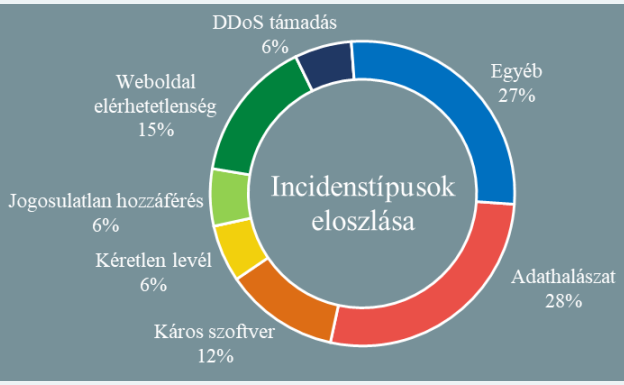
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2022. 17. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2022.04.22. - 2022.04.28.



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

Az FBI figyelmeztet: világszerte fenyegetést jelent a BlackCat zsarolóvírus

(securityaffairs.co)

Az Egyesült Államok Szövetségi Nyomozó Irodája (FBI) figyelmeztetést adott ki a **BlackCat** zsarolóvírusról, amelynek a tavaly novemberi megjelenése óta, 2022 márciusáig mintegy 60 szervezet esett áldozatául világszerte. Az FBI által közzétett gyorsjelentés részletezi a BlackCat RaaS (Ransomware as a Service) támadásokhoz kapcsolódó kompromittáltság *indikátorokat* (indicators of compromise – IoCs), technikai részletek árul el a zsarolóvírusról, valamint javaslatokat fogalmaz meg, amelyekkel mérsékelhető a támadások bekövetkezésének valószínűsége. **Bővebben...**

Új adatvédelmi funkciót kap a Play Store, erre lehet számítani

(bleepingcomputer.com)

Az adatvédelmi újítások harmadik szakaszában arra is lehet majd számítani, hogy az alkalmazásoknál feltüntetésre kerülnek az összegyűjtött adatok védelmére alkalmazott biztonsági mechanizmusok, mint a MASVS szabvány. Ebben a szakaszban például az is tisztázásra kerül, hogy a felhasználók kérhetik adataik törlését, továbbá a gyermekek védelme érdekében az is látható lesz majd, hogy az adott alkalmazás megfelel-e a Google Play Families irányelveknek. **Bővebben...**

IT biztonsági Tanács

Az Anyák napja közeledtével az NBSZ NKI weboldalán arról olvashatunk bővebben, hogy miként járulhatunk hozzá szüleink online biztonságához.

A Lapsus$ új áldozata a T-Mobile

(bleepingcomputer.com)

Az amerikai T-Mobile elismerte, hogy a Lapsus$ kiberbűnözői csoport hetekkel ezelőtt lopott hitelesítőadatokkal hozzáfért a cég belsős rendszereihez. A telekommunikációs óriás szerint sikerült megszüntetniük a hackerek hozzáférését, elmondásuk szerint az incidens során ügyfél és kormányzati adatok nem kompromittálódtak. *„Rendszereink és folyamataink a terveknek megfelelően működtek, a behatolást gyorsan leállítottuk, a felhasznált feltört hitelesítő adatokat pedig letiltottuk."* **Bővebben...**

Legalább száz Lenovo laptop modellt érintő UEFI firmware hibákra derült fény

(bleepingcomputer.com)

A Lenovo három biztonsági hibáról adott ki gyártói közleményt, amelyek közül kettő (CVE-2021-3971, CVE-2021-3972) lehetőséget teremt arra, hogy a támadó kikapcsolja az **UEFI Secure Bootot**, ami biztosítja, hogy a boot folyamat során csak a gyártó által megbízhatónak tartott kód töltődhessen be. A harmadik hiba (CVE-2021-3970) egy helyi támadó számára tetszőleges kód emelt jogosultsággal történő futtatására ad lehetőséget. A biztonsági hibákat felfedező ESET a sérülékenységekről egy bővebb technikai elemzést is közzétett. **Bővebben...**

Antivírus sandboxokhoz lehetett hozzáférni a VirusTotalon keresztül

(thehackernews.com)

A CVE-2021-22204 számon nyomon követett súlyos kockázati besorolású sérülékenység kihasználása távoli kódfuttatását tett lehetővé a VirusTotalon. A hibát a 2021. április 13-án kiadott biztonsági frissítéssel javították. A VirusTotal egy ingyenes szolgáltatás, ami lehetővé teszi, hogy annak webes felületén keresztül több, mint 70 antivírus szolgáltató malware adatbázisát használhassuk egy-egy gyanús fáj, vagy weboldal ellenőrzésére. **Bővebben...**