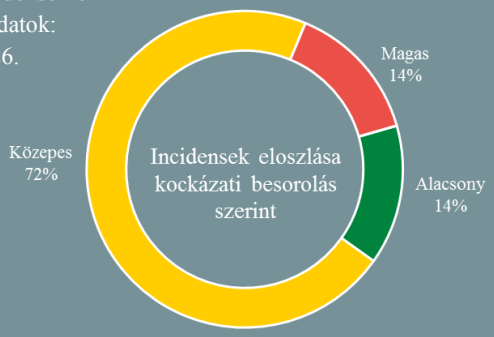
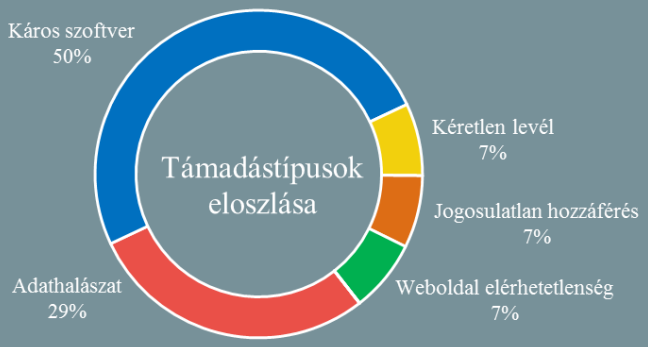
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.09.20. - 2019.09.26.





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

A Google csak Európán belül köteles eleget tenni „felejtés jogának”

(arstechnica.com)

Az Európai Unió Bírósága (EUB) kimondta: az Internetes kereső szolgáltatások nem kötelezhetők arra, hogy globálisan tegyék elérhetetlenné azon linkeket, amelyek törlését a felejtés joga alapján kérelmezték, hanem csupán az európai országokból. A felejtés joga ─ azaz hogy egy személyre vonatkozó információk az érintett kérésére törlésre kerüljenek a keresési találatok közül ─ évek óta vita tárgyát képezi az EU és a Google között. Az EUB 2014-es határozatának értelmében a keresőmotorok kötelesek megszüntetni a „nem megfelelő, nem vagy már nem releváns, illetve túlzó” tartalmakra mutató hivatkozásokat. A Google ennek engedelmeskedve az európai felhasználók számára elérhetővé tett egy online űrlapot, amin leadhatják a tartalomeltávolítási kérelmet, amelyből azóta több millió érkezett be, ezek közül végül 846 000-en hajtottak végre törlést. **Bővebben...**

A Google Alertet is felhasználhatják támadáshoz

(bleepingcomputer.com)

A BleepingComputer arra hívja fel a figyelmet, hogy támadók újabban a Google Értesítőt (Google Alert) is felhasználják, hogy rosszindulatú oldalakra irányítsák a felhasználókat. A Google Értesítő egy hasznos szolgáltatás, amelynek segítségével e-mail, vagy RSS értesítést kaphatunk az adott témakörökkel kapcsolatban a Google kereső által fellelt ─ indexelt ─ új tartalmakról, amelyhez kulcskifejezéseket kell megadnunk. Az utóbbi évben azonban egyre gyakoribbá vált, hogy a támadók úgy próbálnak meg fertőzött oldalakat fókuszba helyezni, hogy azokon gyakori kulcskifejezéseket helyeznek el, annak érdekében, hogy a Google keresője indexelje azokat, majd a felhasználóhoz beérkezzen a káros oldalra mutató értesítés. **Bővebben...**

Egyre több munkaállomás fertőződik Nodersok malware-rel

(zdnet.com)

A Nodersok (vagy a Cisco terminológiájában Divergent) nevű malware először idén nyáron ütötte fel a fejét, azóta pedig már több ezer Windows-os munkaállomást fertőzött meg káros reklámok segítségével. Ennek során egy HTA file töltődik le az áldozatok gépére, amely, ha futtatják, egy többlépéses fertőzési folyamatot indít el, aminek a végén a Nodersok települ a rendszerre. A káros kód azután a Microsoft szerint a fertőzött munkaállomásokat proxy-ként használja a káros forgalom továbbítására, a Cisco szerint azonban kattintásos csalás (click fraud) tevékenységbe kezd. A szakértők felhívják a figyelmet arra, hogy a kártevő még fejlesztés alatt áll, így képességeit bármikor bővíthetik, ami ─ tekintve az elterjedtségét ─ komoly aggodalomra ad okot. **Bővebben...**

A cseh hírszerzés szerint az országra Kína jelenti a legnagyobb kiberfenyegetést

(securityweek.com)

A cseh hírszerzés (NUKIB) 2018-as évet összefoglaló jelentése szerint nagy valószínűséggel kínai állami hackerek indítottak támadást tavaly Csehország egy kulcsfontosságú kormányzati szervezete ellen. Korábban csupán annyi volt ismert, hogy a cseh külügyminisztériumot informatikai támadás érte, azonban már az akkori közleményekben is felmerült, hogy egy idegen hatalom állhat az eset háttérben. A NUKIB jelentését a cseh kormány a jövő héten tárgyalja, a hírszerzés szóvivője szerint addig annak tartalmát nem hozzák nyilvánosságra. A fokozott orosz és kínai kémtevékenységre ugyanakkor már a 2017-es jelentésben is felhívták a figyelmet.

