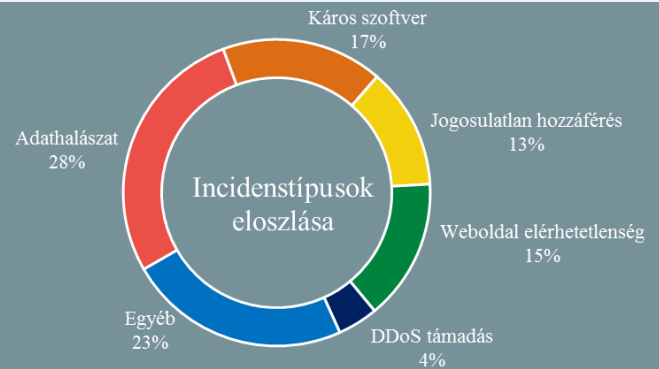


Az NKI által kezelt incidensekre  
vonatkozó statisztikai adatok:  
2021.02.05. - 2021.02.11.



Kövessen minket megújult [weboldalunkon](#), ahol friss IT-biztonsági hírek kerülnek publikálásra!

## Újabb adathalászmódszer, ezúttal morzejelel titkosítják a rosszindulatú csatolmányokat (bleepingcomputer.com)

Újfajta adathalászmódszer ad hírt a BleepingComputer, miszerint a támadók morzejelekkel rejtik el a rosszindulatú URL-eket, hogy megkerüljék a levélszűrőket. A támadás egy adathalászmódszerrel történik, amely mellékletében tartalmaz egy HTML fájlt, ami látszólag egy számlalevél. (A fájl neve e-mailenként változó lehet a következő séma szerint: „[cégnév]\_számla\_[szám].\_xlsx.html”.) A mellékletet szövegszerkesztővel megnyitva, látható az abban elhelyezett JavaScript kód, amelyben a betűket és a számokat morzejelekkel kódolták – így például az „a” betű helyett „.-” szerepel. **Bővebben...**




## Android felhasználók, figyelem: malware-t találtak egy népszerű vonalkódolvasó alkalmazásban

(bleepingcomputer.com)

A Google törölte a Play Store-ról a LAVABIRD népszerű alkalmazását, a Barcode Scannert, miután a Malwarebytes biztonsági kutatói káros kódot fedeztek fel benne. A több, mint 10 milliós letöltéssel bíró app évekig problémamentesen működött, azonban a 2020 decemberi frissítés után sokan furcsa viselkedésre lettek figyelmesek, például böngészőjük magától elindulva rosszindulatú alkalmazásokat reklámozó hirdetéseket jelenített meg. **Bővebben...**

## IT biztonsági Tanács

A közeledő Valentin-nap  alkalmából ezen a héten a biztonságtudatos online ismerkedésről olvashatnak az NBSZ NKI [weboldalán](#).

## Kiberdiplomáciai workshopot tartott Észtország

(cyberscoop.com)

Az észt külügyminisztérium szervezésében harmadik alkalommal került megrendezésre a kibertámadások diplomáciai vonatkozású kérdéseire választ kereső workshop. Ennek során többek közt áttekintésre kerültek a közelmúlt mérföldkönek számító kibertámadások – mint például a WannaCry vagy a NotPetya –, amelyek ráirányították a figyelmet a kibertámadások stratégiai szintű kezelésének szükségességére. Habár az Egyesült Nemzetek Szervezete 2015-ben [ajánlást adott ki](#) a nemzetállamok számára a kibertérben tanúsított felelős magatartásról, ez az elmúlt évek tapasztalatai alapján nem vált a gyakorlat alapjává. **Bővebben...**

## Hackerok megpróbálták megmérgezni egy floridai kisváros ivóvízkészletét

(securityaffairs.co)

A floridai Oldsmar város vízügyi rendszereit kibertámadás érte, amelynek során a támadó többször is megkísérelte veszélyes mértékben – több, mint százszorosára – megemelni az ivóvíz nátrium-hidroxid (NaOH) tartalmát. (A kémiai vegyületet kis koncentrációban a víz savasságának szinten tartásához használják, ám nagyobb dózisban egészségkárosító hatású.) Szerencsére a létesítmény egy operátora észlelte a módosítást és korrigálta az értéket. Mint kiderült, az illetéktelen hozzáférés elsősorban azért nem szűrt szemet számára, mivel gyakorta előfordul, hogy felettese távolról bejelentkezik a rendszerre. **Bővebben...**

## Kritikus böngészőhibák célkeresztben

(securityweek.com)

A Google múlt héten soron kívüli javítást adott ki egy kritikus nulladik napi Chrome [hibához](#), amelyről jelenleg annyi ismert, hogy azt támadók aktívan ki is használják. A böngésző V8 JavaScript motorját érintő sérülékenységről a tech óriás addig nem közöl több információt, amíg a patchet nem telepítették elegendően. Kérdéses, hogy a hiba köthető-e a nemrég ismertté vált, IT-biztonsági kutatókat célzó támadókampanyhoz, amit a hírhedt észak-koreai Lazarus csoportnak tulajdonítanak. **Bővebben...**