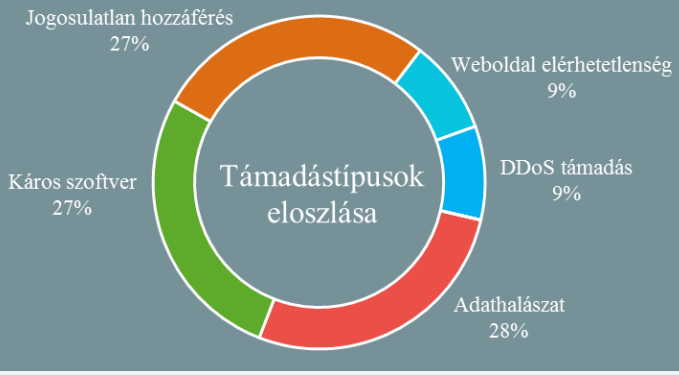
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 13. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.03.22. - 2019.03.28.



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

Újabb sérülékenységet fedeztek fel a svájci e-szavazórendszerben

(zdnet.com)

Biztonsági kutatók egy újabb sérülékenységet fedeztek fel a svájci online szavazórendszer (sVote) kapcsán, ami a kutatók szerint lehetőséget ad a szavazatok manipulálására. Minderre az ausztrál Új-Dél-Wales állam választási bizottsága (New South Wales Electoral Commission ─ NSWEC) közleményben reagált, amelynek apropóját az adja, hogy az NSWEC ugyanazt a rendszert használja, mint Svájc. Az NSWC nyilatkozata szerint ugyanakkor a szóban forgó sérülékenység az ő implementációjukat, az iVote-ot nem érinti. A kutatók szerencsésnek tartják, hogy az sVote nyilvános sérülékenységvizsgálata hozzájárul az iVote biztonságosabb működéséhez, azonban egyikük (Vanessa Teague) arra hívja fel a figyelmet, hogy az ausztrál jog e tekintetben jelentős korlátokat szab: a 2017-es Electoral Act alapján büntetendő a szavazórendszer technológiai hátterére vonatkozó információk nyilvánosságra hozása.

Visszafejthetők a HKCrypt zsarolóvírus által titkosított fájlok

(securityaffairs.co)

Az Emsisoft elérhetővé tett egy dekriptort, amely lehetővé teszi a Hacker Ransomware (HKCrypt) által titkosított fájlok visszafejtését. Az először 2017-ben felbukkant HKCrypto *.hacked* kiterjesztést ad az RC4 algoritmussal titkosított fájlokhoz, majd egy zsarolóüzenettel igyekszik rávenni áldozatait arra, hogy vegyék fel a kapcsolatot a támadókkal a megadott mail címen. A dekriptor és a hozzá tartozó felhasználó útmutató az Emsisoft weboldaláról ingyenesen beszerezhető. A letöltést követően rendszergazdai jogosultsággal kell elindítani a szoftvert, amely azután automatikusan megkeresi és visszafejti a titkosított fájlokat.

A LockerGoga jelenleg az egyik legaktívabb zsarolóvírus

(securityaffairs.co)

A Security Affairs arra hívja fel a figyelmet, hogy az e-mailen keresztül, fertőzött csatolmányként terjedő LockerGoga nevű zsarolóvírus komoly fenyegetést jelent a vállalkozásokra nézve. A MalwareHunterTeam által azonosított vírus amiatt került a figyelem középpontjába, hogy sikerrel okozott jelentős károkat előbb a francia Altran, majd a norvég Norsk Hydro vállalatóriásoknak.

Az SI-LAB szerint a ransomware-t egyes vírusirtó szoftverek (például a Microsoft Windows Defender) annak ellenére sem detektálják, hogy a malware 2019 januárja óta szedi áldozatait. **Bővebben...**

Gyakoriak a GitHub-on keresztül történő adatszivárgások a fejlesztők figyelmetlensége miatt

(nakedsecurity.sophos.com)

Az Észak-Karolinai Egyetem (NCSU) egyes kutatói átfogó vizsgálatnak vetették alá a legnépszerűbb online forráskód kezelő platformot, a GitHubot. Az ellenőrzés során megállapították, hogy arról nap mint nap több ezer, visszaélésre alkalmas hitelesítő adat (SSH kulcsok API tokenek, stb.) szivárog ki, amelyek komolyabb erőfeszítés nélkül visszakereshetőek. A probléma emberi mulasztásból fakad, a fejlesztők ugyanis gyakorta elkövetik azt a hibát, hogy a különböző online szolgáltatásokhoz ─ például Google, Twitter, Amazon Web Services, Facebook ─ használt hitelesítő kulcsaikat ugyanabban a könyvtárban tárolják, mint a Git repository-ba (tároló) feltöltendő kódot, amelyet ilyenformán véletlenül tesznek közzé egy-egy parancssorból indított feltöltés során. **Bővebben...**

Több, mint 500 millió felhasználó lehet veszélyben a UC Browser sérülékenysége miatt

(thehackernews.com)

