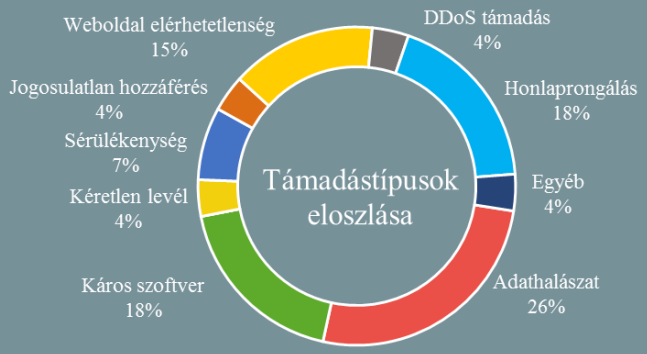
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.06.07. - 2019.06.13.



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

A legtöbb tartalomkezelő rendszer komoly biztonsági hiányosságokkal küzd

(zdnet.com)

A Pireuszi Egyetem kiterjedt kutatást végzett 49 népszerű webes tartalomkezelő rendszer (Content Management System – CMS), valamint 47 népszerű web alkalmazás keretrendszer bevonásával, elsősorban az alapértelmezett jelszókezelési mechanizmusokat vizsgálva. Ez az eljárás, amelynek során a felhasználó által megadott szabad szöveges jelszóból egy látszólag véletlenszerű karakterekből álló változatot konvertálnak, majd ez kerül tárolásra az eredeti jelszó helyett. A jelszó titkosítása általában három összetevőből áll: egy jelszó hash algoritmusból (hasítófüggvény), iterációs lépésekből, valamint egy „salt"-nak hívott véletlenszerű értékből, amelyet hozzáadnak a jelszóhoz, ezáltal nehezítve annak visszafejtését. Ezek közül a leginkább lényeges az algoritmus, amelynek több típusa is ismert, ezek közül azonban jó néhány már elavultnak számít, mint például az MD5, vagy az SHA-1. **Bővebben...**

Rengeteg célpontja van egy új botnet hálózatnak

(securityaffairs.co)

Egy új robothálózatot (Echobot) azonosított a Palo Alto Networks, amely a hírhedt Mirai botnet romjain jött létre. A botnet képességeit tekintve kifejezetten sokoldalúnak számít, ugyanis jelenleg már mintegy 26 exploittal bír, azaz ennyiféle rendszer vagy eszköz elleni kihasználási módot ismer. A legutóbbi variáns elsősorban hálózati útválasztókat (router), illetve hálózati hozzáféréssel rendelkező egyéb eszközöket (például NAS), IP kamerákat, vezeték nélküli prezentációs rendszereket, valamint VOIP telefonokat állít célkeresztbe. A szakértők szerint nem volt könnyű felderíteni a botnet által kihasznált sérülékenységeket, egyesek akkor még nem is rendelkeztek CVE (Common Vulnerabilities and Exposures) azonosítóval, de jó tíz éves is akadt közöttük. **Bővebben...**

Biztonsági hiba merült fel egyes Yubico termékeknél

(securityweek.com)

Egy kriptográfiai hiba miatt a Yubico kénytelen cserélni a **YubiKey FIPS** szériás biztonsági kulcsait. A felmerült probléma szerint a véletlen értékek tárolására szolgáló memória az áram alá helyezéskor elinduló öntesztelő folyamat után egy ideig olyan maradvány értékeket tartalmaz, amelyek csökkenthetik egyes kriptográfiai műveletek erősségét.

A biztonsági hiba a YubiKey FIPS **4.4.2**-es, valamint a **4.4.4**-es verziójú eszközöket érinti, beleértve a **Nano FIPS**, **C FIPS** és **C Nano FIPS** kulcsokat. A probléma a **4.4.5**-ös firmware verzióban javításra került, a cég pedig megkezdte az ügyfelek kiértesítését. Az ingyenes cseréhez egy dedikált oldalt is létrehoztak, amely innen érhető el. **Bővebben…**

DoS támadásra adhatnak lehetőséget a Linux és FreeBSD operációs rendszerek sérülékenységei

(www.heise.de)

Négy különböző hatású sérülékenységet fedezett fel a Netflix a Linux és a FreeBSD Unix-alapú operációs rendszereknél, amelyek közül a legnagyobb hatásfokkal a „SACK Panic" (CVE-2019-11477) elnevezésű biztonsági rés bír. A SACK Panic egy kernel hibaüzenet, amely távoli hozzáférés útján lehetővé teszi az operációs rendszer futásának megakadályozását, vagyis az érintett rendszer vonatkozásában szolgáltatás megtagadás (DoS) kondíciót eredményez. **Bővebben...**

A kétlépcsős azonosítást is megkerüli egy újonnan felfedezett androidos malware

(www.securityweek.com)

