CYBERSECURITY
maxvalor
Heimdal™ Security Alliance Partner

28. hét

# WEEKLY CYBER NEWS


## **Espresso mellé** (1-3 perces)

**Hatékony módszerek tömeges jelszó visszaállításra kiberbiztonsági incidensek során.** A Microsoft Incident Response gyakran javasolja kiberbiztonsági incidensek során a tömeges jelszó-visszaállítást, mellyel fiókjainkat visszaszerezhetjük és megszakíthatjuk a támadók által létrehozott perzisztenciát. Azonban a nagyobb szervezeteknél a tömeges jelszó-visszaállítások koordinálása összetett feladat lehet. Ebben a bejegyzésben bemutatjuk ennek kihívásait, és azt, hogy lehet felkészülni rá a gyakorlatban.

**142 hibát javít a Windowsok júliusi frissítése – ebből 4 súlyos.** Érdemes azonnal telepíteni a Microsoft által kiadott valamennyi frissítést, ugyanis egy sor súlyos hibát javítottak a Windowsokban és számos más programban.

**Tervezési hibát találtak a RADIUS protokollban.** Veszélyben minden hálózat. A sérülékenység kihasználásával megkerülhető a multifaktoros hitelesítés, és közbeékelődéses támadás hajtható végre. Minden eszköz veszélyeztetett, amelyik a protokollt használja.

**A kiberbiztonsági ügynökségek az apt40 támadásaira figyelmeztetnek.** Ausztrália, Kanada, Németország, Japán, Új-Zéland, Dél-Korea, az Egyesült Királyság és az Egyesült Államok kiberbiztonsági szervei közös tanácsadást adtak ki az APT40 nevű, Kínához köthető kiberkémkedő csoportról, amelyben arra figyelmeztetnek, hogy a csoport az újonnan nyilvánosságra hozott biztonsági hibákat képes a nyilvánosságra hozatalt követő órákon vagy napokon belül kihasználni.

**Újfajta kibertámadás terjed, hívásokkal zaklatják az embert, amíg nem fizet.** Az új módszer úgy indul, mint egy szokványos zsarolóvírus-támadás, ám a sikeres titkosítás után jön csak a java: telefonon kezdik zaklatni a célpontot egészen addig, amíg el nem érik, amit akarnak.

**Javított a Microsoft egy súlyos hibát a Windows 11-ben.** Javítja a lefagyó, esetenként eltűnő tálca problémáját a Windows 11 legújabb frissítése. Mutatjuk, hogyan telepítheti, ha önnél is használhatatlan az egyik legfontosabb rendszerelem.

**Rekord szivárogtatás: 10 milliárd jelszót osztottak meg a hackerek.** A RockYou.txt szólista egy 2009-es támadásból származik. A névadó RockYou – egy közösségi alkalmazás- és hirdetési hálózat – pusztító kibertámadást szenvedett el, amelynek következtében több mint 32 millió felhasználó jelszava került nyilvánosságra. Mivel a jelszavakat egyszerű szöveges formában tárolták, a támadók könnyű prédájává váltak. Az összeállítást azóta is bővítik.

## Feliratkozom az új hírcsatornára!

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