Ismertté vált, hogy a kínai fejlesztésű – és különösen Ázsiában igen népszerű – UC Browser nevű webes böngésző egy olyan rejtett funkciót tartalmaz, ami lehetővé teszi, hogy a fejlesztő cég (UCWeb) bármikor új bővítményeket telepítsen a felhasználók androidos készülékeire, megsértve a Google Play Store – „Rosszindulatú viselkedés" szekció alatt részletezett – fejlesztői irányelveit. Az esetre fényt derítő biztonsági cég (Dr. Web) szerint ráadásul mindez nem a biztonságos HTTPS protokollon keresztül történik, ami így lehetőséget ad arra, hogy illetéktelenek a kommunikációba ékelődve (Man-in-the-Middle támadás) káros kódot juttassanak a készülékekre. A The Hacker News megkeresésére, az UCWeb szóvivője elárulta, hogy azóta frissítésre került az UC Browser alkalmazás a Google Playen.

IT biztonsági Tanács

Okoseszközök vásárlása előtt javasolt rákeresni a kiválasztott eszközre egy internetes kereső segítségével olyan kulcsszavakkal kiegészítve, mint a:
„security"/„biztonság",
„hack"/„kibertámadás",
vagy például a
„vulnerability"/ „sérülékenység".
Sok esetben az ilyen egyszerű módon fellelt információk is segíthetnek képet kapni az adott terméket érintő esetleges biztonsági kockázatról.

Szabályai miatt zárolta a hiszékeny felhasználók fiókjait a Twitter

(www.cnet.com)

A Twitter figyelmezteti felhasználóit egy, a platformján hétfő óta lánclevél szerűen keringő álhírre (hoax), amely „színesebb" hírfolyam-megjelenítést ígér azoknak a felhasználóknak, akik profiljukban átállítják a születési évüket 2007-re. A Twitter szabályai szerint viszont ez automatikus kitiltást jelent a közösségi oldalról, hiszen ezáltal a felhasználók életéve nem éri el a 13 éves korhatárt. Az érintett felhasználók - a Twitter csapatának segítségével - visszaszerezhetik hozzáférésüket a zárolt fiókokhoz, a bejelentkezést követően, az utasításokat követve kell módosítaniuk a hibásan megadott születési dátumot - árulta el a közösségi média szóvivője.

Ki állhat az ASUS hack mögött?

(databreachtoday.com)

A Kaspersky által a héten nyilvánosságra hozott, ASUS termékeket érintő malware támadás (Operation ShadowHammer) elkövetőiről még nem tudni semmi biztosat. Az orosz kiberbiztonsági cég elemzése szerint egyes jelek arra engednek következtetni, hogy a művelet kapcsolható a 2017-ben, a Microsoft által azonosított „BARIUM" APT csoport által bevetett „ShadowPad" nevű káros kódhoz. Ezt a Netsarang cég elleni támadás során alkalmazták, a módszer pedig nagyon hasonló volt: akkor is a frissítőszerverek kompromittálásával juttattak backdoort az áldozatok rendszereibe. A BARIUM nem egy új kollektíva. Egyes kutatók úgy vélik, hogy egy nagyobb – „Winniti Umbrellának" nevezett, de számos más néven is nyilvántartott (például „PassCV", „APT17", „Axiom", „Lead", „Wicked Panda", „Gref") kínai hírszerzéshez köthető szervezet tagja.

Újabb védelmi funkcióval bővül a Windows 10 következő kiadása

(www.bleepingcomputer.com)

A Microsoft bejelentette, hogy új funkcióval bővíti a Windows Defender ATP (Advanced Threat Protection) szolgáltatást, amelynek segítségével megakadályozható, hogy más alkalmazások módosításokat hajtsanak végre a kulcsfontosságú biztonsági funkciókon, úgymint a vírusirtó működésének letiltása, vagy a biztonsági frissítések törlése. A szabotázs-védelemmel (Tamper Protection) megakadályozható, hogy a rosszindulatú alkalmazások módosíthassák a Windows Defender víruskereső, a felhőalapú védelem és a zsarolóprogramok elleni (IOAV) védelem, valamint a gyanúsnak vagy rosszindulatúnak vélt aktív folyamatokat tiltó, valós idejű viselkedés-ellenőrző funkció beállításait. **Bővebben...**

Hatástalanítható a LockerGoga zsarolóvírus?

(securityweek.com)

Az Alert Logic szerint – legalábbis néhány variáns esetében – megelőzhető, hogy a LockerGoga zsarolóvírus titkosítsa a fájlokat. A kutatók felfedezték, hogy a vírus enkriptálás előtt átfésüli a merevlemezt, hogy egy listát készítsen azon fájlokról, amelyeket titkosítani fog. Amennyiben ennek során egy olyan .lnk kiterjesztésű (parancsikon) fájlra bukkan, amely érvénytelen hivatkozást tartalmaz, megszakítja a műveletet. Megjegyzendő, hogy ehhez a fájlnak a legutóbb megnyitott elemeket (Recent Items) tartalmazó könyvtárban kellett lennie. Mindemögött egy programozói mulasztás áll, ugyanis a malware készítői nem gondoskodtak az imént vázolt esetben fellépő hiba lekezeléséről. **Bővebben...**