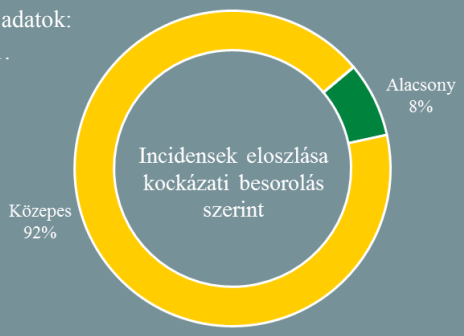
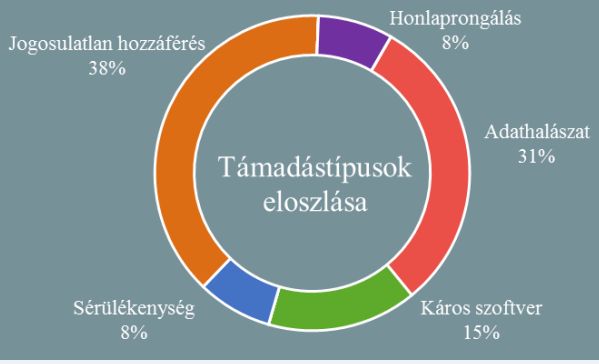
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 08. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.02.15. - 2019.02.21.





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

Németország felajánlja kiberarzenálját a NATO tagok számára

(securityweek.com)

Németország védelmi minisztere bejelentette, hogy csatlakoznak azon államok köréhez ─ mint például az Egyesült Államok, Nagy Britannia, Dánia, Hollandia és Észtország ─ amelyek felajánlják offenzív kiber képességeiket a NATO szövetség számára, a hagyományos haderőnemeket kiegészítendő. A nyilvános kommunikáció nem titkolt célja az ellenséges nemzetek elrettentése, különösen annak figyelembevételével, hogy az Észak-atlanti Szövetség egyre nagyobb összegeket fordít az informatikai hadviselésre. Minderre jó példa, hogy csak az Egyesült Királyság idén 65 millió fontot szán e feladatra.

Nyilvánosságra hozták az új norvég kiberbiztonsági stratégiát

(www.enisa.europa.eu)

2019. január 30-án került publikálásra Norvégia új nemzeti kiberbiztonsági stratégiája, amelynek fókuszában a norvég társadalom digitalizálásával kapcsolatban felmerülő kihívások kezelése áll, emellett a korábbiakhoz képest nagyobb szerepet kapott a köz- és magánszféra közötti, valamint a polgári-katonai, illetve a nemzetközi együttműködés támogatása. A stratégiában megfogalmazott célok teljesítéséhez 1,6 milliárd norvég korona (körülbelül 160 millió euró) összegű költségvetést biztosítanak.

Sorozatban kínál eladásra lopott fiókadatokat egy hacker

(zdnet.com)

A Gnosticplayers álnevet használó hacker (vagy kollektíva) rövid idő alatt harmadik alkalommal kínál lopott fiókadatokat a darknetes Dream Marketen; első alkalommal közel 620, a következőben 127, ezúttal pedig összesen 92,76 millió fiókadat vált ily módon megvásárolhatóvá. A mostani gyűjteményben nyolc cég adatbázisa található, ezek közül a legnagyobb név a GfyCat, egy népszerű GIF megosztó platform. **Bővebben...**

Új mérési szempont a hackerek képességeinek összehasonlításához

(wired.com)

A legtöbb informatikai támadás utáni post mortem elemzés elsősorban a kezdeti támadási vektort helyezi fókuszba, azonban Dmitri Alperovitch, a CrowdStrike műszaki vezérigazgatója szerint ennél sokkal lényegesebb a támadás következő fázisa, azaz amikor a támadók megpróbálnak további node-okat elérni a hálózaton, vagy magasabb jogosultsághoz jutni. **Bővebben...**

Komoly kémkedési vádak kereszttüzében a Huawei

(zdnet.com)

A The Information publikációja szerint a Huawei rendszeresen próbált ipari titkokat szerezni az Apple-től. A kérdéses ─ anonim forrásokra hivatkozó ─ cikk állítása szerint a tech óriás elsősorban kínai Apple-ös beszállítókat környékezett meg, de arra is volt példa, hogy a tajvani Foxconn gyártósori munkásaitól próbált információkat szerezni, például az amerikai cég új okosórájában használt pulzusmérő technológiáról, vagy épp a MacBook Pro csatlakozó kábeléről. **Bővebben...**

Elérhető az alapértelmezett inkognitó mód az iOS-es Firefoxon

(www.bleepingcomputer.com)

A Mozilla bejelentette az alapértelmezett privát böngészési mód beállításának lehetőségét az iOS-es Firefoxon, amelynek használatával ─ a könyvjelzők közé mentett új weboldalak kivételével ─ nem kerülnek tárolásra böngészési adatok. Az iOS Firefox 15.0 emellett további funkciókat ad hozzá a privát böngésző módhoz, például egyszerűbbé vált a normál módba történő váltás, a böngésző bezárása után is megmaradnak a megnyitott tab-ok, illetve egyénileg beállíthatóvá vált, hogy egy új böngészőablak megnyitásakor mi jelenjen meg: könyvjelzők, üres oldal, Firefox kezdőoldal, vagy a felhasználó által megadott URL.

