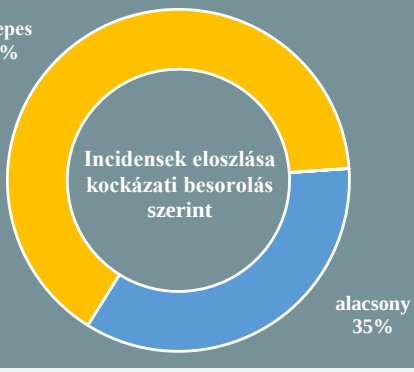
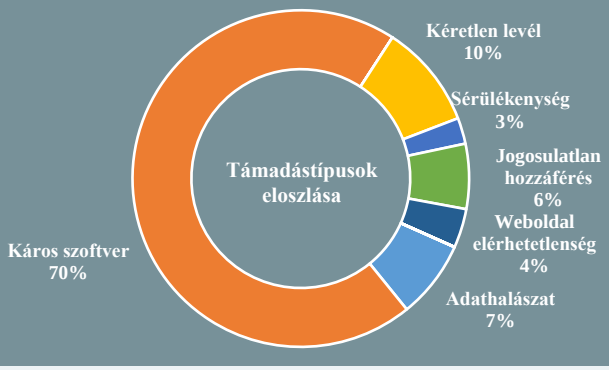
Incidens adatok:
2018.02.09. - 2018.02.15.





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

Folytatódnak a pénzintézetek elleni kibertámadások

(www.securityweek.com)

Az orosz központi bank jelentése szerint 2017-ben gyakoribbakká váltak a bankok elleni támadások, amelyek során széles körben elterjedt eszközöket és módszereket vetnek be (például Metasploit, Cobalt Strike, Empire, Mimikatz). Az oroszországi Globex bank decemberben ismerte el, hogy a SWIFT rendszeren keresztül közel 1 millió dollárt próbáltak megszerezni a támadók, ámbár ennek csupán egy töredékéhez sikerült valóban hozzáférniük. Az indiai City Union bank múlt vasárnap három támadásról számolt be, amelyek összesen közel kétmillió dollártól próbálták megfosztani a pénzintézeteket a SWIFT belső üzenetküldési rendszerének segítségével. A Pandzsáb Állami Nemzeti Bank pedig 1,7 millió dolláros csalásról számolt be, amelyben a hírek szerint a bank alkalmazottjai is érintettek voltak. Az elmúlt években a SWIFT rendszert érintő szofisztikált támadások egyre gyakoribbá váltak, ezért a rendszer mögött álló szervezet – Society for Worldwide Interbank Financial Telecommunication – több intézkedést is hozott a biztonság növelése érdekében. **Bővebben...**

Kibertámadás érte a 2018. évi téli olimpiai játékok rendszereit a megnyitó alatt

(www.bleepingcomputer.com)

Múlt pénteken a helyszínen tartózkodó újságírók problémákat tapasztaltak az internet elérésben, valamint a televíziós rendszer működésében a dél-koreai Phjongcshangban tartott megnyitó ünnepség idején. Habár a szervezők nem nyilatkoztak az esetről, a hatóságok végül vasárnap elismerték, hogy az informatikai rendszerben tapasztalt zavarok egy összehangolt kibertámadás miatt következtek be. Az ennek során alkalmazott káros kódról – amely az 'Olympic Destroyer' nevet kapta – a Cisco Talos biztonsági szakértői publikáltak elemzést. Ebben arról írnak, hogy a vizsgálatok során nem találták nyomát annak, hogy adatszerzés lett volna a támadók célja, úgy tűnik egyedül a károkozás állhatott a szándékukban. A fertőzés kezdeti lépésével kapcsolatban a kutatók nem közöltek információt, mivel elmondásuk szerint többféle forgatókönyv is elképzelhető. A káros kód nem törli az áldozat fájljait, azonban bootolási problémákat okoz, mivel több lényeges Windows folyamatot is leállít, emellett – hogy a helyreállítást megnehezítse – az árnyékmásolatokat is törli. A támadás hátterében egyesek Észak-Koreát, mások inkább Oroszországot vagy Kínát sejtik. **Bővebben...**

Orszorszország miatt törthetett ki NotPetya fertőzés

(www.bleepingcomputer.com)

Az Egyesült Királyság külügyminisztériuma közleményt adott ki, amelyben az orosz kormányt teszi felelőssé a 2017 júniusi 'NotPetya' zsarolóvírus támadás kampányért, mely elsősorban ukrán pénzügyi, energetikai és kormányzati célpontok ellen irányult, de más európai és orosz vállalatok számára is komoly károkat okozott. Az ukrán hírszerzés már jóval korábban élt a váddal, ám ez az első alkalom, hogy egy nyugati kormány hivatalos csatornán nyilvánít véleményt az üggyel kapcsolatban. Mindeközben a brit nemzeti kiberbiztonsági központ (NCSC) is jelezte, "majdnem biztosak" abban, hogy az orosz hadsereg állt a támadás mögött. A Washington Post egy korábbi publikációban, CIA-s forrásokra hivatkozva ennél még pontosabban fogalmaz, ebben ugyanis a GRU-t jelölik meg felelősként, ám ezzel kapcsolatban nem történt hivatalos megerősítés. **Bővebben...**

A Kaspersky után újabb cégeket ért kémkedési vád

(money.cnn.com)

