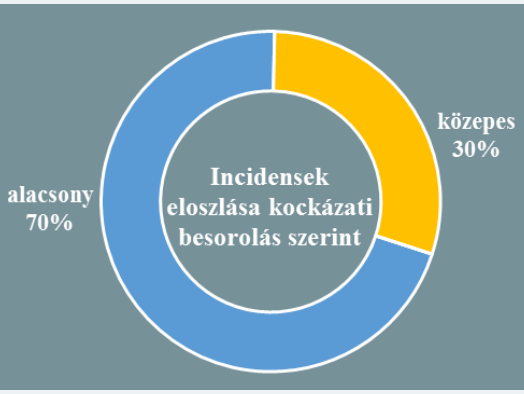
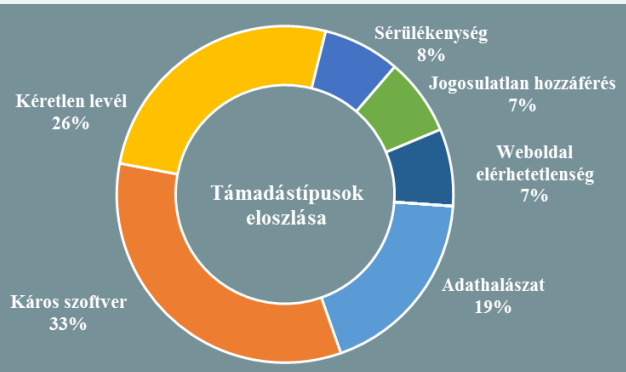
Incidens adatok:
2018.02.23. - 2018.03.01.





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

Legitim tanúsítványokat használnak malware támadásokhoz

(www.helpnetsecurity.com)

A támadók széles körben alkalmazzák a káros kódok digitális tanúsítványokkal történő hitelesítését, ami megnehezíti a vírusirtó szoftverek számára a detektálást és használatuk hozzájárulhat az operációs rendszerek és a hálózati eszközök védelmi funkcióinak megkerüléséhez. A Recorded Future kutatói felfedezték, hogy bár a kiberbűnözők jellemzően még mindig inkább a lopott tanúsítványokat részesítik előnyben, az utóbbi években néhány feketepiaci szereplő már legitim módon kiállított alkalmazás aláíró tanúsítványokat hirdet, valamint domain név regisztráció mellé SSL tanúsítványt is kínál. Az egyik első ilyen szolgáltató, a „C@T" nevű szervezet már 2015 óta végez ilyen jellegű tevékenységet, sőt reklámjukban azt is elmagyarázzák, hogy a tanúsítványokat legális tanúsító hatóságtól (Certificate Authority) – például Comodo, Thawte, Symantec – szerzik be. Ezek teljesen egyediek, csupán egy vásárló számára kerülnek kiállításra, amit akár le is ellenőrizhet az érintett. Az eljárás hatékonyságának demonstrálására a kutatók sikeresen képesek voltak egy korábban még be nem jelentett trójai programot egy valós Comodo tanúsítvány birtokában aláíratni egy CA -val, amelyet követően a VirusTotal oldalon az észlelési arány 8-ról 2-re csökkent. A vizsgálatról készített összefoglalóban azonban kiemelik, hogy a tanúsító szervezetek vélhetően nincsenek tisztában azzal, hogy az általuk kiadott tanúsítványokat káros tevékenységekhez is használják. **Bővebben...**

Törhetőek az iPhone-ok?

