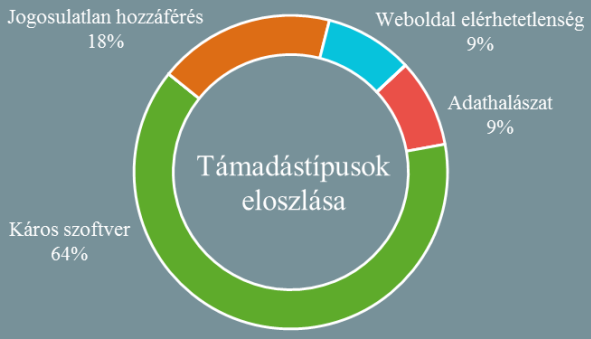
Nemzetközi IT-biztonsági sajtószemle

2019. 20. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.05.10. - 2019.05.16.



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

Több ezer weboldalról gyűjtöttek bankkártya adatokat

(www.zdnet.com)

Informatikai támadás érte a Picreelt, valamint az Alpaca Formot, amelyek célja az volt, hogy a nevezett cégek infrastruktúráján egyes fájlok kompromittálásával további weboldalakat fertőzzenek meg. Eddig ily módon már több, mint 4 600 weboldalra voltak képesek káros kódot juttatni. A Picreel web analitikai szolgáltatást nyújt, ami lehetőséget ad a weboldalak gazdáinak, hogy elemezzék a weboldalt meglátogatók aktivitását. Technikailag ez azt jelenti, hogy hogy a Picreeltől származó JavaScript kódot beágyazzák a saját oldalukba, a támadóknak pedig ezt a kódot sikerült módosítaniuk. Az Alpaca Forms ezzel szemben egy nyílt forrású platform, ami webes űrlapok létrehozását teszi lehetővé. A projekt eredetileg a Cloud CMS vállalat fejlesztésében indult, amely cég továbbra is CDN (tartalomelosztó hálózat) szolgáltatást nyújt a projektnek. A Cloud CMS vezérigazgatója szerint a hackerek ezen CDN-en voltak képesek egy JavaScript fájlt módosítani. A beültetett rosszindulatú kód naplózza az összes felhasználói aktivitást, valamint az űrlapmezők kitöltését, beleértve a bejelentkezési és fizetési adatokat, amelyeket egy Panamai kiszolgálónak továbbít. **Bővebben...**

Harcba száll az Amnesty a kémszoftverek ellen

(cyberscoop.com)

Emberi jogi aktivisták petíciót nyújtanak be egy izraeli bíróságon, az NSO-Group technológia-exportengedélyének visszavonásához, visszaélésekre hivatkozva. Ennek hátterében egy régóta elhúzódó vita áll a kémszoftver gyártó és jogvédő szervezetek között, ugyanis széleskörű vélemények szerint az izraeli cég termékeit számos országban az újságírók és a civil társadalom tagjainak megfigyelésére használják. Az Amnesty szerint a vállalat Pegasus nevű kémszoftverét például az Amnesty International egy kutatója ellen is alkalmazták már. **Bővebben...**

Újabb szög az SHA-1 koporsójába

(zdnet.com)

Francia és szingapúri kutatók tanulmányukban felvázolták az első olyan ütközéses támadást az SHA-1 titkosító algoritmus tekintetében, amelyhez szabadon megválasztható a prefix (chosen-prefix collision attack). Habár a Google már két éve publikálta az SHA-1 elleni első sikeres ütközést (SHAttered) — azaz két eltérő fájl esetében ugyanazon hash értéket előállítását — a mostani változat lényeges lépést jelent a gyakorlati alkalmazhatóság felé, azaz még erősebb bizonyíték az SHA-1 sérülékenységére. **Bővebben...**

Microsoft SharePoint elleni támadásokra figyelmeztetnek kanadai és szaúdi kiberügynökségek

(zdnet.com)

Hacker csoportok SharePoint szervereket támadnak egy kritikus sérülékenységet (CVE-2019-0604) kihasználva, a célpontok között vállalati és állami rendszerek is megtalálhatóak. A támadások közös nevezője, hogy a támadók a China Chopper nevű web shellt használták a sérülékeny szerverek kompromittálására, amellyel távoli hozzáférés szerezhető a célkeresztben álló rendszerhez. Ez ugyanakkor önmagában nem kellő bizonyíték arra vonatkozóan, hogy a támadások összefüggésben lennének egymással, a China Chopper ugyanis egy elterjedt káros szoftver, ami nem kötődik adott régióhoz. **Bővebben...**

Ellentmondásos az IPhone-ok biztonsága

(vice.com)