Az ESET egy elemzője, Lukas Stefanko olyan hitelesítő adatokat gyűjtő káros alkalmazásokat fedezett fel, amelyek újfajta módszerrel képesek az SMS-alapú kétfaktoros autentikáció megkerülésére, a Google által márciusban bevezetett hívásnaplóra és az alapértelmezett SMS-kezelőre vonatkozó korlátozásokat is kijátszva. Stefanko a felfedezést két olyan Android alkalmazás kapcsán tette, amelyek a török BtcTuk kriptovalutát bányászó applikációnak adják ki magukat („BTCTurk Pro Beta", illetve a „BtcTurk Pro Beta"). A káros alkalmazások indításkor hozzáférést kérnek az értesítésekhez, és amennyiben ezt a felhasználó jóváhagyja, egy hamis BtcTurk bejelentkezési oldalt jelenítenek meg a hitelesítő adatok megszerzéséhez. Ez önmagában még nem volna elegendő a kétfaktoros azonosítás miatt, ezért a támadók egy rendszerüzenetnek álcázott hamis hibaüzenetet jelenítenek meg, amelyben tájékoztatják a felhasználót, hogy az SMS ellenőrzési rendszerben végrehajtott változások miatt jelenleg nem érhető el a szolgáltatás mobileszközön. **Bővebben...**

IT biztonsági Tanács

Nyaralás alatt is érdemes kellő figyelmet fordítani digitális eszközeink és alkalmazásaink védelmére, valamint a biztonságtudatos magatartásra, ezért javasolt (legalább) az alábbiak szem előtt tartása:

Kapcsoljuk be a „Telefon keresése" funkciót és kerüljük a nyilvános Wi-Fi hálózatok használatát.

Ne osszuk meg tartózkodási helyünket a közösségi oldalakon.

További javaslatokat weboldalunkon **itt** talál.

Egy újabb adathalász kampány, ezúttal rendszerüzenetnek álcázva

(www.bleepingcomputer.com)

Egy jelenleg is aktív új adathalász kampány során egy ─ látszólag ─ az e-mail szolgáltatótól érkező rendszerüzenet arról tájékoztatja a felhasználókat, hogy egy titkosított üzenet érkezett, amely csak akkor olvasható el, ha a felhasználó bejelentkezik a OneDrive fiókjába. A levélben arra kérik az áldozatot, hogy kattintson az e-mail törzs részében található hivatkozásra, ami ezt követően egy hamisított OneDrive bejelentkezési felületre irányítja át a felhasználót. Az itt megadott felhasználói adatokat azután a támadók szabadon felhasználhatják rosszindulatú tevékenységeikhez. Jelen kampány kiváló példa arra nézve, hogy a felhasználóknak figyelmesnek kell lenniük a bejelentkezés során, ugyanis a kiberbűnözők újabb és újabb módszereket találnak ki a felhasználók megtévesztésére, azonban szerencsére a gyanús URL cím felhasználói szemmel is könnyen észrevehető.

Ügyféladatokat szereztek a Symantec-től

(theguardian.com)

A Symantec igyekszik kisebbíteni a jelentőségét annak az adatszivárgásnak, amelynek köszönhetően egy hacker jelszavakhoz, valamint egy Symantec szolgáltatásokat ─ például CloudSOC ─ használókat tartalmazó ügyféllistához fért hozzá. A listán kormányzati ügynökségek mellett az ausztrál szövetségi rendőrség, pénzintézetek, biztosítók, felsőoktatási intézmények és egyéb közintézmények szerepelnek. Az ausztrál adatvédelmi törvény (The Australian Privacy Act) bejelentési kötelezettséget ír elő minden esetben, amennyiben egy adatszivárgás valószínűsíthetően komoly károkat okoz az érintettekre nézve, a Symantec azonban a szóban forgó incidens kapcsán ezt elmulasztotta megtenni. **Bővebben...**

Véletlen szám generáló szolgáltatást indított a Cloudflare

(zdnet.com)

A Cloudflare elindította a League of Entropy nevű, véletlen számokat előállító szolgáltatását, amelyet vállalkozások, kormányügynökségek, vagy akár független fejlesztők is használhatnak inputként alkalmazásaik számára. A véletlen számok kritikus fontossággal bírnak a modern kriptográfia tekintetében. Amennyiben ezen értékek rosszindulatú szereplők által megjósolhatóvá válnak, az jelentősen hozzájárulhat a titkosítási kulcsok visszafejtéséhez. A szoftverek általában az adott eszközre hagyatkoznak ─ legyen az egy Android okostelefon, vagy éppen egy Linux szerver ─ az ilyen értékek előállításához. Az egyetlen forráson alapuló megoldások esetében azonban számolni kell azzal, hogy azok kompromittálása a véletlen értékek manipulálását eredményezheti. **Bővebben...**

Banki ügyfeleket céloz egy trójai programmal operáló új adathalász kampány

(securityaffairs.co)

A Cofense biztonsági szakértői egy új adathalász kampányra figyelmeztetnek, amelynek célpontjában kereskedelmi banki ügyfelek állnak. A támadó kampány során káros kóddal (WSH RAT) fertőzik az áldozat rendszerét, amely a Houdini számítógépes féreg (Worm) egy friss variánsa. A Remote Access Tool (RAT) típusú kártevők képesek az áldozat rendszereinek távoli vezérlésére, ez a variáns ráadásul hatástalanítja a vírusvédelmi megoldásokat, és a felhasználó fiók felügyeletet (UAC) is letiltja. **Bővebben...**