Tibeti vezetőket próbáltak kémszoftverrel fertőzni

(cyberscoop.com)

A Torontói Egyetem biztonsági kutatócsoportja, a Citizen Lab egy tibeti vezetők elleni kiberkémkedési kampányra derített fényt. 2018. november és 2019. május között magas beosztású tibeti tisztviselők, parlamenti képviselők, valamint a Dalai Láma közvetlen munkatársai álltak a mobiltelefonokat célzó Poison Carp malware kampány középpontjában. Ennek során a támadók magukat újságírónak, az Amnesty International kutatóinak és egyéb nonprofit szervezetek munkatársainak kiadva a WhatsApp alkalmazáson keresztül küldtek kémszoftver telepítésére szolgáló linkeket az áldozatoknak. A kísérletek egyike sem volt sikeres, és bár egy felhasználó jelentette a hivatkozás megnyitását, elegendő védelemnek bizonyult, hogy az eszközén a legfrissebb szoftverek futottak. A Citizen Lab Kínát tette felelőssé a támadásokért. **Bővebben...**

IT biztonsági Tanács

A támadók folyamatosan végeznek káros tevékenységeket a közösségi oldalakon is, annak reményében, hogy a felhasználók az ismerősök által ajánlott vagy tőlük érkező online tartalmakat nagyobb bizalommal és érdeklődéssel fogadják. Ezen elv mentén előfordulhat, hogy például a Facebook szolgáltatásain keresztül, egy általunk jól ismert felhasználótól kapunk egy káros weboldalra mutató hivatkozást, vagy egy fertőzött média fájlt.

Az ilyen és ehhez hasonló megkeresések esetén érdemes az NBSZ NKI weboldalán javasolt intézkedések szerint eljárni.

Ismét támadó kampány indult kelet-európai és közép-ázsiai külügyminisztériumok ellen

(cyberscoop.com)

Az ESET blogján közölt információkat az orosz állami hátterű Sednit (ismertebb nevén Fancy Bear, vagy Zebrocy) APT csoport legutóbbi, augusztus 20-án indult támadó kampányáról. Ennek során fertőzött csatolmánnyal rendelkező e-mailek érkeztek az áldozatokhoz, amelyek megnyitása után ─ több lépésben ─ egy backdoor (hátsó ajtó) települ a célrendszerre. Újdonság, hogy egyes letöltő modulok ezúttal Nim nyelven íródtak. A Kaspersky megfogalmazásában a Sednit „profilozási és hozzáférési specialistákból" áll, azaz fő feladata kezdeti hozzáférést szerezni az áldozathoz, majd a további műveletek elvégzéséhez átengedni a terepet más csoportok számára. Az orosz APT kollektívák közötti kollaboráció azonban a Checkpoint szerint ebben ki is merül, a műveletek során használt kódokat és toolokat például jellemzően nem osztják meg egymással, vélhetően azért, hogy ezzel is csökkentsék a detektálás valószínűségét.

Ki kicsoda az orosz kiberkémkedésben?

(thehackernews.com)

Oroszország egyike azon államoknak, akik elsőkként ismerték fel a kiberműveletekben rejlő lehetőségeket, az évtizedek során fejlesztett és csiszolt technikák segítségével pedig a kiberkémkedés mestereivé váltak. Olyan hírhedt incidensek kötődnek a nevükhöz, mint például az amerikai elnökválasztásba történő beavatkozás, egy ország ellen alkalmazott NotPetya zsarolóvírus, vagy az áramszünetet okozó, ukrán energiaszektor elleni támadás, ismertté téve a Fancy Bear, a Turla, a Cozy Bear, vagy például a Sandworm nevű hacker kollektívákat. A kiberháborús képességek nagyarányú fejlesztése az orosz APT csoportok ökoszisztémáját egy rendkívül komplex struktúrává tette, amelyben az összefüggések felismerése már igen komoly kihívást jelent, ezért az Intezer és a Check Point kutatói célul tűzték ki, hogy elősegítsék az orosz hacker műveletek értelmezését. **Bővebben...**

Microsoft Office 365 biztonsági ajánlások

(bleepingcomputer.com)

A finn kiberbiztonsági központ (NCSC-FI) egy részletes útmutatót adott közre a Microsoft Office 365 javasolt biztonsági beállításairól, amely elsősorban az adathalász támadások kivédésére fókuszál. Eszerint a legfontosabb az identitásvédelem biztosítása, ennek keretében pedig többek közt javasolt, hogy az adott vállalat minél inkább próbáljon egyedi login felületet kialakítani, követelje meg a nehezen törhető jelszavak használatát, engedélyezze a kétfaktoros azonosítást, valamint fordítson külön figyelmet a rendszergazdai jogok körültekintő kiosztására. A következő kategória az Office 365 e-mail fiókok biztosítása, ennek részeként például javasolt elutasítani minden olyan levelet, amely nem TLS kapcsolat felett érkezett, illetve a káros tartalmú e-mailek elleni védelem gyanánt alkalmazni az Office 365 Advanced Threat Protection-t. **Bővebben...**

Közel 5 millió felhasználói adat került nyilvánosságra a Door Dash adatszivárgásában

(securityaffairs.co)

A Door Dash nevű amerikai étel házhoz szállító cég megerősítette, hogy egy adatsértés következtében közel 5 millió felhasználó és kereskedő személyes adata szivárgott ki. Ezek között megtalálhatóak profil adatok, e-mail címek, kézbesítési címek, rendelési előzmények, telefonszámok. **Bővebben...**