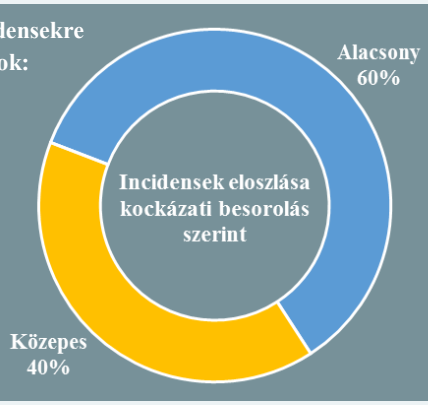
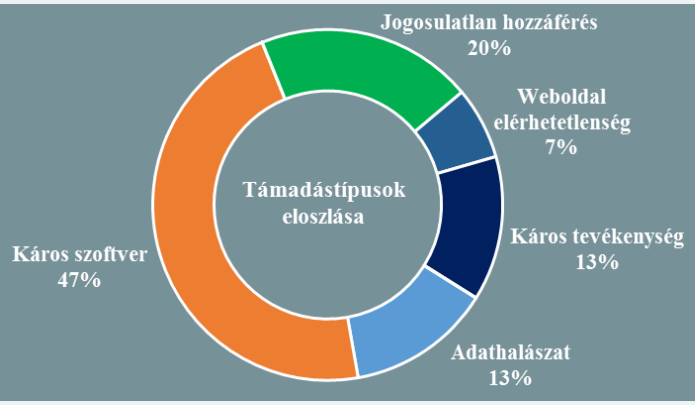
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.11.01. - 2018.11.08.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

A Stuxnethez hasonló támadás történt Irán ellen

(securityaffairs.co)

Az iráni Hadashot TV hírműsorban elhangzottak szerint a Stuxnet egy új, pusztító variánsa támadta meg az ország egy stratégiai fontosságú hálózatát. A nevezett vírus eredeti verzióját 2010-ben iráni nukleáris létesítmények ellen vetették be, amely ─ a széles körben elfogadott nézet szerint ─ az Egyesült Államok, az izraeli hírszerzés, valamint a GCHQ brit titkosszolgálat együttműködése révén készült. A mostani malware támadásról bővebb információkat mindeddig nem hoztak nyilvánosságra, csupán annyit, hogy ez a korábbinál is „erőszakosabb" és „kifinomultabb", a hátterében pedig ismét Izraelt sejtik, akik a publikáció elkészültéig nem reagáltak a vádra. A Security Affairs megemlíti, hogy az utóbbi hónapok során a Mossad állítólag több műveletet is folytatott Irán ellen, amelyek során dokumentumokat szereztek meg Irán titkos nukleáris programjáról. Ayatollah Ali Khamenei iráni vezető az eset kapcsán cselekvésre szólította fel a kibervédelem terén (is) posztot gyakorló védelmi tisztviselőket.

Francia nukleáris létesítményekről loptak adatokat

(securityaffairs.co)

Német és francia hírforrások szerint több, mint 65 GB-nyi dokumentumot tulajdonítottak el egy számítógépes támadás során, amelyek többek között atomerőművekre és börtönökre vonatkozó érzékeny információkat is tartalmaztak. A támadás valamikor 2018 júniusában történt és az Ingerop vállalatot érte. Az eltulajdonított dokumentumok egy része Franciaország legrégebbi ─ azonban a tervek szerint még 2022-ig üzemelő ─ atomerőművéről tartalmaz részletes adatokat, emellett börtön alaprajzok és kamera pozíciók, valamint egy nukleáris szemétlerakó tervezete is megtalálható közöttük, mindezek pedig számtalanféle visszaélésre adhatnak módot.

Újabb adatszivárgás történt a Facebooknál?

(www.infosecurity-magazine.com)

Kártékony böngésző kiegészítők útján férhettek hozzá mintegy 81 000 Facebook fiókhoz, amelyek adatait ─ köztük privát üzenetekkel ─ nemrég a Darkneten árulták, további 176 000 profiléval egyetemben, amelyek valószínűleg nem kompromittált, csupán a nem megfelelő biztonsági beállítások miatt nyilvánosan hozzáférhető információkat tartalmaznak. A támadók a BBC Russian Service-nek ugyanakkor azt nyilatkozták, hogy ennél is több ─ 120 millió ─ fiókhoz fértek hozzá, azonban ez a Digital Shadows digitális kockázatelemző cég szerint valószínűtlen. **Bővebben...**

Az Oracle szerint valóban történt internetes forgalom elterelés Kína részéről

(www.zdnet.com)

Az Oracle internetes forgalom-elemző divíziója (Internet Intelligence) megerősítette az amerikai Haditengerészeti Főiskola és a Tel Aviv Egyetem kutatói által nemrég publikált tanulmány megállapításait, miszerint a China Telecom ─ Kína egyik legnagyobb, állami kézben lévő internet szolgáltatója ─ valóban térített el internetes adatforgalmat az utóbbi években, ugyanakkor Doug Madory, a részleg vezetője nem foglalt állást a tanulmány azon részeivel kapcsolatban, amelyek az eltérítés motivációival foglalkoznak. A felfedett részletek szerint az érintett nemzetközi forgalom nagy része az Egyesült Államok belföldi forgalma volt, ami a BGP routolási protokoll sérülékenységeinek kihasználásával egy kitérő során előbb a kínai szolgáltató rendszerén haladt át. Madory szerint a jövőbeli hasonló esetek elkerüléséhez az internetszolgáltatóknak minél előbb el kell kezdeniük a magasabb biztonsági szintű megoldások alkalmazását, mint például az RPKI.

