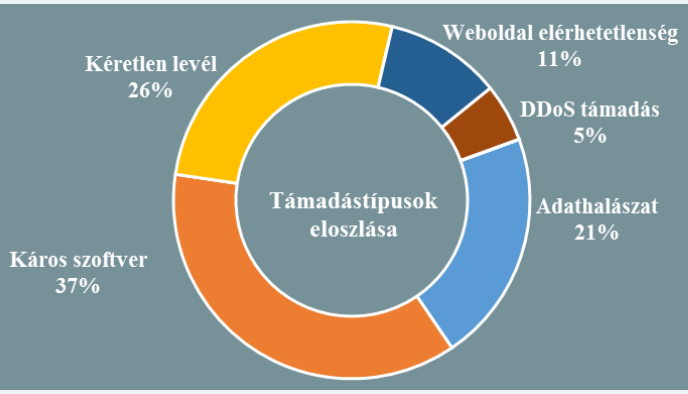
Incidens adatok:
2018.03.09. - 2018.03.15.



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

Lehetséges, hogy a britek kibertámadást indítanak Oroszország ellen

(www.dailymail.co.uk)

Theresa May brit miniszterelnök a múlt héten történt idegméreg támadásra reagálva Oroszországgal szembeni szankciók meghozását tervezi, melyről az Egyesült Királyság a NATO-val, EU-val, az Egyesült Államokkal, valamint az ENSZ-szel történő közös egyeztetést követően hoz végleges döntést. A hírek szerint egyes diplomaták kiutasítása mellett az intézkedési csomag részét képezhetik majd az orosz propaganda terjesztéséhez használt hálózatok elleni informatikai támadások is. May egy múlt heti interjúban elmondta, két lehetőséget lát az orosz dezinformációs tevékenységre való reagálásra: a saját narratíva terjesztését, vagy kibertámadás indítását. Sir Chris Deverell tábornok, az Összhaderőnemi Parancsnokság (Joint Forces Command) parancsnoka korábban már felfedte, hogy az Egyesült Királyságban létezik olyan – a Védelmi Minisztérium és a GCHQ hírszerző ügynökség által működtetett – speciális egység, amit kifejezetten támadó jellegű kibertevékenység miatt hoztak létre. A kiberfegyverek bevetésével kapcsolatban azonban elhangzott az is, hogy az csak jól behatárolt körülmények és a törvényesség figyelembevételével lehetséges. **Bővebben...**

Átfogó kiberhadművelet alatt lehet az Egyesült Királyság

(www.securityaffairs.co)

A múlt héten Ahmed Zaki, az NCC Group biztonsági kutatója egy szofisztikált malware támadásról tartott előadást a Kaspersky's Security Analyst Summit (SAS) rendezvényen. Az NCC tavaly májusban értesült róla, hogy egy, a brit kormányzati szektor számára szolgáltatásokat nyújtó szervezet rendszere kompromittálódott, melynek kapcsán azonnal hozzákezdtek a vizsgálatokhoz. Ezek során megállapították, hogy a támadók sikeresen hozzáférést szereztek a szervezet VPN hálózatához, egy lopott tanúsítvány segítségével. Az alkalmazott kártékony kódok alapján úgy vélik, az elkövető az a – széles körben elfogadott nézet szerint kínai kötődésű – APT15 csoport volt, mely tevékenységéről ismert, hogy legkésőbb 2010 óta folytat aktív és kiterjedt kiberkémkedést világszerte. A kutatók szerint a tárgyalt támadás nem egy elszigetelt eset volt, hanem minden valószínűség szerint egy nagyszabású művelet része lehet, amely brit kormányzati és katonai célpontok ellen zajlik. **Bővebben...**

Fizikailag elkülönített rendszerek között is lehetséges adatot mozgatni

(www.thehackernews.com)

Kutatók, akik a múlt hónap során demonstrálták, hogy lehetséges adatot lopni még a fizikailag izolált, Faraday-kalitkában lévő számítógépekről is, most azt bizonyították be, hogy két, azonos szobában lévő, de fizikailag teljesen elkülönített számítógép képes lehet adatot cserélni ultrahangokon keresztül. A kutatás azért számít különösen érdekesnek, mert az internettől és a lokális hálózattól légréssel izolált rendszerek számítanak a legbiztonságosabbnak jelenleg, mivel közöttük csupán valamilyen fizikai adathordozó segítségével (pl.: USB drive) valósulhat meg adatmozgatás. A „MOSQUITO"-nak elnevezett technika során a csatlakoztatott hangszórókat (passzív hangszórók, fülhallgatók, stb.) alakítják át kvázi-mikrofonná az audio chipek egy specifikus funkciójának felhasználásával. A közel ultrahangon (18-24kHz) kibocsátott jeleket 3 méter távolságból voltak képesek célba juttatni, azonban nagyobb teljesítményű audio eszközök segítségével akár 8 méterre is növelhető a távolság és 10-166 bit/mp sebesség is elérhető. **Bővebben...**

Szándékosan tiltották ki az iráni felhasználókat az App Store-ból?