(www.forbes.com)

Az izraeli Cellebrite – mely egyike a piacvezető digitális forensic-szolgáltatást nyújtó vállalatoknak – a hírek szerint olyan technológiát fejlesztett ki az elmúlt fél évben, amellyel közel az összes, jelenleg a piacon lévő iPhone-hoz képes hozzáférni, beleértve az eddigi csúcsmodell iPhone X-et is. A vállalat az „Advanced Unlocking and Extraction Services" nevű szolgáltatásának részeként biztosít hozzáférést az Android mellett immár az iOS rendszerű készülékekhez is – az 5-ös verziótól a legfrissebb 11-esig bezárólag – bármely bűnüldöző hatóság vagy más jogi felhatalmazással bíró szerv számára, relatíve alacsony (1 500 dollár/eszköz) áron. Az alkalmazott eljárásról nem árultak el bővebb információt, a cég közleményében mindössze az szerepel, hogy ennek segítségével „meghatározható vagy kikapcsolható a PIN védelem, a képernyőzárolási minta vagy jelszó". A cég ügyfelei között található az amerikai kormányzat és az FBI is, utóbbival már 2013-óta szerződéses kapcsolatban állnak és a hírek szerint már igénybe is vették a szóban forgó szolgáltatást. **Bővebben...**

Illegális tartalmak elleni ajánlások

(securityaffairs.co)

Az Európai Bizottság új ajánlásokat tett közzé, melyben előírja az internetes vállalatok számára, hogy egy illegális tartalomra vonatkozó bejelentést követően egy órán belül kerüljön eltávolításra az adott tartalom, legyen az terrortámadással, erőszakos tevékenységekkel, gyűlöletbeszéddel, kiskorúak szexuális zaklatásával, hamisított termékek forgalmazásával vagy szerzői jogok megsértésével kapcsolatos. Az ajánlás elsősorban az olyan közösségi média óriások főbb szolgáltatásaira vonatkozik, melyek napi szinten kitettek a terrorizmus propaganda tevékenységének, mint például a Facebook, a Youtube és a Twitter. A médiavállalatok eddig elért eredményeinek elismerése mellett az EB egyértelművé tette, hogy készek jogszabályban rögzíteni az elvárásokat, amennyiben a vállalatok nem tesznek eleget a követelményeknek. A megfelelés biztosításához olyan automatikus detektáló rendszerek használatát javasolja a Bizottság, mely képes az illegális tartalmak azonnali azonosítására, valamint a már egyszer eltávolított tartalmak újabb feltöltési kísérleteinek megakadályozására. **Bővebben...**

Fontos biztonsági funkció a következő Android verzióban

(www.bleepingcomputer.com)

Az Android P már blokkolni fogja, hogy a háttérben futó alkalmazások hozzáférjenek a készülék kamerájához, illetve mikrofonjához. A rosszindulatú szoftverek egyes változatai (kémprogramok) ugyanis képesek arra, hogy a készülék kamerájának segítségével képeket készítsenek az áldozatok környezetéről, vagy rögzítsék az eszköz közelében zajló beszélgetéseket, melyeket továbbítanak a támadóknak. Ezeket a technikákat már 4-5 éve használják adatgyűjtésre, ezért sokak szerint meglepő, hogy az Android forráskódot gondozó szervezet (AOSP) miért csak most áll elő a védekezési megoldással. A hírek szerint a módosítást múlt hét hétfőn hagyták jóvá és már integrálták is az Android forráskódjába. A felhasználók és a fejlesztők legkorábban májusban tesztelhetik az Android P-t, melynek béta verziója nyáron válhat elérhetővé, a végleges verzió megjelenése pedig nagyjából augusztus végére, szeptember elejére várható. **Bővebben...**

IT biztonsági Tanács

Az online vásárlások során használjunk virtuális bankkártyát, melyen nem célszerű magasabb összeget tárolni, csupán ami az aktuális vásárláshoz szükséges. Ennek használatával lényegesen kissebb veszteség érheti a felhasználót, amennyiben illetéktelenek megszereznék a kártya adatait. Sok esetben ezek fizikailag sem kerülnek legyártásra, ezzel is csökkentve a visszaélés lehetőségét. A konkrét lehetőségekről érdeklődjön bankjánál.

