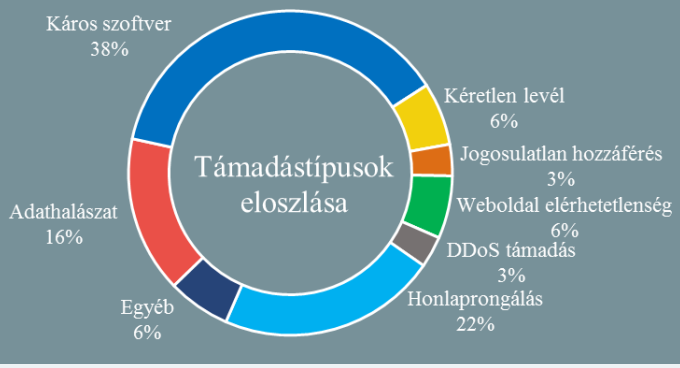
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 35. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.08.23. - 2019.08.29.



Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Nyugdíjas tisztviselőket vett célba egy észak-koreai hacker csoport

(www.zdnet.com)

Dél-koreai nyugállományú diplomatákat és hivatali, illetve katonai tisztviselőket céloz egy Észak-Koreához köthető hacker csoport műveleteivel. Simon Choi, az IssueMakersLab alapítója egy a ZDNetnek adott interjúban elárulta, hogy a Kimsuki vagy Velvet Chollima néven ismert hacker csoport legutóbbi – július közepétől augusztus közepéig tartó – kampánya során nyugdíjas nagykövetek, tábornokok, illetve Dél-Korea Külügyminisztériumának és Egyesítési Minisztériumának tagjainak számára, olyan adathalász levelek kerültek megküldésre Gmail és Naver e-mail fiókjaikon keresztül, amelyek egy hamis bejelentkezési oldalra irányították át az áldozatokat. A vizsgálatok alapján viszont nem lehetett megállapítani, hogy az elkövetőknek sikerült-e kompromittálniuk az e-mail fiókokat. Choi szerint a nyugalmazottak támadása olyan szempontból jó döntésnek minősül a kollektíva részéről, hogy a nyugállományban lévők – mivel nem állnak a szervezet kiberbiztonsági védelme alatt – könnyebben sebezhetőek és a beérkező támadásokról nem kapnak riasztást a védelmi rendszertől.

Adatsértést jelez a Chrome új funkciója

(www.bleepingcomputer.com)

A Google beépített adatszivárgási értesítővel látja el böngészőjét, amely figyelmezteti a felhasználókat, ha veszélybe kerülhettek bejelentkezési adataik. Kiderült ugyanis egy, a Google által végzett tanulmányból, hogy a bejelentkezési adatok 1,5%-a érintett korábbi adatszivárgásokban, illetve, hogy a felhasználók 26%-a – amennyiben értesítést kapnak az adatszivárgás tényéről – valóban megváltoztatja jelszavát. A tanulmány eredményeit figyelembe véve a Google úgy döntött, hogy ezt a funkciót beépíti a Chrome-ba, amely a böngészőbe történő bejelentkezést követően, a jelszóvédelem funkció bekapcsolásával lesz majd elérhető. **Bővebben...**

Az NCSC sietteti a Python 3-ra való átállás

(securityaffairs.co)

Az Egyesült Királyság Nemzeti Kiberbiztonsági Központja (NCSC) amiatt sürgeti a fejlesztőket, hogy alkalmazásaikban mielőbb térjenek át a Python legújabb verziójára, ugyanis a 2-es főverziónak 2020. január 1-vel megszűnik a támogatása. Azon szervezetek, akiknek alkalmazásai a támogatás megszűnését követően továbbra is a Python 2.x verzióját használják, kockára teszik rendszereik és adataik biztonságát, ugyanis a biztonsági frissítések hiányában a támadók könnyedén kihasználhatják a sérülékenységeket. **Bővebben...**

Már az internetszolgáltatók is érintettek a hongkongi tüntetéssorozatban

(www.zdnet.com)

A hongkongi internetszolgáltatók egyesülete (HKISPA) nyilatkozatot tett közzé szerdán, amelyben kritikával fogadja a Hongkong nyílt internetes hálózatát korlátozó terveket. Az Egyesület figyelmeztetése szerint ugyanis a megfontolatlanul bevezetett korlátozások – hatékonyság hiányában – további korlátozásokhoz fog vezetni, ami hasonlóan Kínához, egy hatalmas tűzfal bevezetését eredményezheti. Bár egyelőre enyhe szigorításokról van szó, mégis – a nyílt hálózati korlátozások – visszatarthatják a külföldi vállalatokat a hongkongi befektetésektől. A HKISPA nyilatkozata már egy válaszreakció volt az önkormányzat által megvitatott internetes szolgáltatóknak tervezett végrehajtási rendeletre, amelyben egyes internetes alkalmazások szelektív módon kerülnének leállításra. **Bővebben...**

Több ezer androidos eszközt fertőztek meg négy hónap alatt

(www.bleepingcomputer.com)

