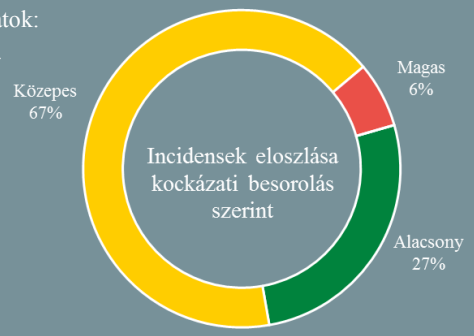
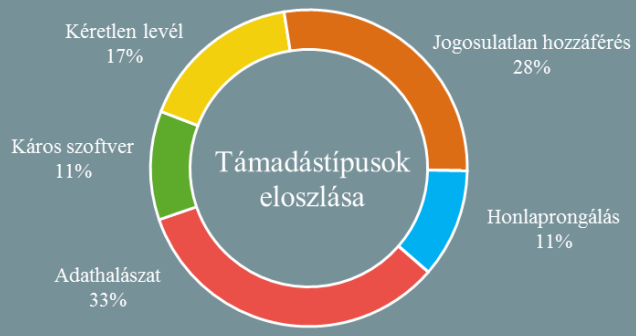
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.07.05. - 2019.07.11.





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

Így készül Kanada a 2019-es választások biztosítására

(cbc.ca)

Kanadai biztonsági szervek az idén esedékes szövetségi választásokkal kapcsolatban még nem tapasztaltak közvetlen fenyegetést, ám egyes kormánytisztviselők szerint az ellenséges külföldi szereplők már felkészültek a kampányba történő beavatkozásra. A szövetségi kormány már 2019. elején bejelentette, hogy létrehoz egy 5 fős belső csoportot, amelynek feladata a választások befolyásolására irányuló tevékenységek észlelése és a nyilvánosság tájékoztatása lesz. Vezető tisztségviselőktől származó információk szerint magas küszöbértéket tűztek ki annak kapcsán, hogy mely beavatkozási kísérletet hozzák majd nyilvánosságra, arra hivatkozva, hogy a túl gyakori figyelmeztetések is károsak lehetnek. A testület elsősorban a külföldi incidenseket vizsgálja majd, ám belföldi események kapcsán is határozhat úgy, hogy azok a választásokra nézve kockázatot hordoznak magukban. **Bővebben...**

Az Európai Unió 10 millió eurót szán kiberbiztonsági képességfejlesztésre

(ec.europa.eu)

Izrael Oroszországot vádolja a Ben Gurion reptéren tapasztalt GPS jelek forgalmában keletkezett zavarokért, a Kreml azonban tagadja a vádakat. Június elejétől többször is megszakadt a Ben Guiron reptér forgalmának GPS jelátvitele, amely bár nem okozott balesetet, mégis „jelentős hatást gyakorolt" a reptér működésére ─ állítja a reptéri hatóság. Az orosz izraeli nagykövet elmondása szerint Oroszország nem hajtott végre támadásokat a reptér ellen, a vádakat dezinformációnak titulálta, amelyeket szerinte nem lehet komolyan venni. A szakértők vizsgálatai alapján a GPS rendszerbe történő beavatkozás kizárólag a légtérben közlekedő gépek esetén okozott zavarokat, pontatlan helyadatokat eredményezve ─ derült ki a BBC cikkéből.

Fájlnélküli malware kampányra hívja fel a figyelmet a Microsoft

(thehackernews.com)

A Microsoft egy széleskörű malware támadási kampányra figyelmeztet, amelynek során egy ún. fájlnélküli vírussal (fileless malware) történik a fertőzés. A szóban forgó káros kód az Astaroth trójai, amely körülbelül 2017 óta van jelen, és képes különböző érzékeny adatok ellopására, billentyűzet leütések figyelésére. Az ilyen típusú kártevők futtatható állományok nélkül működnek, azaz a fájlrendszeren nem hagynak nyomot. A vírus terjesztése célzott adathalász levelekkel történik, amelyek egy hivatkozást tartalmaznak, ami egy .LNK kiterjesztésű fájlra (parancsikon) mutat. Amennyiben az áldozat erre rákattint, több legitim Windowsos rendszereszköz (WMIC, Bitsadmin) kompromittálásával meg is kezdődik az adatgyűjtés. **Bővebben...**

Kiterjesztett funkciókkal bírnak a hírhedt Finfisher kémprogram új verziói

(zdnet.com)

A Kaspersky a FinFisher (FinSpy) kémprogram új mobilos verzióit azonosította, amelyek kifejezetten Android és iOS rendszerű telefonok ellen készültek, és már 2018 óta aktívan használják is őket kiberkémkedési műveletek során, legutóbb például Mianmarban. A Gamma Group által készített szoftver új kiadásai kiterjesztett adatgyűjtési képességekkel bírnak: hozzáférnek az SMS/MMS üzenetekhez, e-mailekhez, a készülék GPS helyzetéhez, fényképekhez, naptár bejegyzésekhez, valamint a telefon memóriájában lévő adatokhoz is. Mindezek mellett képesek üzenetek és képek kinyerésére a népszerű csevegő programokból, valamint a telefonhívások rögzítésére. **Bővebben...**

