

# WEEKLY CYBER NEWS



## Espresso mellé (1-3 perces)

**Hackerek válnak más hackerek célpontjává. [Egyes hackerek más hackereket céloznak meg egy hamis OnlyFans eszközzel, amely elvileg segít a fiókok ellopásában, azonban ehelyett megfertőzi a potenciális támadókat a Lumma Stealer malware-rel.](#)**

**3 dolog, amit soha ne csinálj a mobiloddal a repülőtéren. A repülőtéren lenni izgalmas időtöltés, azonban a nyaralási pörgés sok utazót arra készíthet, hogy megfeledkezzen az óvatosságról. [Carolyn Pearson utazási biztonsági szakértő három módszert fedett fel, amellyel az utazók biztonságban tarthatják mobileszközeiket a repülőtéren.](#)**

**79 oka van, hogy azonnal rácsapjon a frissítés gombra a Windowsban. [Számptalan hibát foltozott be a Microsoft a támogatott Windows 10 és 11 rendszerekben, valamint az egyéb szoftverekben.](#)**

**Quishing: QR fenyegetés az elektromos autók számára. [A 'quishing' egy olyan adathalász típusú támadás, ahol a csalók QR kódokat használnak arra, hogy megtevésszék a felhasználókat, és érzékeny információkat szerezzenek meg ezáltal.](#)**

**440 GB adatot loptak el a világ egyik legnagyobb kiberbiztonsági vállalatától. Egy illegális hackerfórumon tette elérhetővé valaki azokat az adatokat, amiket a Fortinet nevű kiberbiztonsági cég egyik Azure-szerveréről szerzett. [A vállalat szerint csak kevés ügyfél érintett az esetben.](#)**

**Zero-day sérülékenységet javítottak az Adobe Acrobat Readerben. [Egy kiberbiztonsági kutató arra figyelmezteti a felhasználókat, hogy frissítsék az Adobe Acrobat Readert, miután 2024.09.12-én kiadtak egy javítást egy távoli kódfuttatást lehetővé tevő zero-day sérülékenységre, amelyhez már elérhető egy PoC exploit.](#)**

**A Veeam a Backup & Replication szoftver kritikus RCE hibájára figyelmeztet. A Veeam 2024. szeptemberében számos termékéhez adott ki biztonsági frissítést, amellyel a Veeam Backup & Replication, a Service Provider Console és ONE szoftvercsomagok 18 súlyos és kritikus hibáját kezeli. [A kezelt problémák közül a legsúlyosabb a CVE-2024-40711, amely a Veeam Backup & Replication \(VBR\) kritikus \(CVSS v3.1 pontszám: 9.8\) távoli kódfuttatást \(RCE\) lehetővé tevő sebezhetősége, amely hitelesítés nélkül is kihasználható.](#)**

## **[Feliratkozom az új hírcsatornára!](#)**

\* A Weekly Cyber News csatornára külön feliratkozás szükséges, kérünk, a gomb megnyomásával jelezd erre irányuló szándékodat! Köszönjük!