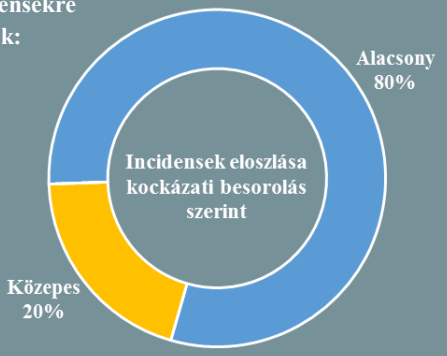
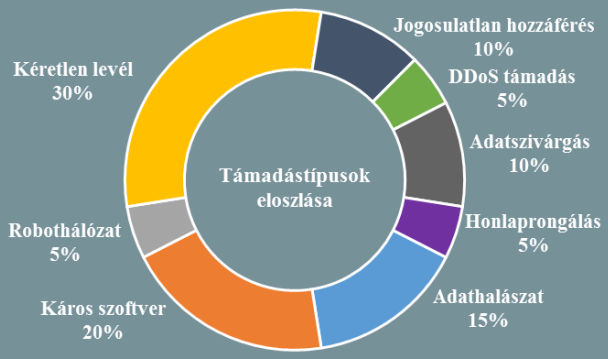
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 27. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.06.29. - 2018.07.05.





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

Új fegyver a belsős adatszivárogtatás ellen?

(www.ccdcoe.org)

A május végén Tallinnban megrendezett CyCon X konferencián került bemutatásra egy svájci kutatócsoport munkája, mely egy új, a belső alkalmazottak által végrehajtott adatlopások elleni technológiára vonatkozóan tett javaslatokat. A tanulmányban arra hívják fel a figyelmet, hogy a rosszindulatú munkatársak oly módon is eltulajdoníthatnak érzékeny, bizalmas információkat, hogy azt a képernyőjükön megjelenítik, és a képernyőről mobiltelefonjuk segítségével képet készítenek, amit később illetékteleneknek továbbítanak. Az ilyen típusú adatlopás vizsgálata során általában közel lehetetlen a felelős azonosítása, azonban a konferencián bemutatott új módszer ezt nagymértékben megkönnyítheti. A kutatók javaslata alapján olyan vízjelezési technológiát célszerű alkalmazni, mely az emberi szem számára láthatatlan, de a gépi értelmezés során információt szolgáltathat a bejelentkezett felhasználóról, a kép készítésének idejéről, vagy akár a kép elkészítésének helyéről is. A javasolt technológia lehetővé teszi, hogy a képernyőről készült fénykép is hordozza ezeket az információkat, illetve biztosítja, hogy a vízjel elemeinek törlése, sérülése esetén is lehessen releváns adatokat visszanyerni. Emellett biztosítja azt is, hogy a vízjelek felismerése esetén se lehessen azokat meghamisítani, ezzel a gyanút más személyre terelni, vagy a vízjelben kódolt adatokat bármilyen eljárással módosítani. **Bővebben...**

Új kiberbiztonsági együttműködés litván javaslatra

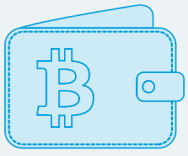
(www.infosecurity-magazine.com)

Több EU-s ország is részt vesz a Litvánia által javasolt új kiberbiztonsági együttműködésben, amely egy közös kiber-válaszerő létrehozását célozza, a jövőbeli kibertámadások elleni harc elősegítéséhez. A szándéknyilatkozatot eddig Litvánián kívül öt ország írta alá – Románia, Horvátország, Észtország, Hollandia és Spanyolország – melyhez év végéig várhatóan még további négy európai nemzet fog társulni. Belgium, Németország, Görögország és Szlovénia csupán megfigyelőként csatlakozik majd, az Egyesült Királyság bármilyen fokú közreműködéséről azonban nem érkeztek hírek. A nyilatkozatban minden ország vállalja egy kiber egység létrehozását, melynek tagjai a résztvevő országok biztonsági szakértői közül kerülnek majd ki és feladatuk az incidensek közös kivizsgálásában, kezelésében és semlegesítésében való részvétel lesz. Az első közös gyakorlat még idén megrendezésre kerül, ennek Litvánia ad majd otthont. **Bővebben...**

Malware támadással térítik el a virtuális pénz utalásokat

(www.bleepingcomputer.com)

A kriptovaluta tranzakciók során továbbra is jellemző gyakorlat, hogy a felhasználók a hosszú és nehezen megjegyezhető címeket nem kézzel írják be, hanem átmásolják. Ez azonban lehetőséget nyújt egy olyan malware támadásra, ami a felhasználó gépét megfertőzve azt figyeli, hogy a Windows vágólapon megjelenik-e kriptovaluta cím, és amennyiben igen, azt meghamisítja egy, a támadók felügyelete alatt álló pénztárca címére, így a figyelmetlen felhasználó rossz helyre utalja az összeget. A módszer egyáltalán nem új keletű, a Bleepingcomputer legutóbbi felfedezése azonban aktualitást kölcsönöz a témának, ugyanis utóbb egy olyan mintát azonosítottak, aminek a monitorozáshoz használt címlistája már nagyságrendekkel több – egészen pontosan 2,3 millió – kriptopénztárca címet tartalmazott. **Bővebben...**



Útmutató mobil appok biztonságossá tételéhez

(www.ncsc.nl)

