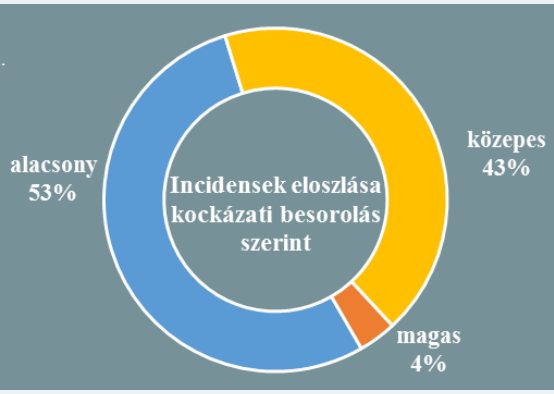
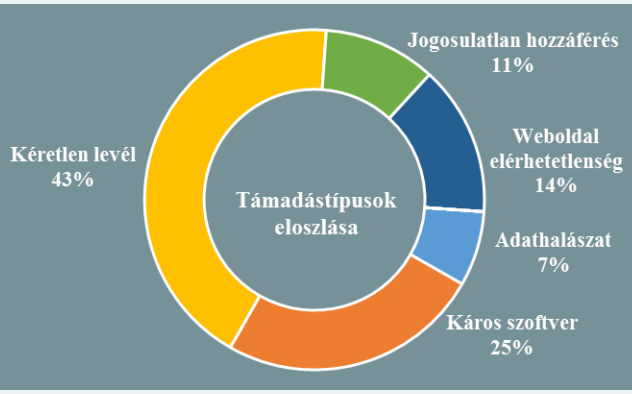
Incidens adatok:
2018.03.02. - 2018.03.08.





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

Komoly biztonsági hibákat fedeztek fel a 4G/LTE protokollokban

(www.bleepingcomputer.com)

Egyetemi kutatók az LTEInspector nevű nyílt forráskódú szoftver segítségével összesen tíz új sérülékenységet azonosítottak az LTE protokollokban, további kilenc, már ismert mellett. A publikusan elérhető "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE" című tanulmányukból kiderül, hogy a sérülékenységek – többek között – módot adhatnak más felhasználók nevébena hálózatra való feljelentkezésre, üzenetek küldésére és elfogására, egy adott eszköz helyzetének meghamisítására, vagy akár eszközök leválasztására a hálózatról. Még aggasztóbbá teszi a felfedezést, hogy a biztonsági rések közül nyolcat sikeresen ki tudtak használni egy relatíve alacsony költségű (körülbelül 3 900 dolláros) tesztrendszeren, ami azt jelenti, hogy a bűnözők számára ez nem lényeges korlátozó tényező a számtalan potenciális felhasználási móddal – például alibi gyártás a mobil eszköz helyzetére vonatkozó adatok módosításával – szemben. A kutatók a sérülékenységek javítását nem tartják valószínűnek, mivel az utóbbi évek során feltárt problémák sem kerültek kezelésre, emellett elismerik, hogy a visszafelé-kompatibilitás megőrzése is komoly nehezítő tényező. **Bővebben...**.

Izrael bővítené a kiberkémkedési arzenálját

(www.motherboard.vice.com)

Izrael hacking eszközöket vásárolna európai kiberbiztonsági cégektől, a berlini képviseletén keresztül – értesült a Motherboard. Pénteken a lap már nyilvánosságra hozott egy 2015-ös elektronikus levelet, melyet az izraeli kormány több amerikai biztonsági cég számára is megküldött. A levélben arról írnak, hogy zero-day információkat szeretnének vásárolni a bűnüldöző hatóságok és hírszerző ügynökségek részére, széleskörű felhasználásra. Egy meg nem nevezett európai forrás most egy 2017 augusztusában, ugyancsak a berlini nagykövetségtől érkezett levelet osztott meg a Motherboard-dal, amelyben szintén nulladik napi sérülékenységek kapcsán végzett kutatásokról, vagy egyéb együttműködési lehetőségekről érdeklődnek. A korábbihoz képest viszont különbség, hogy már nem csupán azokkal a cégekkel keresik a kapcsolatot, akik fő tevékenységként foglalkoznak exploit fejlesztéssel, hanem afelől is érdeklődnek, hogy a megkeresett vállalatok rendelkeznek-e olyan kapcsolattal, akiktől ilyen jellegű technológiát lehetne vásárolni. **Bővebben...**