Az újabb Android verziók kevésbé érintettek káros kód fertőzésben

(zdnet.com)

A Google első ízben közöl az Android biztonságára vonatkozó statisztikai adatokat, miután az utóbbi években többször állította, hogy lényegesen javított a rendszer biztonságán. Az átláthatósági jelentés szerint a legalább egy potenciálisan káros alkalmazást (PHA) tartalmazó eszközök aránya a régebbi Android verziókat futtató eszközök esetében 0.5% felett van, a 6-os verzió (Marshmallow) felett azonban ez lényegesen alacsonyabb: a Nougatnál (7.x) 0.25%, az Oreo (8.x) és a Pie (9.x) tekintetében pedig 0.14%. Az Android biztonsági csapata szerint mindez többek között a folyamatos biztonsági fejlesztéseknek és frissítéseknek köszönhető, valamint annak, hogy az alkalmazás fejlesztőket igyekeznek rábírni azon gyakorlat követésére, hogy az applikációk csak a lehető legkevesebb érzékeny adathoz férjenek hozzá. **Bővebben...**

IT biztonsági Tanács

Az amerikai NCCIC **tájékoztató elemzést** adott ki a JexBoss nyílt forrású eszközről, amelyet biztonsági szakemberek ─ például auditok, sérülékenység vizsgálatok során történő használata ─ mellett a kiberbűnözők is alkalmaznak a JBoss alkalmazásszerver sérülékenységének felderítésére. A Cisco Talos szerint például a 2016-os SamSam ransomware kampány során a támadók ezzel nyertek kezdeti hozzáférést a megcélzott infrastruktúrákon. A riport részletesen bemutatja az eszköz működését és a lehetséges felhasználási módjait, valamint védekezési javaslatokkal is szolgál.

Átfogó DDoS támadás érte Kambodzsa internetszolgáltatóit

(www.zdnet.com)

Kambodzsa legnagyobb internet szolgáltatóit az utóbbi néhány nap során elosztott szolgáltatásmegtagadással járó támadások érték, emiatt egyes helyi szolgáltatók ─ mint például az EZECOM, a SINET, a Telcotech, valamint a Digi ─ ügyfelei a hét során szinte folyamatosan problémákat tapasztaltak az online szolgáltatások elérésében. Helyi hírportálok szerint ez az országot ért egyik legnagyobb ilyen jellegű támadás sorozat, amelynek volumene hétfőn a 150 Gbps sávszélességet is elérte. Mindeddig nincs információ arra vonatkozóan, hogy az eseményért kit tennének felelőssé, az országban jelenleg nincsenek zavargások, zsarolási kísérletről pedig nem számoltak be az érintett vállalatok.

Egy nyílt forrású szoftverrel meghatározható az internetre kötött sérülékeny IP kamerák valós helyzete

(motherboard.vice.com)

A Kamerka nevű tool segítségével cím alapján kereshetőek a közeli, internet felől hozzáférhető kamerák. Készítője szerint az alkalmazás több különálló programból tevődik össze: az egyik a Shodan, ami az internetre kötött eszközök felderítéséért felel, a Geopy modul a helymeghatározást, a Folium pedig az eredményeket tartalmazó, HTML alapú térkép előállítását végzi. A Motherboard validálta a program működését, aminek a segítségével London, New York és Párizs területén is tártak fel nem biztosított kamerákat. Bár a teszt során olyan eszközt nem találtak, ami élő képet közvetített volna ─ valamint a legtöbbjük nem bizonyult autentikáció nélkül hozzáférhetőnek ─ több esetben is elértek olyan admin felületeket, amelyekről ismert, hogy könnyen kitalálható jelszavakkal rendelkeznek.

Több, mint félmillió embert érinthet a Bankers Life adatszivárgása

(tripwire.com)

Komoly adatszivárgási incidens történt az egyesült államokbeli Bankers Life egészségügyi biztosító cégnél, amelynek során mintegy 566 217 ügyfelük személyes azonosításra alkalmas információi kompromittálódhattak. A cég közleménye szerint ismeretlen támadók hozzáférést szereztek a vállalat egyes dolgozóinak hitelesítési adataihoz, amelyek segítségével 2018. május 30. és szeptember 13. között hozzájuthattak a biztosítottak személyes adataihoz. A biztonsági esemény kivizsgálása során megállapításra került, hogy az érintett ügyfelek neve, születési ideje, biztosítási információi és a személyi azonosítójuk (Social Security Number) utolsó 4 számjegye vált elérhetővé a támadók számára, azonban egyes esetekben a teljes azonosító, valamint banki információk is kompromittálódhattak. Arról nem közöltek információkat, hogy a támadók hogyan vették birtokba a felhasznált hitelesítő adatokat.

Az Egyesült Államok kiberparancsnoksága vírusmintákat tesz közzé a VirusTotalon

(www.scmagazineuk.com)

A 2012 óta az Alphabet tulajdonában lévő VirusTotal rendelkezik az egyik legnagyobb online malware minta adatbázissal, amely a jövőben az amerikai kiberparancsnokság alá tartozó Cyber National Mission Force (CNMF) alegység által feltöltött, nem minősített vírusmintákat is tartalmaz majd. A bejelentést ugyanakkor kritikák is övezik, mivel a minták letöltése a VirusTotalon csak fizetős szolgáltatásként érhető el.