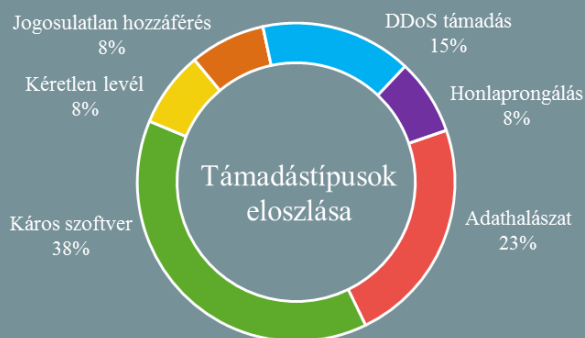


Az NKI által kezelt incidensekre
vonatkozó statisztikai adatok:
2019.04.26. - 2019.05.02.



Kövessen minket megújult [weboldalunkon](#), ahol friss IT-biztonsági hírek kerülnek publikálásra!

Hogyan veszélyezteti a dezinformáció az Európai Parlamenti választásokat? (heise.de)

Hamarosan körülbelül négyszáz millió európai választó polgár járulhat urnákhoz új parlamentet választani. Ennek okán felmerül egy sor kérdés: mennyire megbízhatóak a választások a mai korszakban, amit az álhírek (Fake News) uralnak; milyen felelősségük van ezzel összefüggésben a klasszikus médiáknak; a közösségi oldalak (Facebook, Twitter) milyen szerepet játszanak ebben a helyzetben. A félelem mindenestre nagy, hogy a digitális dezinformálás befolyásolhatja a szóban forgó választásokat. Az aggodalom pedig talán nem alaptalan, hiszen az amerikai választási kampánytól a Brexitig számos alkalommal felmerült ezen befolyásoló tényezők szerepének kérdése. Egyes szakértők szerint a jelenség túl van dimenzionálva, így az interneten keringő tartalmak hatása elhanyagolható a politikai események vonatkozásában, és valójában csak arra jók, hogy kommunikációs témát adjanak a közvélemény felé.

Bővebben...

Folyamatosan bővül az Electrumot célzó botnet (bleepingcomputer.com)

Immár 152 000 fertőzött gépből áll az a botnet hálózat, amellyel DDoS (túlterheléses) támadásokat hajtanak végre az Electrum szerverei ellen, az eddigi károkat körülbelül 4,6 millió dollárra becsülik. A támadásokat az ElectrumDoSMIner trójai végzi, amelyet a MalwareBytes Labs naponta átlagosan 2 000 fertőzött munkaállomásról távolít el, azonban még így is folyamatosan nő a botnet. A biztonsági kutatók most egy új loadert azonosítottak (Trojan.BeamWinHTTP), amellyel a támadók az ElectrumDoSMInert célba juttatják, azonban feltételezések szerint akár több száz további malware-t alkalmazhatnak e célból. A legtöbb fertőzött gép főképp az ázsiai–csendes-óceáni (APAC) térségben, illetve Dél-Amerikában található.

Céltzott kibertámadás érte az Amnesty Internationalt (www.zdnet.com)

Az Amnesty International 2019. március 15-én észlelte, hogy hongkongi képviselte ellen kibertámadást indítottak. A civil szervezet egy globális munkacsoportot állított fel a biztonsági esemény megakadályozására és kivizsgálására, amely megállapította, hogy az elkövetők egy jól ismert kínai állami kötődésű APT csoporthoz hasonló módszereket és technikákat (Tactics, Techniques and Procedures – TTP) alkalmaztak. Bár a támadást sikeresen elhárították, a vizsgálat lezárásáig nem közölnek bővebb információt arra vonatkozóan, hogy a támadás mely területet célozta és milyen feltételezett okból.



Bővebben...

Amennyiben telepítve van, sürgősen frissítse a Dell SupportAssist programot (thehackernews.com)

Egy kritikus távoli kódfuttatási sérülékenységet ([CVE-2019-3719](#)) fedeztek fel a Dell SupportAssist segédprogramban, amelynek kihasználásával átvehető az irányítás az adott rendszer felett. A program — amely a legtöbb Dell számítógépen előtelepített — feladata például az adott termék egyedi azonosítóinak (Service Tag, Express Service Code) felderítése, driver frissítések kezelése, valamint hardver diagnosztikai tesztek végzése. Mindez technikailag úgy történik, hogy a Dell SupportAssist a háttérben egy lokális webszervert indít az eszközön, ami különböző parancsokat vár URL paraméterben.

Bővebben...