Súlyos sérülékenységet azonosítottak az androidos Chrome böngészőben

(ehackingnews.com)

Egy, a Pwn2Own hacking konferencián nyilvánosságra hozott androidos Chrome kritikus sérülékenység lehetővé teszi, hogy bármely androidos eszköz felett át lehessen venni az irányítást. A támadóknak ehhez először rá kell bírniuk a felhasználót egy káros weboldal meglátogatására, ezt követően azonban tetszőleges applikációt képesek letölteni a készülékre, egyúttal teljes hozzáférést nyerve ahhoz. A Chrome böngésző JavaScript V8 motorját érintő biztonsági rés kihasználását a kutatók egy kerékpáros játék telepítésével demonstrálták. A Google állítólag értesült a hibáról, azonban a javítási szándékról még nem érkeztek hírek.

IT biztonsági Tanács

Az ausztrál kiberbiztonsági központ (Australian Cyber Security Centre - ACSC) frissítette az „Essential Eight Maturity Model” elnevezésű gyűjteményét, amely a szervezetek számára javasolt stratégiákat tartalmaz a kiberbiztonsági incidensek hatásainak enyhítésére.

A nyolc stratégia a következő: az alkalmazások fehérlistázása, az applikációk naprakészen tartása, megfelelő Microsoft Office makró beállítások hazsnálata, a felhasználói alkalmazások karbantartása, a rendszergazdai jogosultságok korlátozása, az operációs rendszerek naprakészen tartása, többfaktoros hitelesítés használata, valamint napi szintű biztonsági mentések készítése. A modell három fejlettségi szintet különböztet meg minden egyes stratégia esetében: részlegesen, többségében, valamint teljes mértékben megvalósított. Ezek közül az ACSC természetesen a harmadik szint elérését javasolja.

Letartóztattak egy bolgár biztonsági szakértőt egy óvodai szoftver sérülékenységének nyilvánosságra hozásáért

(ehackingnews.com)

Petko Petkovot azért tartóztatták le, mert június 25-én készített egy videót a helyi óvodákban használatos önkormányzati IT-rendszer sérülékenységének kihasználásáról, majd ezt nyilvánosan közzétette a Facebook-on. A videó azt mutatja be, hogyan támadja meg a helyi önkormányzat portálját, amelyen keresztül a szülők kérvényezhetik gyermekük felvételét az óvodába. A biztonsági szakértő, Stara Zagora város csaknem 236 000 lakosának személyes adatait tölthette le, emellett közzétett egy linket, a GitHub-ra feltöltött kihasználó kódhoz (PoC), amihez ezáltal bárki számára hozzáférést biztosított. **Bővebben...**

Malware támadás ért horvát kormányzati rendszereket

(zdnet.com)

2019 februárja és áprilisa között egy hacker csoport támadást indított horvát kormányzati intézmények ellen. A támadók ─ akikről feltételezik, hogy valamely nemzetállam támogatását élvezik ─ célzott adathalász e-maileket alkalmaztak, amelyek látszólag a horvát postaszolgálattól, illetve különböző kiskereskedelmi cégektől érkező szállítási értesítések voltak. Az e-mailek egy hiperhivatkozást tartalmaztak, amennyiben az áldozat erre rákattintott, egy Microsoft Excel dokumentum töltődött le. Az ebbe ágyazott makró szkript azután a dokumentum megnyitásakor további káros kódokat töltött le, amennyiben az automatikus makró futtatás engedélyezve volt az áldozat rendszerén. A szakemberek összesen kétféle malware-t azonosítottak a támadások során: az egyik az Empire backdoor, a másik pedig a SilentTrinity, amely szintén egy sérülékenység vizsgálók által alkalmazott program. **Bővebben...**

Hackerek kompromittálták a görög országkód szerinti TLD-ért felelős domain regisztrátort

(zdnet.com)

DNS eltérítéses támadás (DNS hijacking) érte Görögország .gr, valamint .el országkód szerinti legfelsőbb szintű tartományainak (country code top-level domain – ccTLD) kezeléséért felelős ICS-Forth-ot (Institute of Computer Science of the Foundation for Research and Technology). A szervezet nyilvánosan elismerte az incidens tényét, és e-mailben tájékoztatta a domain tulajdonosokat az esetről, még április 19-én. A támadást ahhoz a „Sea Turtle”-ként hivatkozott csoporthoz kötik, amely már korábban is végzett ilyen műveleteket. **Bővebben...**

Új funkciókkal lép fel az internetes zaklatók ellen az Instagram

(nakedsecurity.sophos.com)

Az Instagram bejelentette, hogy mesterséges intelligenciát (AI) alkalmaz a zaklatás-gyanús tartalmak felismerésére, és egy új funkció segítségével ─ a korábban riportált posztok alapján ─ figyelmeztetni fogja károsnak ítélt posztok íróit arra, hogy biztosak-e abban, hogy el szeretnék küldeni az üzenetet. Mindennek a hátterében az áll, hogy a fiatalok között igen népszerű közösségi platformon rendszeresek a zaklatások, amelyek egyes esetekben tragédiákhoz is vezethetnek. **Bővebben...**