A napokban széles körben nyilvánosságot kapott egy WhatsApp sérülékenységet kihasználó exploit, amelyet felhasználva a számítógépes bűnözők képesek kémszoftvert telepíteni a mobiltelefonokra. Az esetre egy iPhone felhasználó megfigyelései nyomán derült fény, aki felvette a kapcsolatot a Citizen Lab nevű prominens biztonsági kutatócsoporttal. A WhatsApp fejlesztői rajtuk keresztül értesültek a biztonsági problémáról és rövid időn belül meg is szüntették a sérülékenységet. Az ügy rávilágít az iPhone-ok biztonságának ellentmondásos vonatkozásaira, ugyanis a szakértők szerint az iPhone-ok szigorúan zárt rendszere közel lehetetlenné teszi annak észlelését, hogy az eszközt feltörték, miközben több iOS-t érintő 0. napi (zero-day) sebezhetőség is ismert. **Bővebben...**

IT biztonsági Tanács

Egy amerikai kormányzati kiberügynökség ajánlásokat adott ki az elektronikus levelezés MS Office 365-re történő migrálása során a biztonságos konfiguráláshoz. Például felhívja a figyelmet arra, hogy a multifaktoros autentikáció az Azure Active Directory (AD) Global Administrator fiókokon nem alapértelmezett.

Mindehhez kapcsolódik egy másik ajánlás is, ami a fiók kompromittálást célzó (ATO) támadások egy gyakori típusa ellen nyújthat védelmet. Eszerint javasolt beállítani egy szabályt, hogy azon e-mailek, amelyek windows.net domain-re (azaz MS Azure Blob Storage-re) mutató linket tartalmaznak, generáljanak biztonsági figyelmeztetést.

Apple felhasználók helyadatait szivárogtatta ki a Twitter

(www.cyberscoop.com)

A Twitter bejelentése szerint egy biztonsági hiba következtében felhasználói helyadatokat gyűjtött és szivárogtatott ki egy hirdető partnercég számára. A probléma azon felhasználókat érintette, akik egynél több Twitter fiókot használnak ugyanazon iOS rendszeren. A közlemény szerint, bár a cég „szándékában állt" eltávolítani a helyzetre vonatkozó információkat az ún. real-time bidding, egyfajta a programozott vásárlás ─ azaz automatizált rendszerekkel történő reklámfelület értékesítés ─ során, azonban végül csak pontatlanabbá tette őket, így az információ egy irányítószámra vagy városra korlátozódott, 5 kilométeres pontossággal. **Bővebben…**

Orosz kormányzati portálok érzékeny személyes adatokat szivárogtatnak

(zdnet.com)

Több, mint 2,25 millió orosz állampolgár személyes és útlevél adatai szivárogtak ki, amit Ivan Begtin, az Informational Culture, egy orosz nonprofit szervezet társalapítója fedezett fel. Begtin blogján arról ír, hogy kormányzati tanúsító központokat, 50 állami portált, valamint egy kormányzati ügynökségek által üzemeltetett e-Bidding platformot átvizsgáló nyomozása során 23 site esetében találta úgy, hogy azok orosz társadalombiztosítási azonosítókat (SNILS), 14 weboldal pedig útlevél adatokat tett bárki számára hozzáférhetővé. Bár az érzékeny információk nem minden esetben voltak könnyen kinyerhetőek, némelyik egy egyszerű Google kereséssel felfedezhető volt. **Bővebben...**

Ismét ASUS szoftver frissítést használtak malware terjesztésre

(welivesecurity.com)

Az ESET szerint a BlackTech nevű kiberkémkedési csoport feltételezetten MitM (man-in-the-middle) támadásokat hajtott végre az ASUS WebStorage frissítési folyamata ellen, abból a célból, hogy backdoort (Plead) juttasson a célkeresztben álló ─ többségében kelet-ázsiai ─ rendszerekre. Jelenleg nem ismert, hogy a támadók pontosan milyen módszert alkalmaztak, azonban több forgatókönyv is elképzelhető: az egyik elképzelés szerint az ellátási láncot sikerült kompromittálniuk, a másik lehetséges szcenárió egy MitM támadás. Az ESET szerint ez utóbbi támadási mód a valószínűbb, eszerint a támadók képesek voltak az ASUS WebStorage HTTP kapcsolaton keresztül megvalósuló frissítési folyamatába ékelődni és a frissítés egy káros kódot tartalmazó, módosított verzióját továbbítani az áldozatoknak. **Bővebben...**

Tömegellenőrzés: jogvédők a légi utas-adatok tárolása ellen

(heise.de)

2018 májusa óta az Európai Unió valamennyi tagállama a légi forgalmat igénybe vevő utasok adatait öt éves időtartamú tárolás céljából kezeli, egyúttal összeveti biztonsági adatbázisok tartalmával. Az ellenzők szeretnék elérni ezen gyakorlat megszüntetését, különös tekintettel arra, hogy ezen adatok közül több is különleges adatnak minősül és álláspontjuk szerint ennek okán sérülnek a személyek adatvédelmi jogai. Az egyik német jogvédő szervezet (GFF) a wiesbadeni közigazgatási bírósághoz fordult a fentiek okán annak érdekében, hogy a légi-utasforgalom adatai ne kerüljenek automatikusan átadásra a szövetségi nyomozóhatóságnak (BKA) a normákban előírt – többek között terrorizmussal összefüggő – kiértékelés céljából. **Bővebben...**