Automatikusan törölhetők a Google által gyűjtött egyes felhasználói adatok (techcrunch.com)

Ismert, hogy a Google részletes információkat tárol a felhasználók tevékenységéről (például hely- és böngészési előzményeket). Az ilyen jellegű adatgyűjtést a felhasználók kikapcsolhatják készülékeiken, de ebben az esetben a Google szolgáltatásokat érintően egyes személyre szabási funkciók csorbát szenvedhetnek. A másik lehetőség eddig az volt, hogy a begyűjtött adatokat a felhasználók időközönként manuálisan törölték, azonban [most már beállítható](#), hogy a 3, vagy 18 hónapnál korábban tárolt adatok automatikusan törölődjenek a szerverekről. Ezzel a megoldással a személyre szabott ajánlatok továbbra is megérkeznek majd, azonban a Google korlátozottabb mennyiségben tárol majd adatokat a felhasználókról. **Bővebben...**

IT biztonsági Tanács



Május első csütörtökén ünnepeljük a **Jelszó világnapját** (World Password Day), amely idén május 2-ra esett. Ennek alkalmából érdemes **felülvizsgálatot tartani az általunk használt jelszavak megbízhatóságáról**.

Minden bejelentkezési felülethez használjunk **különböző**, lehetőleg **minél hosszabb** jelszavakat, és jó, ha ezek speciális karaktereket is tartalmaznak. A komplex jelszavak tárolása a legegyszerűbb módon **jelszószéffel** oldható meg. Amennyiben szükséges fejben tartanunk a jelszót, válaszszunk egy **több értelmes szóból álló mondatot**. Ahol csak lehet, alkalmazzunk többfaktoros hitelesítést, azonban lehetőleg ne SMS-en keresztül.

Állami kibertevékenységtől tart a Slack (motherboard.vice.com)

A Slack szerint a hagyományos kiberfenyegetések mellett a platform a szervezett kiberbűnözés, valamint az állami háttérű hacker tevékenység fókuszában áll. Mindez egy speciális dokumentumból (Form S-1 Registrartion Statement) derül ki, amelyet a cég az amerikai tőzsdére lépés miatt készített el. Ezekben a vállalatoknak kötelezően nyilvánosságra kell hozniuk a különböző céges adatok mellett a potenciális befektetői kockázatokat is. Azon elektronikus szolgáltatást nyújtó cégek, amelyek szintén ki szeretnének lépni a tőzsdére, és már érte őket kibertámadás (lásd: [Uber](#), [Lyft](#), [Pinterest](#), [Snapchat](#), [PagerDuty](#)) mind rendelkeznek egy külön szekcióval, amelyben a „jogosulatlan hozzáférés”-típusú támadásokat részletezik. A Slack egy 2015-ös adatszivárgást „vallott be”, amelynek során e-mail címek és hashelt jelszavak kompromittálódtak. **Bővebben...**

Biztonsági incidens a Docker Hubnál (bleepingcomputer.com)

Illetéktelenek hozzáfértek a Docker Hub egy adatbázisához, amely mintegy 190 000 felhasználó érzékeny adatait tartalmazta, köztük felhasználóneveket, jelszó hasheket, valamint külső Githubos és Bitbucketes tárolókhoz (repository) tartozó hozzáférési kulcsokat. A kompromittálódott adatok lehetővé tehetik harmadik fél számára, hogy hozzáférjenek az említett tárolókhoz és — jogosultságtól függően — módosítsák az azokban található kódokat, majd az automatikus build funkción keresztül a Docker lemezképet. A BleepingComputer arra hívja fel a figyelmet, hogy egy ilyen támadás végső soron ellátási-lánc elleni támadások (supply chain attack) kivitelezésére adhat módot. A Docker 2019. április 25-én értesült az incidensről. **Bővebben...**

Vigyázzon ezzel a weboldallal, fertőzött PC tisztító szoftvert terjeszt! (bleepingcomputer.com)

Biztonsági kutatók felfedeztek egy malware terjesztő weboldalt (gcleaner[] info), amely olyan windowsos PC tisztító szoftvert reklámoz (G-Cleaner, vagy Garbage Cleaner), amely megtévesztő módon legitim tisztító szoftvernek adja ki magát, azonban valójában egy jelszólopó trójai programot takar (AZORult). Amint ez telepítésre kerül, igyekszik megszerezni a felhasználó böngészőjében és FTP kliensében lementett jelszavait, valamint hozzáférni különféle érzékeny adatokhoz, mint például a kriptovaluta pénztárcákhoz. Habár a káros oldal már egy hónapja ismertté vált, a BleepingComputer publikációjának elkészültekor továbbra is elérhető volt. A cikk írója kiemeli, hogy a felhasználóknak egy-egy program letöltése előtt javasolt leinformálni az adott weboldalt — például felhasználói visszajelzések után kutatni — valamint a szoftvereket telepítés előtt feltölteni a VirusTotalra, hogy megbizonyosodjanak annak megbízhatóságáról.

15 nap alatt kell majd telepíteni a kritikus frissítéseket az amerikai kormányzati rendszereken (thehackernews.com)

Az elmúlt évek során többször szembesülhettünk azzal, hogy a hackerek kíméletlenül lecsapnak azon rendszerekre, ahol a biztonsági frissítések telepítése nem, vagy nem rendszeresen történik. Az Egyesült Államok Belbiztonsági Minisztériuma (United States Department of Homeland Security – DHS) emiatt elrendelte, hogy a kormányzati ügynökségek gyakrabban telepítsék a kritikus kockázati besorolású sérülékenységeket befolytózó hibajavításokat az interneten keresztül hozzáférhető rendszerek tekintetében. **Bővebben...**