Nyilvánosságra került a Memcached szerverek kihasználási módja

(www.bleepingcomputer.com)

Február végén a GitHub, néhány nappal ezelőtt pedig egy meg nem nevezett amerikai szolgáltató szenvedett el rekord mértékű (előbbi 1,3 utóbbi 1,7 Tbps sávszélességű) szolgáltatásmegtagadást okozó hálózati támadást, amelyeket a támadók sérülékeny Memcached rendszerek kihasználásával okoztak. Nem sokkal ezt követően már publikussá is vált a kihasználás lehetséges módja (proof-of-concept), ráadásul rögtön két változatban. Mindezt súlyosbítja, hogy a GitHub-ra és a Pastebin-re is feltöltött állományok között mintegy 17 000 sérülékeny szerver címe is megtalálható. Biztonsági kutatók számítottak rá, hogy előbb-utóbb elérhetővé válik a metódus, ami azonban komoly aggodalomra ad okot, hiszen így alacsonyabb technikai felkészültséggel rendelkezők számára is lehetővé vált ilyen jellegű támadások indítása. Daniel Smith, a Radware kutatója szerint nagyon valószínű, hogy a most ismertté vált technikák rövid időn belül a feketepiaci DDoS-as-a-Service „szolgáltatók” portfóliójában is meg fognak jelenni. **Bővebben...**

Meddig tarthat az iPhone-ok állítólagos sérülékenysége?

(www.forbes.com)

Az izraeli Cellebrite mellett már egy amerikai startup (Grayshift) is azt állítja, hogy képes hozzáférni az Apple iPhone készülékekhez. Reklámjuk szerint 15 000 dollár fejében rendelkezésre bocsátanak egy online elérhető szoftvert (GreyKey), ami képes feloldani az iOS10 és 11-es verziót futtató készülékek képernyő zárolását. Ez ugyan licencenként csak 300 használatot tesz lehetővé, azonban létezik korlátlan verzió is, amit 30 000 dollárért kínálnak. Bár a pontos kihasználási módról nem érhető el nyilvános információ, Ryan Duff, a Point3 Security igazgatója szerint a Grayshift hasonló megoldásra juthatott, mint a Cellebrite, ami vélhetően egy próbálgatás-alapú támadás a Secure-Enclave ellen. Duff szerint azonban – az üzleti modellből fakadóan – a javítás valószínűleg nincs messze, mivel ha az Apple mérnökei szert tesznek a GreyKey-re, előbb-utóbb azonosítani fogják a sérülékenység okát. **Bővebben...**

IT biztonsági Tanács

Különböző szolgáltatások igénybevétele esetén, gyakran kérik el tőlünk személyes adatainkat. Az adatkezelés megkezdése előtt érdemes utánajárni a szolgáltatók adatvédelmi és adatkezelési irányelveinek, melyekről kötelesek egyértelműen és részletesen tájékoztatni az érintetteket.

Kérjünk felvilágosítást az adatgyűjtés céljáról, a rólunk tárolt adatok kezelési módjáról, illetve azok törlési lehetőségeiről.