Az eddigi legsúlyosabb túlterheléses támadás

(www.securityweek.com)

Az Akamai közleményben tudatta, hogy egyik ügyfelük 2018. február 28-án az eddigi legnagyobb mértékű elosztott szolgáltatásmegtagadásos (DDoS) támadást szenvedte el, amely volumenében mintegy duplája volt az eddigi csúcstartónak (2016 szeptember, Mirai botnet). A támadás kezdeti csúcs szakaszában 1,35 Tbs sávszélességű volt és a népszerű kódmegosztó platform, a GitHub ellen irányult, amely az események hatására körülbelül 10 percig nem, vagy csak szakaszosan volt elérhető. Az elemzések során kiderült, hogy a háttérben egyes rosszul konfigurált Memcached rendszerek kihasználása történt. Ez egy olyan nyílt forráskódú technológia, amely a webes kiszolgálók számára nyújt segítséget a memóriakezelésben, a kiszolgálás sebességét javítva. Nem megfelelő beállítások (például UDP használata) esetén azonban ezek sérülékenyek lehetnek ún. amplification támadások kivitelezésére. Ennek során a támadó az adott szerver felé olyan csomagokat küld, melyekben meghamisítja a küldő IP címet – nem sajátját, hanem az áldozatét tünteti fel – így a válaszok már efelé kerülnek elküldésre. A problémát az okozza, hogy a kezdeti kérés hiába volt csupán néhány bájtnyi, a szerver válasza több ezerszer (akár 51 200-szor) nagyobb méretű is lehet. **Bővebben...**

A titkosító kulcsokat is Kínába viszi az Apple

(securityaffairs.co)

Az Apple bejelentette, hogy a kínai iCloud felhasználók adatai mellett az azokhoz hozzáférést biztosító kulcsok is áthelyezésre kerülnek az Egyesült Államokból Kínába. A lépés a nemrég bevezetett kínai jogszabálynak való megfelelés érdekében született, melynek értelmében a kínai állampolgárok iCloud-os adatainak védelmét az ország határain belül kell megvalósítani, ugyanakkor azokhoz kínai szervezetek részére hozzáférést is kell biztosítani, így a jövőben a kínai hatóságoknak már nem kell az amerikai szervekhez fordulniuk az adatigénylésekkel kapcsolatban. A tech óriás a tervek szerint jövő hónap végén kezdi meg az ügyfelek enkriptált adatainak migrálását a kínai adatközpontba, a kulcsok áthelyezésének pontos idejéről azonban még nem közöltek információt. Az Apple a témával kapcsolatban igyekszik hangsúlyozni, hogy a kulcsokat biztonságos módon fogják tárolni, azokhoz csak a cég munkatársai férhetnek hozzá és kizárólag a hatályos kínai jogszabályi előírásoknak megfelelően szolgáltatnak majd adatot, a jogi kereteken túllépő „kiskapu” lehetőségét határozottan cáfolják. **Bővebben...**

Az amerikai határőrség nem ellenőrzi megfelelően az e-útleveleket

(www.bleepingcomputer.com)

Az Egyesült Államok – habár kifejezetten szigorú határátlépési szabályokkal rendelkezik – nem ellenőrzi az e-útlevelekben található digitális aláírások érvényességét, mivel az Egyesült Államok Vámügyi és Határvédelmi Hivatala (CBP) nem rendelkezik az ehhez szükséges szoftverrel. Az e-útlevél kiváltása 2007 óta minden olyan külföldi állampolgár számára kötelező, aki a vízummentességi programban résztvevő országok valamelyikéből érkezik az Államokba. Az e-útlevélbe integrált chip több adat mellett egy digitális aláírást is tartalmaz, amely a kártya birtokosának azonosítására szolgál és nem hamisítható, mivel azt kizárólag a hatóságok képesek módosítani. Ron Wyden és Claire McCaskill szenátorok a CBP-nek címzett nyílt leveléből azonban az derül ki, hogy a határőrség munkatársai csak a chip-en tárolt adatok egy részét képesek ellenőrizni, a digitális aláírást azonban egy dedikált szoftver hiánya miatt nem. **Bővebben...**

NEMZETI KIBERVÉDELMI INTÉZET GOVCERT