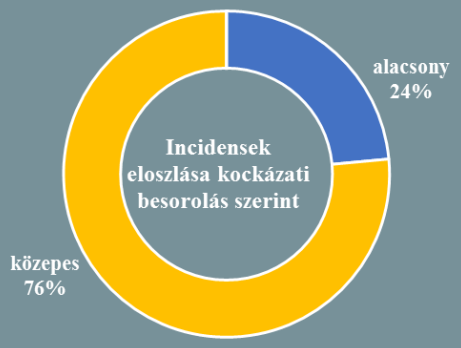
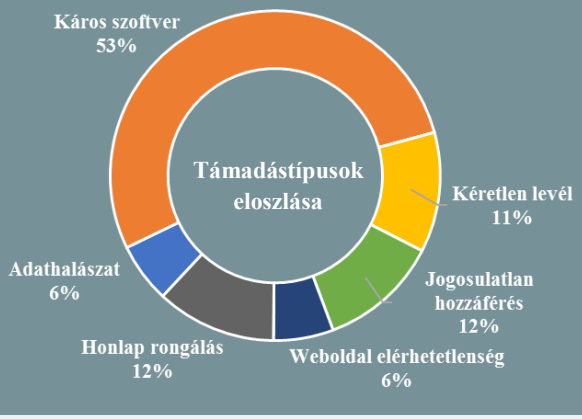
Incidens adatok: 2017.10.18. — 2017.10.24.





Szigorúbb adatvédelmi szabályok az e-kommunikációs szolgáltatásokhoz

(www.helpnetsecurity.com)

Az Európai Parlament Állampolgári Jogi, Bel- és Igazságügyi Bizottsága (LIBE) megszavazta az uniós polgárok magánéletének védelmében hozott új szabályzatot, amely olyan elektronikus hírközlési szolgáltatásokra vonatkozik, mint az SMS-, a telefon, valamint az internetes szolgáltatások. Az új rendelet (Regulation on Privacy and Electronic Communications) a GDPR általánosabb megközelítését hivatott kiegészíteni. A Bizottság betiltaná a cookie-kal történő adatgyűjtést és a felhasználók nyilvános hotspotokon keresztül történő nyomon követését, ha a felhasználók ehhez nem adták egyértelmű hozzájárulásukat, illetve szigorú adatfeldolgozási korlátokat kívánnak szabni. **Bővebben...**

EU-s kiberdiplomáciai eszköztár

(www.euractiv.com)

EU-s diplomaták megegyeztek a kölcsönös segítségnyújtásról hackerek felderítésével és vád alá helyezésével, valamint kibertámadások esetén a tagállamok közötti segítségnyújtással kapcsolatban. Az október 11-én egyeztetett irányelvek a támadásokkal kapcsolatos megelőző intézkedések mellett a lehetséges reakciókat tekintve diplomáciai beavatkozást és különböző szankciók kilátásba helyezését is lehetővé teszik. Abban az esetben is lehetőség van a megjelölt akciók lefolytatására, amennyiben az csupán a „barátságtalan cselekedet” jogi kategóriába tartozik. Az eszköztárral kapcsolatos júniusi egyeztetés során a miniszterek megegyeztek arról, hogy az EU-nak nem szükséges bizonyítania, hogy a támadás adott országból érkezett, mielőtt válaszlépést tesznek. Biztonsági szakértők ezt aggályosnak vélik és arra hívják fel a figyelmet, hogy egy támadás valós eredőjének felderítése sokszor nem egyértelmű. **Bővebben...**

Friss APWG jelentés

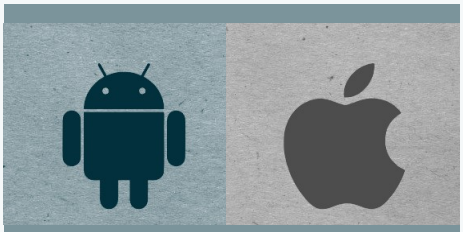
(www.globalsecuritymag.com)

Az adathalászat mérséklésére létrehozott Anti-Phishing Working Group (APWG) legújabb összefoglalójában – többek között – arról ad hírt, hogy 2017 első félévében kissé megnőtt a logisztikai és a hajózási szektort, valamint a fájl megosztó és felhő szolgáltatásokat érő adathalász tevékenység. Azonban összességében a célkeresztben továbbra is leginkább a pénzügyi, a ’SaaS’ és a webmail szolgáltatások állnak. Felhívják a figyelmet arra, hogy a sikeres felhasználónév és jelszó lopások segítségével nem csak közvetlen módon nyílhat lehetőség a támadóknakpénz szerzésére, hanem — a rendszereken szerzett jogosultságoknak hála — számtalan egyéb káros tevékenységet is végezhetnek, például kéretlen reklám levelek terjesztésébe kezdhetnek vagy akár árukat is rendelhetnek illetéktelenül. Komoly problémát okoz az ingyenes webhoszting szolgáltatások és weboldal készítő eszközök könnyű és olcsó hozzáférhetősége. **Bővebben...**

Támadás érte a cseh parlament választási weboldalakat

(www.ehackingnews.com)

A múlt hétvégén tartott parlamenti választások során a Cseh Statisztikai Hivatal (CZSO) arról számolt be, hogy az adatok feldolgozása közben egy ún. elosztott túlterheléses támadás (DDoS) érte a választási infrastruktúrájukat. A CZSO szóvivője Petra Bacova tájékoztatása alapján átmenetileg elérhetetlenné váltak a volby.cz és a volbyhned.cz weboldalak, azonban a támadás nem befolyásolta a választások eredményeit. A két weboldal működését sikeresen helyreállították, valamint a vizsgálatot is megkezdték az üggyel kapcsolatban. **Bővebben...**