A holland Nemzeti Kiberbiztonsági Centrum (NCSC) egy, a mobil appok biztonságával kapcsolatos útmutatót adott ki. Mivel a mobilon alkalmazott programok egyre fontosabb szerepet játszanak életünkben, emiatt a különféle támadásoknak is mind jobban kitettek, ezért egyaránt fontos, hogy a mobil készülékek és az azokra telepített programok is biztonságosak legyenek. A kiadvány intézkedési javaslatokat tartalmaz, hogy miként tehetőek az alkalmazások még biztonságosabbá, hogyan lehet a felhasználókat megvédeni a különféle támadásoktól. Az anyag oly módon került strukturálásra, hogy az illeszkedik a webes alkalmazások biztonságával kapcsolatos tájékoztatóhoz, így, ha a mobil app szerver oldalán webalkalmazás biztosítja a felhasználói interakciót, a mobilalkalmazásokra tett javaslatok zökkenőmentesen integrálhatóak a webalkalmazásokkal kapcsolatosan kiadott tájékoztatóhoz. **Bővebben...**

IT biztonsági Tanács

A Symantec biztonsági kutatói **közreadtak** egy online eszközt a nemrég több, mint félmillió hálózati berendezést megfertőző VPNFilter malware detektálásához.

Az eszköz ugyan nem képes pontosan meghatározni, hogy az adott hálózaton ténylegesen jelen van-e a vírus, csupán annak egy komponensének (ssler plugin) a tevékenységét, ám így is javasolt egy gyors vizsgálatot végezni vele.

Újabb sérülékenységeket találtak a 4G-nél, ami az 5G-t is érintheti

(www.bleepingcomputer.com)

Egy akadémikusokból álló csoport a 4G/LTE hálózati protokoll esetében három sérülékenységet azonosított. A biztonsági rések közül kettő passzívnak számít, azaz általuk „csupán” lehallgatható a mobil forgalom, a harmadik segítségével azonban az adatok módosítása is lehetséges. Ez utóbbi során ugyanis olyan metainformációk nyerhetők ki, amelyek felhasználásával meghatározható, hogy az áldozat milyen weboldalt látogat meg. Továbbá egy „aLTEr”-nek elnevezett támadási vektor elméletben arra is lehetőséget nyújt, hogy a támadók a DNS csomagok módosításával (DNS spoofing) eltérítsék a webes forgalmat, egy általuk választott – például potenciálisan káros – webhely felé. Szerencsére a kutatók szerint a valóságban kicsi a valószínűsége az ilyen típusú támadásoknak, mivel azok kivitelezése csak speciális, és igen költséges eszközökkel lehetséges. **Bővebben...**

Újrahasznosított kiberfegyverek

(www.ccdcoe.org)

Biztonsági kutatók vizsgálták annak a lehetőségét, hogy miként lehet egy már létező kiberfegyvert úgy felhasználni, hogy a káros kód nagy része érintetlen marad, miközben annak irányítása átkerül az új tulajdonoshoz. A május végén publikált tanulmányukban egyrészt megvizsgálták, hogy ki lehet-e cserélni egy káros kódban (malware) a töltetet (payload) vagy az irányító szerver(ek) adatait, illetve vizsgálták az ilyen elképzelt tevékenység hatásait, következményeit is. A kiberfegyverek újrahasznosításának előnye, hogy nincs szükség hosszas, időrabló és pénzigényes vizsgálatokra, hogy újabb és újabb kiaknázható sérülékenységek kerüljenek feltárásra, illetve nem kell megvásárolni a piacról az azonosított 0-day sérülékenységeket, elég csak magát a töltetet átírni, hogy immár az új tulajdonos érdekeit szolgálhassa. A tanulmányban ismertetett eljárás hátránya lehet, hogy amennyiben a rosszindulatú kódok száma megnő, az a kibertámadások számára is hatást gyakorolhat, mivel az olyan szegényebb országok ─ esetleg aktivista csoportok ─ akik eddig nem engedhették meg maguknak, hogy szofisztikált támadó képességet hozzanak létre, ezzel a módszerrel immár hatékony és erős fegyverekhez juthatnak, szinte ingyen. **Bővebben...**

Egy adatlopás, ami majdnem tönkretette az élvonalbeli kémszoftver gyártót

(www.motherboard.vice.com)

Egy nyilvánosságra került vádirat szerint az izraeli NSO Group egy volt munkatársa kémprogramokat ─ köztük a széles körben használt Pegasus kódját ─ tulajdonított el a cégtől, és próbálta meg értékesíteni a vállalat ügyfélkörén kívül a darkneten, mintegy 50 millió dollár értékű kripto valutáért. A cég kizárólag kormányok részére kínálja piacvezetőnek számító kiber eszközeit, melyek közül egyes verziók lehetővé teszik, hogy a támadók mobil eszközökről ─ akár iPhone -ról is ─ a tulajdonos tudta nélkül kinyerjenek szinte bármilyen információt. A tolvaj a sötét webes hirdetésében azt állította, hogy egy külső támadás során sikerült hozzáférnie az NSO rendszereihez, egy érdeklődő azonban felvette a kapcsolatot a vállalattal, és közösen sikerült beazonosítaniuk a támadót. A személyt most a nemzetbiztonság veszélyeztetésével is vádolják, mivel az adatlopás az NSO-t szakmailag teljesen ellehetetlenítette volna, emellett hátrányosan érintheti az amerikai Verint részéről felmerült mintegy 1 milliárd dolláros felvásárlási terveket is. **Bővebben...**