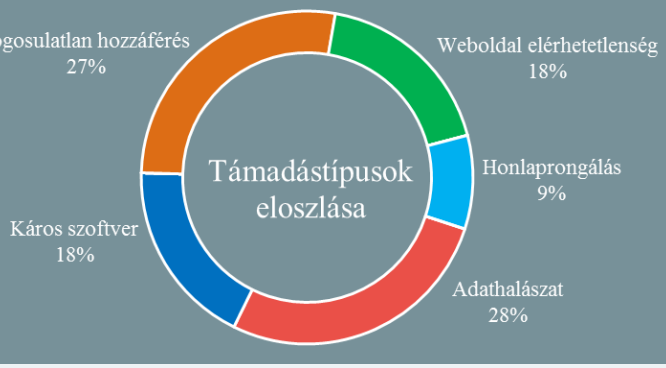
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.11.22. - 2019.11.28.



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

Az uniós tagállamok között nincs egyetértés az e-Privacy rendelet részleteivel kapcsolatban

(euractiv.com)

Átmenetileg megrekedtek a tárgyalások az EU azon törekvései kapcsán, amelyek a Facebook, a WhatsApp és a Microsoft Skype szolgáltatások számára a távközlési cégekkel azonos versenyfeltételek megteremtésére irányultak, miután a tagállamok a november 22-ei ülésen nem tudtak megegyezni a javasolt szabályok hatóköréről. Az Európai Bizottság két évvel ezelőtt nyújtotta be az e-Privacy rendeletre vonatkozó javaslatait, amely biztosítaná, hogy az online üzenetküldő és e-mail szolgáltatásokat nyújtó tech vállalatokra ugyanolyan szigorú szabályok vonatkozzanak, mint a távközlési szolgáltatókra. A tárgyalások során azonban olyan komplex témakörök merültek fel ─ mint például a nyomkövető sütik használata, gyermek pornográf tartalmak felderítése és törlése, hozzájárulási követelmények ─ amelyek kapcsán mindeddig nem született konszenzus. Egyelőre nem tisztázott a következő lépés, az egyeztetések folytatására a 2020. január 1-vel kezdődő horvát elnökség ideje alatt minden bizonnyal sor kerül majd.

Máris igen népszerű az eddigi legfejlettebb darkwebes keresőmotor

(securityweek.com)

A Kilos egy, a Google-hoz hasonló keresőmotor, azonban kifejezetten a darkwebes tartalmak felderítésére szakosodott. Korábban is léteztek ilyen szolgáltatások ─ például a Torch, a TorLinks, vagy az elődjének számító Grams ─ azonban az IntSights kiberfenyegetés felderítő cég egy szakembere szerint ezeknél fejlettebb keresőképességgel és szűrési lehetőségekkel rendelkezik. Többek közt beállítható akár az is, hogy csak olyan hirdetőket mutasson, akik a fizetést Bitcoinban, Litecoinban vagy Moneroban fogadják, vagy épp egy adott országba szállítanak. **Bővebben...**

Lényegesen nőtt a VPN alkalmazások használata világszerte

(zdnet.com)

A Top10VPN jelentése szerint az elmúlt 12 hónapban több, mint 480 milliószor töltöttek le mobil VPN alkalmazást a hivatalos Android és iOS app store-okból, ami a megelőző évhez képest mintegy 54%-kos növekedést jelent. A VPN alkalmazások népszerűsége az előző évhez képest az ázsiai és csendes-óceáni térségben (APAC) nőtt leginkább, ami nem meglepő, hiszen a térséget komoly politikai és társadalmi zavarok sújtották az elmúlt évben. Ebből a régióból egyébként a maga 75,5 milliós letöltésével Indonézia vezeti a listát. **Bővebben...**

A finn kormányzati szektor tudatosító képzésekkel veszi fel a harcot a kibertámadásokkal szemben

(ehackingnews.com)

A finn közintézmények az utóbbi időben napi szinten szenvednek el kibertámadásokat, legutóbb például több, mint 200 finn kormányzati szerv kapott zsarolólevelet egy titokzatos bűnözői csoporttól (#Tietovuoto321). A kibertámadások között a zsarolóvírusok kiemelt szereppel bírnak, ami világszerte komoly fenyegetést jelent a szervezetek számára. Mindez Finnországban olyan fokúvá vált, hogy a hatóságok a Pénzügyminisztérium irányítása alatt álló Népességnyilvántartási Központ szervezésében kiberbiztonsági képzést indítanak a közszféra intézményei számára, amelytől azt remélik, hogy hatékonyan hozzájárul az intézmények védekezési képességének növeléséhez.