(www.bleepingcomputer.com)

2018. március 15-én Iránban elérhetetlenné vált az Apple App Store, ily módon megszűnt az applikációk letöltésének a lehetősége, beleértve a frissítések telepítését is. Meysam Firouzi, egy iráni biztonsági kutató a Bleeping Computer-nek elmondta, a tiltás minden bizonnyal IP-szűréssel valósult meg, mivel VPN használatával képes volt hozzáférni az alkalmazásbolthoz. Az online magazin az üggyel kapcsolatban megkereste az Apple-t, ám a publikáció elkészültéig nem érkezett válasz, így nem tudni pontosan, hogy mi állhat a döntés hátterében. Nem minden előzmény nélküli az eset, ugyanis 2017 augusztusában a tech óriás törölte az összes, iráni fejlesztők által készített appot, az USA gazdasági szankcióira hivatkozva. Egy, a NY Daily News-ban, március elején publikált cikk szerint azonban az iráni hírszerzés mind a Google Play-en, mint az App Store-on káros kóddal fertőzött alkalmazásokat helyezett el, amelyeket megfigyelésre, valamint malware támadásokhoz használtak. **Bővebben...**

IT biztonsági Tanács

Amennyiben nem hivatalos viszonteladótól készülünk okostelefont vásárolni, érdemes a vásárlás előtt elkérni a termék IMEI vagy sorozatszámát, melyet a választott márka hivatalos ügyfélszolgálatának bediktálva információt kaphatunk az adott készülékről.

Ezzel elkerülhetjük olyan eszközök vásárlását, melyeknek nem minden szolgáltatása (biztonsági frissítés, mobilnet, stb.) érhető el az adott országban, mivel előfordulhat, hogy azokat más régióba szánták.

Szabadon tesztelhető egy litván mobil hálózat kibertámadásokkal szembeni ellenálló képessége

(www.csoonline.com)

Litvánia legnagyobb mobil szolgáltatója, a Latvijas Mobilais Telefons (LMT) nyilvános felhívásában arra bátorítja a kiberfegyverrel rendelkezőket, hogy indítsanak hálózati támadást a rendszereik, egészen pontosan annak egy virtualizált változata ellen. A Mobile Cyber Range elnevezésű virtuális gyakorlóteret már a NATO is használta kibergyakorlat során, most a mobil hálózatok védelmének tesztelése a cél. Az LMT a teljes mobil infrastruktúrát képes szimulálni a SIM kártyáig bezárólag, így a támadások pontosan olyan körülmények között tesztelhetők, mint a valóságban, anélkül, hogy azok bármiféle káros hatást gyakorolnának az előfizetőkre. **Bővebben...**.

Az EU is egyre jobban fókuszál a mesterséges intelligenciára

(www.europa.eu)

Múlt péntek óta van lehetőség az Európai Bizottság által felállított új szakértői csoporthoz való csatlakozáshoz, melynek a mesterséges intelligencia hatékony és etikus módon történő felhasználására kell majd ajánlásokat kidolgoznia. Ennek értelmében például javaslatokkal kell szolgálnia a Bizottság részére az "Európai MI Szövetség" létrehozásához, és az év végéig be kell nyújtania az MI etikus fejlesztésére és felhasználására vonatkozó iránymutatások, az Alapjogi Chartára alapozott tervezetét. A szakértői munkához kiinduló pontként korábbi, a témakör szempontjából releváns kutatásokat tekintenek, mint például az ipari technológiákról készült jelentés. A jelentkezési határidő 2018. április 9-ig tart, ugyanis a Bizottság már májusban működtetni szeretné a szakértői csoportot. **Bővebben...**

Wildcard tanúsítvány támogatást kapott az ACME protokoll

(www.community.letsencrypt.org)

Az Internet Security Research Group (ISRG) bejelentette, hogy elérhetővé vált az automatizált tanúsítvány kibocsátást megvalósító ACME protokoll kettes verziója, ami már képes a wildcard SSL tanúsítványok kezelésére, azaz támogatja az egy adott domain alatti összes aldomain egyetlen tanúsítvánnyal történő hitelesítését. A wildcard tanúsítványok kizárólag az új verzióval érhetők el, az igényléshez pedig a használt kliens szoftver frissítése szükséges. Az ISRG közleményében jelezte, hogy szándékukban áll minden ügyfelet az új verzió alkalmazására bírni, ezzel együtt alapesetben a hagyományos, nem wildcard tanúsítványok használatát javasolják. **Bővebben...**

Nem nyújt megfelelő védelmet a Firefox mesterjelszava

(www.bleepingcomputer.com)

A Firefox és a Thunderbird szoftverek már kilenc éve lehetőséget biztosítanak egy titkosítási kulcs (ún. „mesterjelszó") beállítására, amivel minden a böngészőben, vagy a levelező kliensben tárolt jelszó titkosítható. Bevezetésekor a biztonsági kutatók üdvözölték a funkciót, hiszen a korábbi metódushoz – a pusztán szabadszövegként tárolt jelszavakhoz – képest ez jelentős előrelépést jelentett. Wladimir Palant, egy népszerű böngésző kiegészítő (AdBlock Plus) fejlesztője mindazonáltal felfedezte, hogy a mesterjelszó titkosításához olyan algoritmust (SHA-1) alkalmaznak, ami nem biztosít kellő védelmet a próbálgatáson alapuló (brute force) jelszótörő támadásokkal szemben. **Bővebben...**