Hírszerzési ügynökségek (CIA, NSA, FBI, valamint DIA) vezetői, az Egyesült Államok hírszerzési bizottsága (Senate Intelligence Committee) előtt fejtették ki álláspontjukat, miszerint a Huawei és a ZTE kínai okostelefon gyártók termékei és szolgáltatásai magas biztonsági kockázatot jelentenek az Egyesült Államok számára, így óvatintik a lakosságot azok használatától. A vád szerint a nevezett gyártók "túl szoros kapcsolatot ápolnak külföldi kormányokkal", ez pedig káros tevékenységekre, megfigyelésre adhat módot. Mindez nem minden előzmény nélküli, már 2012-ben merültek fel kételyek a cégekkel kapcsolatban, a kormányzat pedig egyes esetekben megakadályozta, hogy szövetségi ügynökségek számára technológiát értékesítsenek. Januárban azután hirtelen megszakadtak a Huawei és az AT&T közötti tárgyalások, amelyek a kínai gyártó telefonjainak az amerikai picon történő értékesítéséről szóltak, két szenátor pedig ennél is tovább ment, február elején törvényjavaslatot nyújtottak be, amelynek értelmében minden kormányzati szervet eltiltanának a szóban forgó gyártók termékeinek használatától. **Bővebben...**

IT biztonsági Tanács

A támadók sok esetben a futtatható fájlokat valamilyen más fájltípusnak (pl.: dokumentumnak) álcázzák, legyünk emiatt figyelmesek a fájlkiterjesztésekre. Windows – és macOS – rendszerek esetében ez alapértelmezetten nem jelenik meg, ezért manuálisan kell bekapcsolni.

Az egyes Windows verziók esetében az alábbi Microsoft támogatási oldalon találhat ehhez segítséget:

https://support.microsoft.com/en-us/help/14201/windows-show-

Atomtudósok próbáltak kriptovalutát bányászni egy szigorúan őrzött orosz állami létesítményben

(www.bleepingcomputer.com)

A hatóságok fizikusokat tartóztattak le Oroszországban, mivel azok az ország legerősebb szuperszámítógépeit engedély nélkül bitcoin bányászatra használták fel. Az esetet a rendőrség helyett a KGB-utód Szövetségi Biztonsági Szolgálat (FSZB) kezelte, mivel az az ország vezető nukleáris laboratóriumában (RFNC-VNIIEF) történt. Maga az intézet egy, a külvilágtól elzárt és katonailag biztosított városban (Sarov) található, amelyet kizárólag a kutatóintézet munkatársai lakják. Az Interfax értesülései szerint a bányászatra használt egy pataflop-os szuperszámítógép egy szigorúan izolált hálózaton működött, így nem szabadott volna csatlakoznia a világhálóra. Amint ez megtörtént, riasztások érkeztek a biztonsági szolgálathoz, így a tevékenységre gyakorlatilag azonnal fény derült és a résztvevőket átadták a hatóságoknak. Nem ez volt az egyetlen jogtalan kriptobányászati incidens a régióban a múlt hét során, egy ukrán professzor is ezzel próbálkozott egy lutski felsőoktatási intézményben, amire a hírek szerint a videokártyák által keltett zaj miatt lettek figyelmesek. **Bővebben...**

Melyik szektornak kerülnek a legtöbbe a számítógépes támadások?

(www.helpnetsecurity.com)

A Ponemon intézet friss tanulmányában arról számol be, hogy a kibertámadások a pénzügyi szervezetek számára jelentik a legtöbb kiadást. A tanulmány elkészítéséhez a kiberbűnözők által okozott incidensek során felmerülő direkt költségeket vizsgálták, a hosszabb távú helyreállításból adódóakkal nem számoltak. Az eredmények szerint a szolgáltatás megtagadást okozó támadások, az adathalászat, valamint a belső fenyegetés okozza a legtöbb kárt a bankoknak és a hitelintézeteknek. Kiderült továbbá, hogy a pénzügyi szektor számára a kiberbűnözésből fakadó átlagos költségek 40%-kal nőttek az elmúlt három év során, cégenként ez 12,97 millió dollárt jelentett 2014-ben, tavaly azonban már 18,28 millió dollárt. Ezzel együtt, véleményük szerint a pénzügyi szektor körültekintően jár el a biztonsági technológiák beszerzésének tervezéskor, és ezzel sikeresen lejjebb is tudják szorítani a kiadásokat. **Bővebben...**

NATO fejlesztési tervek

(nationalcybersecurity.com)

Jens Stoltenberg NATO főtitkár egy brüsszeli konferencián a NATO parancsnoki struktúrájának reformjáról nyilatkozott. A tervek között említésre került egy új összevont parancsnokság felállítása, amelynek feladata az Atlanti-óceán alatti transzkontinentális telekommunikációs kábelek védelme, valamint új szárazföldi parancsnokságok létrehozására is törekednek, ám ezek pontos helyéről, valamint a létrehozás határidejéről még nem született végleges döntés. Stoltenberg elmondta, a fejlesztések fontos részét képzi a kibervédelem is, mivel az európai szerverek elleni támadások jelentősen emelkedtek az elmúlt két év során, amiért egyes nemzetek Oroszországot tették felelőssé. A távlati cél az, hogy minden előrelátható szövetséges katonai küldetésnek vagy műveletnek legyen kiber vonatkozása is. Ezzel kapcsolatban máris döntés született egy új kiber műveleti központ létrehozásáról a szövetség brüsszeli főparancsnokságának (SHAPE) részeként. **Bővebben...**