azt tapasztalja, hogy egy legitim e-mail beszélgetésben érkezik új üzenet. Az Emotet botnet spamelő hálózata ─ a lekapcsolás megnehezítésére ─ két fő klaszterből áll (E1, E2) és jelenleg mindkettő az új kampánnyal van elfoglalva. **Bővebben...**