A Malwarebytes Labs kutatói fedezték fel az xHelper elnevezésű ún. Trojan dropper káros programot, ami május óta 32.000 androidos okostelefont és tabletet fertőzött meg, ezzel az eredménnyel pedig bekerült a cég 10 leggyakrabban felfedezett káros programjai közé. Az xHelper különlegessége, hogy terjedéséhez, illetve jelenlétének elrejtéséhez nem a fertőzött eszközök egy APK-t (application package file) használja, ami az „Eszközök" mappában telepítésre kerül, hanem JAR fájlnak álcázott titkosított DEX (Dalvik Executable) fájlokkal terjed, amelyek a dekódolást követően egy ELF (Executable and Linkable Format) fájlként kerülnek végrehajtásra a fertőzött eszközökön. A vizsgálatok során az is kiderült, hogy az xHelper két módon, egyrészt észrevétlenül (csak az alkalmazáslistában jelenik meg a program), másrészt részben leplezett módon képes működni, utóbbihoz egy ikon is létrejön az értesítések menüben, amelyet különböző riasztásokkal áraszt el. A felhasználók ezek egyikére kattintva egy webes játékokat tartalmazó weboldalra kerül átirányításra ahonnan a program készítői eltulajdonítják a kattintásokért járó bevételt. **Bővebben...**

IT biztonsági Tanács

Munkahelyi környezetben előfordulhat, hogy a szűkös határidők, stressz, a túl sok párhuzamosan futó feladatok vagy a szükséges információk hiánya miatt, véletlenül az arra nem jogosultakkal osztunk meg adatokat.

Az ilyen jellegű adatszivárogtatás bekövetkezésének kockázata csökkenthető az NBSZ NKI weboldalán található javaslatokkal.

Évek óta káros weboldalakkal fertőzhetők az iPhone készülékeket

(techcrunch.com)

A Google Project Zero által közzétett blogbejegyzésben egy olyan évek óta működő sérülékenységről számolnak be, amelynek kihasználásával a támadók teljes körű hozzáférést szerezhetnek az iPhone készülékekhez. A Google biztonsági kutatói számos olyan weboldalt fedeztek fel, amelyek az iPhone felhasználók meglátogatása során root jogosultságot szerző káros kóddal fertőzi meg az eszközöket. A legmagasabb hozzáférési jogosultsággal a támadóknak különböző egyéb rosszindulatú szoftver telepítésre van lehetőségük a felhasználók tudta és engedélye nélkül, aminek következtében a támadók hozzáférhetnek az eszközön tárolt képekhez, üzenetekhez, helyadatokhoz, mentett jelszavakhoz stb. **Bővebben...**

A Facebook „technikai hibát" fedezett fel a Messenger Kids alkalmazásb

(thenextweb.com)

A Messenger Kids alkalmazást a 13 évnél fiatalabb felhasználók számára vezette be a Facebook, annak érdekében, hogy a szülőknek ne kelljen attól tartaniuk, hogy gyerekeikkel idegenekkel lépnek kapcsolatba a csevegő alkalmazáson keresztül. Azonban 2019. június 12-én – 10 hónappal az alkalmazás megjelenését követően – egy olyan hibát azonosítottak az applikáció működésében, amely lehetővé tette a kiskorúak számára, hogy a csoportos beszélgetésekben felnőttekkel is kapcsolatba léphessenek szülői felügyelet nélkül. A média óriás hetekkel azután ismerte el a „technikai hibát", hogy Edward Markley és Richard Blumental amerikai demokratikus szenátorok felszólították a Facebookot, hogy gondolja újra és kezelje prioritásként a gyermekek online adatvédelmét és biztonságát. **Bővebben...**

Az oroszországi Tele2 megfigyeli előfizetőit

(www.ehackingnews.com)

Az élvonalban lévő Tele2, tartalomelosztó hálózaton (Content Delivery Network vagy Content Distribution Network – CDN) keresztül terjeszti rosszindulatú szkriptjeit, amellyel képes az Oroszországi ügyfelek által végzett tevékenységekről információt szerezni, mindezt természetesen a felhasználók tudta nélkül. Magát a kódot úgy fejlesztették, hogy az minél több hirdetést legyen képes megjeleníteni a weboldalon, továbbá a kód segítségével kulcsszavak is kiszámíthatók a célzott hirdetések kialakításához, amelyhez a szolgáltató http linkeket használ https helyett. Ezzel a módszerrel harmadik fél által nem csupán az ügyfelek tevékenysége monitorozható, hanem a weboldalon történő összes aktivitás figyelemmel kísérhető. **Bővebben...**

Adatokat szivárogtathatott az orosz SORM hardverberendezés

(www.zdnet.com)

Egy biztonsági kutató, Leonid Evdokimov augusztus 25-én a Chaos Constructions biztonsági konferencián ismertette, hogy az orosz SORM (System for Operative Investigative Activities) lehallgató berendezések közül néhány, felhasználói adatokat szivárogtatott ki, ugyanis az orosz hatóságok által az internetes forgalom lehallgatására szánt hardverberendezések az interneten tárolták az adatokat. Az orosz internet- és telekommunikációs szolgáltatóknak kötelező a SORM eszközök telepítése, a jogszabályoknak való megfelelés érdekében. **Bővebben...**