IT biztonsági Tanács

A mobil készülékek rendkívül sok személyes adatot tárolnak a felhasználókról, többek közt potenciálisan fényképeket, videókat, jelszavakat, e-maileket, SMS-eket. Éppen ezért leselejtezés előtt fontos biztonságosan törölnünk a készüléket, amit legkönnyebben a gyári beállításokra történő visszaállítással tehetünk meg. Mindezt attól függetlenül érdemes elvégeznünk, hogy milyen módon szabadulunk meg a berendezéstől (elajándékozás, eldobás, stb.)

A készülék mellett további fontos teendő az eltávolítható memóriakártyá(k)ról és a SIM kártyá(k)ról történő gondoskodás, azaz amennyiben az újrafelhasználhatóság nem megoldott, ajánlott azok megsemmisítése.

Több millió egészségügyi segélyhívás hanganyaga szivárgott ki a svéd vészhívótól

(thenextweb.com)

A Computer Swaden tech portál információi szerint a 1177 Vårdguiden (Svédország egészségügyi segélyhívójának) egy alvállalkozója, a thaiföldi Medicall mintegy 2,7 millió vészhívás hangfelvételeit tárolta titkosítatlan formában, egy hitelesítés nélkül nyíltan bárki számára elérhető szerveren. A szóban forgó hívások a Computer Swaden szerint rendkívül szenzitív információkat tartalmaznak a betegekről, mint például a betegségek tünetei, kórelőzmények, gyógyszeres kezelések, társadalombiztosítási számok. Mindezek mellett ráadásul 57 000 telefonszám is megtalálható az adatbázisban, ami lényegesen megkönnyítheti a betegek beazonosítását. **Bővebben...**

Ukrajna az EU-val közösen készül a kiberfenyegetések kezelésére

(www.bleepingcomputer.com)

A közeljövőben Ukrajna több közös gyakorlatot is szervez az Európai Unióval, amelyek célja az orosz számítógépes fenyegetésekkel szembeni megfelelő reagálási modellek kialakítása. Az ukrán Nemzetbiztonsági és Védelmi Tanács (NSDC) rendelkezésére álló információk szerint ugyanis Oroszország minden valószínűség szerint teljes arzenálját ─ beleértve a kibernetikus eszközöket is ─ beveti majd a március 31-én esedékes ukrán elnökválasztás befolyásolására, nyilatkozta Oleksandr Turchinov, az NSDC titkára.

Ingyenes „threat intel” eszközt ad közre a Kaspersky

(securityweek.com)

A Kaspersky CyberTrace egy ingyenes fenyegetés felderítő (threat intelligence) szoftver, amellyel az orosz IT-biztonsági cég segítséget szeretne nyújtani a vállalkozások számára. A program naprakész védelmet ígér azáltal, hogy összegyűjti a különböző forrásokból érkező fenyegetési információkat, amelyeket összevet a cég infrastruktúráján működő SIEM (biztonsági információ- és eseménykezelő) szoftver által azonosított eseményekkel. A Kaspersky CyberTrace a SIEM megoldások széles körével integrálható, mint például az IBM QRadar, a Splunk, az ArcSight ESM, a LogRhythm, az RSA NetWitness, valamint a McAfee ESM. A Kaspersky mindemellett ─ évek óta először ─ pénzügyi mutatókat is közölt, ezek pedig az Észak-amerikai piacon történő visszaesés ellenére is stabil növekedést jeleznek.

Sérülékenységeket fedeztek fel több népszerű jelszókezelő program kapcsán

(zdnet.com)

Az Independent Security Evaluators (ISE) tanulmányában egyes népszerű jelszókezelő programok (1Password, Dashlane, KeePass, LastPass) valós biztonsági szintjéről szeretne hiteles képet adni. Vizsgálatuk során kiderült, a szoftvereket több sérülékenység is sújtja, a 1Password 4-es verzió esetében például felfedezték, hogy bizonyos körülmények között a széfet nyitó mester jelszó szabad szöveges formában hozzáférhető a RAM-ban, ráadásul úgy, hogy a jelszószéf eközben zárolt állapotban van. Habár az összes vizsgált programról kijelenthető, hogy nem képesek a hirdetésükben szereplő védelmi szintet nyújtani ügyfeleik számára, a ZDNet szerint ezzel együtt javasolt a használatuk, mivel hiányuk lényegesen nagyobb kitettséget jelent a jelszótörő támadásokkal szemben. **Bővebben...**