Magyar kutatók elemeztek kiszivárgott NSA kódokat

(www.securityweek.com)

Az NSA-hez köthető Equation Group korábban nyilvánosságra került hacker eszközeinek elemzése során a magyar Crysys Lab munkatársainak új, nem támadó jellegű funkciót sikerült azonosítaniuk. A Budapesti Műszaki és Gazdaságtudományi Egyetemen működő Crysys – akik többek között a Duqu APT felfedezésével szereztek ismertséget – a "Lost in Translation" fájlok között találtak rá a "Territorial Dispute" modulokra, amelyeket véleményük szerint az amerikai hírszerző ügynökség konkurens APT-k felderítésére használhatott. A Crysys szerint a kódok relatíve egyszerűek, a céleszközön megadott fájlok, Windows registry bejegyzések és egyéb, ismert APT-k indikátorai után kutatnak. A kutatók érdekes felfedezésnek tartják, hogy bár több százezer indikátor érhető el, ami APT-tevékenységhez kapcsolódik, az eszközök mégis mindössze 1-5 indikátort használtak. Ennek oka vélhetően az, hogy a működtető operátorok a lehető legkevesebb információhoz férjenek hozzá. A kutatás egyik vezetője, Bencsáth Boldizsár a SecurityWeek-nek elmondta, olyan mintát is találtak (SIG32), ami valószínűleg egy, a nyilvánosság előtt még ismeretlen APT-hez tartozik. **Bővebben...**

A Windows Defender észleli a FinFisher-t

(www.zdnet.com)

A Microsoft közleményben tudatta, hogy a Windows saját védelmi komponense jelenleg képes detektálni a kormányzatok által széles körben használt FinFisher kémprogramot. Múlt év során biztonsági kutatók olyan Word dokumentumokba ágyazott verziókról adtak hírt, amelyeket nulladik napi Microsoft Office sérülékenységek kihasználásával próbáltak orosz ajkú célpontok rendszereire juttatni. Az ESET kutatói ezek analízisével kapcsolatban problémába ütköztek, a szoftver fejlesztői által alkalmazott fejlett sandbox felismerő technikák miatt. A Microsoft is megerősíti, hogy az ellenőrzést megnehezítő kifinomult megoldások komoly energia befektetésről tanúskodnak, amelyek a hagyományos elemző eszközökkel közel lehetetlenné teszik a feldolgozást, ilyen például a virtuális környezetek észlelése és az ún. „spagetti kódolás" alkalmazása. Ennek ellenére az Office 365 Advanced Threat Protection sikeresen felismeri a csatolmányokba ágyazott FinFisher kódokat, emellett a Windows Defender is észleli a FinFisher támadási technikáit, mint például a memória befecskendezés. **Bővebben...**

Az DHS újfent elbukott a biztonsági auditon

(www.csoonline.com)

Az amerikai Belbiztonsági Minisztérium (DHS) felügyeleti szerve (OIG) által végzett éves vizsgálat ismét aggasztó képet festett a rendszerek biztonsági állapotáról, melynek legfőbb tanulsága, hogy a DHS elavult szoftverekkel dolgozik és nem fordít kellő figyelmet a kritikus sérülékenységek javítására, beleértve azt is, amit a WannaCry zsarolóvírus terjesztéséhez használtak ki. Donald Trump miniszterelnök a kritikus rendszerek védelméről szóló 2017 májusi rendeletében minden szövetségi szerv számára előírta a NIST keretrendszer alkalmazását. Az ebben meghatározott funkcióknak („Megismerés", „Védelem", „Esemény észlelése", „Esemény kezelése" és „Helyreállítás") való megfelelést a vizsgált rendszerek tekintetében 1-5-ig rangsorolták, ahol az 1-es besorolás („Rögtönzött") a legalacsonyabb szintet, az 5-ös („Optimalizált") besorolás, pedig az informatikai biztonsági követelményeknek való teljes körű megfelelést jelenti. Ezek közül a 4-es szintet már elégségesnek fogadják el, amit a DHS csak a „Megismerés" és a „Esemény kezelése" funkciók kapcsán ért el, a többi tekintetében azonban súlyos hiányosságokat tártak fel. Például kiderült, hogy olyan elavult szoftverek is használatban vannak, mint a Windows Server 2003, amihez már 2015 júliusa óta nem érhető el gyártói támogatás. **Bővebben...**