Alkalmazásfejlesztői mulasztás miatt több ezer androidos app sérülékeny

(securityweek.com)

A Trend Micro szerint több ezer androidos alkalmazást érint egy GIF feldolgozási sérülékenység (CVE-2019-11932), amelyet nemrég a WhatsApp kapcsán fedeztek fel. A sérülékenység kihasználása egy káros kódot tartalmazó GIF fájl segítségével volt lehetséges, ahhoz azonban, hogy a fájl automatikusan letöltődjön a támadónak az áldozat kontakt listájában kellett lennie. A támadó ezt követően hozzáférhetett az áldozat eszközén tárolt fájlokhoz és a WhatsApp-os üzenetekhez, a távoli kódfuttatáshoz azonban már egy másik hiba kihasználása ─ vagy egy további káros alkalmazás megléte ─ volt szükséges. Ugyan a biztonsági probléma a csevegőprogram **2.19.244**-es verziójában orvoslásra került, azonban a hiba hátterében álló programkönyvtárat (libpl_droidsonroids_gif.so) továbbra is rengeteg applikáció használja. Csak a Google Play-en több, mint 3 000 ilyen alkalmazás található, a third party app store-okat nem is számolva.

IT biztonsági Tanács

Idén is elérkezett a Black Friday akció, amelynek során a kereskedők jellemzően komoly árkedvezményeket kínálnak a vásárlók számára. Ez alól az online webáruházak sem kivételek, azonban az ilyen nagy tömegű online vásárlásra buzdító kampányokat az internetes csalók is igyekeznek kihasználni.

Az NBSZ NKI ünnepi szezonra vonatkozó IT biztonsági tanácsai itt olvashatók, a Black Friday kampányok kockázataival kapcsolatban pedig itt találhat bővebb információt.

Visszakozik a Twitter

(bleepingcomputer.com)

A mikroblog eredeti tervei szerint decembertől megkezdte volna azon fiókok törlését, amelyekbe az elmúlt fél év során nem jelentkeztek be, elsősorban azért, hogy megelőzzék azok feltörését. A cég azonban most elismerte, hogy az elképzelés kapcsán nem készültek fel minden eshetőségre, például arra, hogy az elhunytak rokonsága számára lehetőséget biztosítsanak szerettük posztjainak megőrzésére, ami határozott ellenkezést váltott ki a felhasználókból. A Twitter ezért úgy döntött, addig elhalasztja a törlés megkezdését, amíg nem tudnak erre egy megfelelő megoldással szolgálni. Idő közben a non-profit Internet Archive jelezte, hogy szívesen nyújtana lehetőséget az eltávozottak Twitter fiókjainak archiválásában.

Több ezerben mérhető a zsarolóvírusok áldozataivá vált szervezetek száma

(bleepingcomputer.com)

A holland kiberbiztonsági központ (NCSC) figyelmeztetése szerint legalább 1 800 vállalat szenvedett zsarolóvírus támadást világszerte. A BleepingComputer ugyanakkor hozzáteszi, hogy ez vélhetően egy konzervatív becslés, ugyanis a szerevezetek sok esetben egyszerűen csak helyreállítják az adatokat, vagy kifizetik a váltságdíjat és nem jelentik az incidenst. A jelentés három ransomware-t nevez meg a legtöbb fertőzés okaként (LockerGoga, MegaCortex, és Ryuk), amelyek egyazon digitális infrastruktúrán osztoznak. Az NCSC az érintett cégek neveit nem hozta nyilvánosságra, csupán annyit tudni, hogy ezek jellemzően nagy ─ milliós, milliárdos árbevétellel rendelkező ─ szervezetek, különböző szektorokból, mint például az autó-, az építő-, vagy a vegyipar. Azt is tudni lehet, hogy legalább egy áldozat kritikus infrastruktúrák közül került ki, amely egy amerikai vegyipari cég holland leányvállalata.

Több webes termékét javította a Kaspersky

(securityweek.com)

Wladimir Palant biztonsági kutató még 2018 decemberében több sérülékenységről tájékoztatta a Kaspersky-t, amelyek a cég különböző védelmi termékeiben, a reklámok és nyomkövetők blokkolását végző funkcióival összefüggésben okoztak problémákat. Az érintett termékek az Anti-Virus, Internet Security, Total Security, Free Anti-Virus, Security Cloud, és a Small Office Security voltak. A cég idén júliusban értesítette a kutatót arról, hogy a hibák javításra kerültek, azonban Palant úgy találta, hogy a javítás valójában még rosszabbá is tette a helyzetet, ugyanis a sérülékenységek kihasználása a korábbi reklámblokkolás és nyomkövetés védelem megkerülése helyett már a kliensekre vonatkozó rendszer információk begyűjtését is lehetővé tette a meglátogatott weboldalak számára. A Kaspersky erre egy blog posztban reagált, amelyben kitartanak azon állításuk mellett, miszerint a sérülékenységek befoltozásra kerültek.

A Google nyilvánosságra hozta az állami támogatású hacker csoportokról gyűjtött információit

(securityweek.com)

Shane Huntley, a Google fenyegetés elemző csapatanának (TAG) egy munkatársa keddi blogbejegyzésében hozta nyilvánosságra az állami támogatású hackercsoportok által végzett kiberműveletekről, illetve dezinformációs kampányokról rendelkezésre álló statisztikai adataikat. Eszerint 2019 harmadik negyedévében a Google több, mint 12 000 ilyen támadási kísérletről küldött riasztást ügyfeleinek. A támadások 90%-a a felhasználók bejelentkezési adatainak megszerzésére irányult. **Bővebben...**