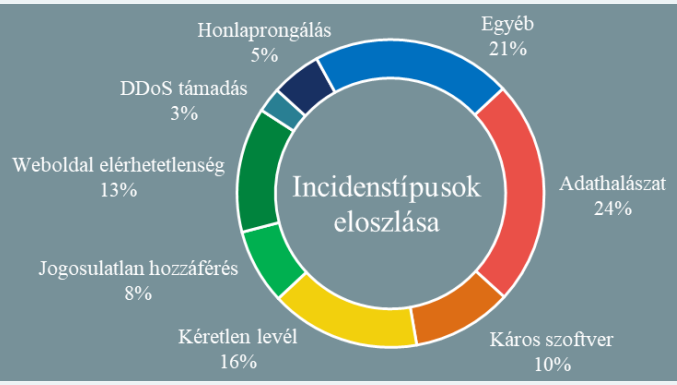
Nemzetközi IT-biztonsági sajtószemle

2022. 04. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2022.01.21. - 2022.01.27.



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

PowerPoint fájlokkal is terjesztik a távoli hozzáférést biztosító trójaiakat

(bleepingcomputer.com)

A Netskope's Threat Labs által közzé tett jelentés szerint 2021 decembere óta olyan újfajta adathalász módszer figyelhető meg, amelyben a kiberbűnözők nem csak adatokat lopnak, hanem PowerPoint fájlokat használnak olyan trójaiak terjesztésére, amelyekkel távoli hozzáférést szerezhetnek a felhasználó eszközei felett. A nyomon követett kampányban két RAT-ot (Remote Access Trojan) azonosítottak, a Warzone-t és az AgentTesla-t. A rosszindulatú PowerPoint adathalász melléklet obfuszkált makrót tartalmaz, amelyet a PowerShell és az MSHTA kombinációjával hajtanak végre. **Bővebben...**

Komoly biztonsági hiba érintette a Google kamera alkalmazását

(heise.de)

A heise.de jelentése súlyos, QR-kódokat érintő biztonsági hibákra hívta fel a Google figyelmét, amely több mobil készüléket is érint, többek között az Android 11 és 12 rendszerű Pixel mobiltelefonokat és egyes OnePlus készülékeket.

A sérülékenység lényege, hogy a Google Android Pixel telefonokon használt kameraalkalmazás meghamisítja a QR-kódokból származó http(s) hivatkozásokat. **Bővebben...**

Veszélyes hibát fedeztek fel, amivel hackerek root jogot szerezhetnek Linux rendszereken

(bleepingcomputer.com)

A Qualys kutatói tavaly novemberben egy súlyos biztonsági hibát azonosítottak a linuxos **polkit** nevű autorizációs keretrendszer **pkexec** alkalmazásában, ami minden nagy Linux disztribúcióban alapértelmezetten megtalálható. A hiba root szintű jogosultság-kiterjesztést tesz lehetővé, azaz a támadó egy már kompromittált rendszert teljesen az irányítása alá vonhat. A CVE-2021-4034 azonosítójú sebezhetőségre **PwnKit**-ként is hivatkoznak. **Bővebben...**

Több, mint 90 WordPress téma és plugin tartalmazott backdoort

(bleepingcomputer.com)

A WordPress pluginokban rejlő biztonsági kockázatra hívja fel a figyelmet a Jetpack. Jelentésük szerint az AccessPress cég által fejlesztett ─ többségében ingyenes ─ mintegy 40 WordPress téma és 53 kiegészítő (plugin) tartalmazott olyan káros PHP kódot, ami lényegében hátsó ajtót nyitott azokhoz a WordPress oldalakhoz, amelyekre telepítésre kerültek. **Bővebben...**

Kibertámadás a Nobel-díj átadásakor

(thehackernews.com)

A Nobel Alapítvány és a Norvég Nobel Intézet nyilvánosságra hozta, hogy 2021. december 10-én, a díjátadó élő közvetítése alatt elosztott szolgáltatás-megtagadással járó támadás (DDoS) érte weboldalaikat. A hivatalos közlemény szerint a kibertámadás rendkívül nagy terhelésnek tette ki azokat a webhelyeket, amelyeken a Nobel-díjjal és a Nobel-díjasok eredményeivel kapcsolatos új információkat teszik közzé. **Bővebben...**

Biztonságosabb lesz a dokumentumszerkesztés a Google Drive-ban

(bleepingcomputer.com)

A Google mostantól figyelmezteti a Google Drive felhasználókat a potenciálisan gyanús fájlok megnyitásáról, így remélhetőleg mérsékelve az adathalász támadások, valamint a káros programok terjesztésének lehetőségét. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán az elfeledett felhasználói fiókokról és azok kezeléséről olvashat bővebben.