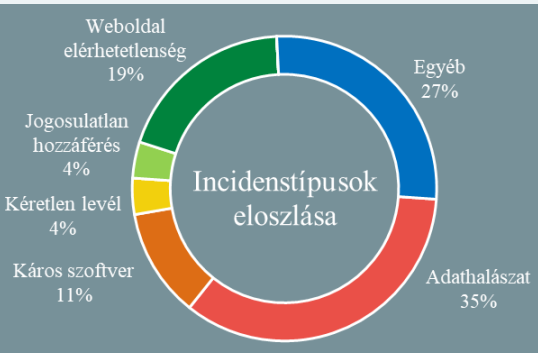
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2022. 16. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2022.04.14. - 2022.04.21.



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

Ezt a márkát használják jelenleg a legtöbb adathalász támadásnál

(bleepingcomputer.com)

A LinkedIn nemcsak az üzleti életben népszerű, a Check Point kutatói szerint a közösségi platform megszemélyesítésével véghezvitt kibertámadások száma jelentősen megnőtt az elmúlt időszakban. A kiberbűnözők leggyakrabban megtévesztő üzenetek és hamis weboldalak segítségével jutnak érzékeny adatokhoz (jelszavak, bankkártya adatok, stb.). A LinkedIn az előző negyedévében (2021 Q4) még csupán az ötödik volt a támadásokhoz leggyakrabban használt márkák listáján, 2022 Q1 során azonban már a megszemélyesítéses támadások 52%-a LinkedIn témájú volt. **Bővebben...**

Sérülékeny codec miatt az androidos felhasználók kétharmada volt kockázatnak kitéve

(bleepingcomputer.com)

A Check Point fedezte fel, hogy a Qualcomm és MediaTek processzorral ellátott androidos eszközök az Apple Lossless Audio Codec (ALAC) implementálási hibái folytán lehetőséget adtak távoli kódfuttatásra, ráadásul egyes hibák viszonylag egyszerű kihasználást tettek lehetővé. Az ALAC egy hangkódolási formátum, amit az Apple dolgozott ki, azonban 2011-ben nyílt forráskódúvá tett. A cég azóta már több biztonsági hibajavítást is kiadott hozzá, azonban ezeket nem minden gyártó alkalmazza — mint kiderült a telefonos chipgyártó piac két vezető szereplője a Qualcomm, és a MediaTek sem. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán az 5 leggyakoribb jelszavak elleni támadási módszerről olvashat.

Vigyázat, befektetési csalás!

(nki.gov.hu)

A **befektetési csalások** számában jelentős növekedés figyelhető meg a korábbi évekhez képest. Az FBI IC3 2021-es évre vonatkozó jelentése szerint az utóbbi évben főleg a **kriptovalutákba történő befektetés** vált a befektetési csalások fő témájává. Sajnos ez a csalási forma hazánkban is megjelent, jelen összefoglaló a **Dakken Group** (**hxxps://dakkengroup[.]com**) által elkövetett csalásokra szeretné felhívni a figyelmet, amelyről az NBSZ NKI-hez több bejelentés is érkezett. A csalók esetenként akár több millió forinttal is megkárosíthatják az áldozatokat, az alábbiakban az erről a csalásról rendelkezésre álló információkat tesszük közzé. **Bővebben...**

Hiába a februári javítás, máig kihasználják a Windows Print Spooler egy súlyos hibáját

(bleepingcomputer.com)

Az Egyesült Államok Kiberbiztonsági és Infrastruktúra-biztonsági Ügynöksége (CISA) újabb **három sérülékenységgel** bővítette az aktívan kihasználható sebezhetőségek listáját, az egyik közülük, rendkívül súlyos. A CVE-2022-22718 számon nyomon követhető biztonsági rés a Windows összes verzióját érinti, kihasználásával pedig lokálisan – felhasználói beavatkozás nélkül – kiterjeszthető a jogosultsági szint a célzott rendszeren. **Bővebben...**

Kritikus hibát javítottak az Elementor WordPress kiegészítőben

(securityweek.com)

Az Elementor az egyik legnépszerűbb bővítmény — több, mint 5 milliós letöltéssel rendelkezik — WodPress oldalak létrehozására, mivel rendkívül egyszerű a használata, drag-and-drop technikával gyakorlatilag néhány perc alatt „összedobálhatunk” magunknak egy WP oldalt. A plugin kapcsán azonban egy olyan sebezhetőséget fedeztek fel, amelynek sikeres kihasználásával egy támadó teljesen az irányítása alá vonhatja a sérülékeny oldalt. **Bővebben...**