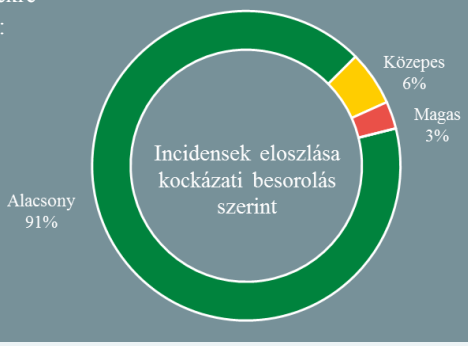
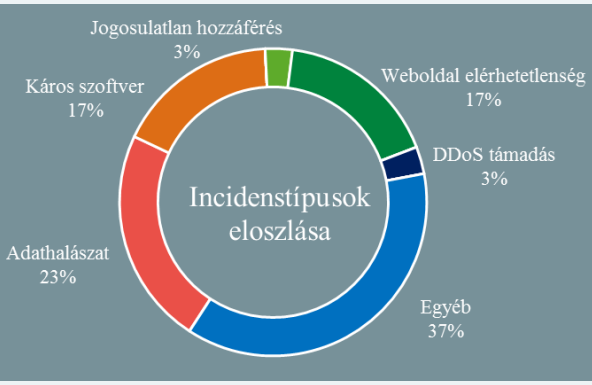
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 26. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.06.25. - 2021.07.01.





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

Anonimitást veszélyeztető javítást kapott a Tor böngésző, ellenőrizze a verziót!

(securityaffairs.co)

A Tor böngésző **10.0.18**-as verziójában javításra került az a hiba, amely lehetővé tette a felhasználók nyomon követését a telepített alkalmazások „ujjlenyomatának" (jellemzőinek) rögzítésével. A FingerprintJS szakértői egy új módszert fedeztek fel, amelyet sémaáradásnak (scheme flooding) neveztek el. Ez lehetővé teszi a felhasználók azonosítását, miközben különböző asztali böngészőket (Safarit, Chrome-ot, Firefox-ot és akár Tort) használnak. A módszerrel támadók képesek lehetnek akár a Tor böngészőt használók profilozására is. **Bővebben...**

A Google biztonsági szigorításokat vezet be androidos alkalmazásfejlesztők számára

(thehackernews.com)

A Google friss bejelentése szerint új biztonsági előírásokat vezet be a Play Áruházon regisztrált fejlesztői fiókok tekintetében, úgy mint a kétfaktoros azonosítást (2FA), és a fejlesztők által megadott elérhetőségek ellenőrzését. A Google Play Trust and Safety csapatának elmondása szerint a 2FA nem csupán a felhasználói fiókok biztonságához járul majd hozzá, hanem az alkalmazásbolt biztonságára nézve is fontos lépés. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán a kalózszoftverekkel kapcsolatos kockázatokról olvashat bővebb információkat.

Nyomkövetés-mentes keresőmotorral állt elő a Brave

(bleepingcomputer.com)

Egyelőre ugyan csak béta verzióban, de elérhetővé vált a Brave böngésző új, adatvédelemre fókuszáló keresőmotorja (Brave Search), amely alternatívát kíván nyújtani a hatalmas mennyiségű felhasználói adatot gyűjtő tech óriások ─ mint a Google és a Microsoft ─ keresőmotorjaival szemben. A **Brave Search** legfőbb jellemzői, hogy nem gyűjt adatot a felhasználók böngészéseiről, nem profilozza a felhasználókat, saját keresési indexet használ, és mindezt transzparensen teszi, azaz nincs titkos algoritmus, ami befolyásolja a keresési találatokat. **Bővebben...**

Szinte az összes LinkedIn felhasználó adatát árulják egy hacker fórumon

(securityaffairs.co)

A RestorePrivacy weboldal szerint kiberbűnözők a LinkedIn hivatalos API-jával visszaélve 700 millió felhasználó adatát töltötték le sikeresen, majd a szenzitív információkat egy hacker fórumon kínálták eladásra. A LinkedIn összesen 756 millió felhasználóval rendelkezik, így az adatsértésben a felhasználók több, mint 92%-a érintett. A kiszivárogott adatok között a felhasználók neve, neme, e-mail címe, fizikai címe, földrajzi helyzete, felhasználóneve, szakmai tapasztalataira vonatkozó információk, további közösségi oldalaik elérhetőségei és a LinkedIn profiljukhoz tartozó URL címe is megtalálható. **Bővebben...**

Másodjára sikerült csak javítani a SonicWall eszközöket érintő kritikus hibát

(thehackernews.com)

Egy már javítottnak vélt biztonsági hibát fedeztek fel Sonicwall készülékekben ─ köztük fizikai és virtuális tűzfalakban ─ amely a SonicOS különböző verzióit érinti. A CVE-2021-20019 (első alkalommal CVE-2020-5135) azonosítóval ellátott hiba egy memóriaszivárgás (memory leak) következménye, amely egy speciálisan szerkesztett HTTP kérés útján használható ki, amelynek során illetéktelenek távolról kényes információkhoz férhetnek hozzá. **Bővebben…**