Jutalom jár a hibák feltárásáért

(www.helpnetsecurity.com)

A Google új bug bounty programjában egyenlőre a legnépszerűbb alkalmazások tekintetében (Alibaba, Dropbox, Duolingo, Headspace, Line, Snapchat, Mail.Ru, és a Tinder) 1 000 dolláros jutalomért kereshetők a sérülékenységek. Kikötés, hogy a feltárt hibáról egy részletes megvalósíthatósági példát (PoC) is csatolni kell a jelzéshez, amelynek az Android OS 4.4-es vagy annál magasabb verzióján kell működnie. **Bővebben...**

Tájékoztatás kérés az Apple-től

(www.engadget.com)

Amerikai szenátorok részletes tájékoztatást kértek az Apple-től a kínai App Store-ból eltávolításra került VPN alkalmazásokkal kapcsolatban. Többek között arra voltak kíváncsiak, hogy a cég tett-e kísérletet az alkalmazások újbóli elérhetővé tételére. Az Apple még nem adott hivatalos választ. **Bővebben...**

IT biztonsági Tanács

Szervezetünk biztonsági kultúrája meghatározhatja az egyén biztonságtudatos magatartását.

Ennek érdekében szervezzünk képzéseket olyan témákban, mint az adatok megosztásának szabályai és a rosszindulatú weboldalak felismerése. Ezáltal arra ösztönözzük a felhasználókat, hogy felelősséget vállaljanak a tevékenységeikért, továbbá, hogy képesek legyenek önállóan is felmérni a kockázatokat.

Technológiai akadályok a kiberbűnözők felderítésében

(www.helpnetsecurity.com)

Az Europol sürgeti az internet-szolgáltatókat, hogy hagyjanak fel a Carrier Grade Network Address Translation (CGN) technológia használatával. A CGN segítségével adott esetben több felhasználó is ugyanazon a publikus IP címen keresztül éri el az internetet. Eredetileg ezt egy átmeneti kerülő megoldásnak szánták a fogyóban lévő IPv4 címek okozta probléma kiküszöbölésére, amelyet az IPv6-ra történő fokozatos átállás során felszámoltak volna. Egyes szolgáltatók azonban ezt a megoldást teljes mértékben helyettesítőként alkalmazzák a mai napig, ezzel komoly nehézségeket okozva a kiberbűnözők utáni nyomozásban, mivel sok esetben az IP cím az egyedüli nyom az azonosításhoz. Az Europol ügyvezető igazgatója Rob Wainwright szerint különösen aggasztó, hogy a mobil -internet szolgáltatók 90%-ban ilyen technológiával kapcsolják a felhasználókat a világhálóra. **Bővebben...**

Kritikus rendszereket támadnak az Egyesült Államokban

(www.wccftech.com)

Figyelmeztetést adott ki az amerikai Belbiztonsági Minisztérium (DHS) és az (FBI) egy kiritikus infrastruktúrák elleni célzott kibertámadási kampány miatt. Eszerint egy államilag szponzorált hacker csoport aktív ipari kémkedést folytat egyesült államokbeli energia-, nukleáris-, víz-, légügyi és egyéb kritikus gyártási ágazatok vállalatai és kormányzati létesítményei ellen. A riasztás szerint a kampány már legalább 2017 májusa óta tart. Az amerikai kormányzati CERT által közzétett információk szerint a csoport jól felkészült és számos rosszindulatú eszközt használ, miközben egyéb, másokat érintő károkat is okoznak a támadások során. Elemzők attól tartanak, hogy a támadások egy új fázisba érhetnek, amikor operatív rendszerekhez igyekeznek hozzáférést szerezni, amelynek segítségével még pusztítóbb támadásokat intézhetnek. **Bővebben...**

Elérhető a Windows 10 új zsarolóvírusok elleni védelmi funkciója

(www.bleepingcomputer.com)

A Windows 10 múlt héten elérhetővé vált frissítésével (Fall Creators Update), a Microsoft egy olyan anti ransomware funkciót (Controlled Folder Access) vezetett be, amely segítségével kontrollálható, hogy a kijelölt könyvtárakban található fájlokon mely alkalmazások és milyen műveleteket végezhetnek, ami – elméletileg – védelmet nyújthat a zsarolóvírusok ellen. A BleepingComputer több zsarolóvírus variánssal tesztelte a funkciót (Asasin Locky, x1881 CryptoMix, Comrade HiddenTear, és a Wyvern BTCWare), amelyek sikeresnek bizonyultak, azaz meg tudták előzni a védett könyvtárak titkosítását. A publikációban a beállítással kapcsolatban step-by-step leírás is található, azonban hangsúlyozzák, hogy ez a megoldás sem nevezhető teljes értékű védelemnek, csupán egy hasznos kiegészítő. **Bővebben...**

Fokozódó mobil fenyegetettség

(www.betanews.com)

A Kaspersky új jelentése szerint a felhasználók túlzott mértékben támaszkodnak a mobil készülékeikre, ami növekvő biztonsági kockázatot hordoz magában. Az elemzés kitér arra is, hogy a felhasználók – kortól és foglalkozástól függetlenül – a PC-s környezet helyett egyre inkább okos telefonokon keresztül bonyolítják a levelezésüket, illetve a netes vásárlásokat. Többek között arra is felhívják a figyelmet, hogy a legtöbb mobil készülék sérülékeny és nincs ellátva megfelelő védelemmel, sőt, a megkérdezettek 41%-a ismerte el, hogy egyáltalán nincs védelmi szoftver a készülékeiken. **Bővebben...**