TLP: WHITE
Szabadon terjeszthető!

Rendkívüli tájékoztató
Dharma zsarolóvírus terjesztésről

(2019.03.21.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet rendkívüli **tájékoztató**t ad ki **Dharma** nevű **zsarolóvírus terjedésével kapcsolatban**. A zsarolóvírus különböző országok üzleti és állami szférában működő szervezeteinek informatikai hálózatait támadja meg.

A Dharma Ransomware a távoli asztal elérést biztosító protokoll (RDP) biztonsági hibáit kihasználva jut be a sértettek informatikai rendszerébe, és fertőzi meg azt, amely következtében a gyakori kiterjesztéssel rendelkező fájlokat (dokumentum, táblázat, képek) titkosítja, és megakadályozza a hozzáférést, amíg az áldozat a meghatározott összegű Bitcoin váltságdíjat a zsaroló által megadott Bitcoin tárcába (számla) el nem küldi.

A zsarolóvírus támadás kockázatának csökkentése érdekében az NBSZ NKI az alábbi intézkedéseket javasolja:

- **Nyitott portok felülvizsgálata,** a szükségtelen portok bezárása, a szükséges portok fokozott felügyelete, naplózása.
- A **gyakori portok** internet irányából történő **elérésének korlátozása** (megadott IP címekről, bizonyos felhasználók számára).
- **Üzemeltetéshez használt portok** (SSH, RDP, Telnet, LDAP, NTP, SMB, stb.) **külső hálózatból történő elérésének tiltása**, üzemeltetési feladatok ellátásához javasolt a rendszerek VPN kapcsolaton keresztül történő elérése.
- **Határvédelmi rendszerek szoftvereinek naprakészen tartása.**
- **Határvédelmi eszközök feketelistájának frissítése** (több gyártó rendelkezik nyilvánosan elérhető listákkal pl.: Cisco), ezáltal csökkentve a támadás kockázatát.
- A **szükségtelen felhasználók felfüggesztése**, a távoli eléréssel rendelkező felhasználók szükséges mértékre történő csökkentése, **felhasználók jogosultságainak időszakos felülvizsgálata**.
- **Jelszavak kötelező periodikus cseréje, szigorú jelszóházirend alkalmazása mellett.**
- Rendszeres online és **offline** (szalagos egység, külső merevlemez) **biztonsági mentés**, archiválás.

Biztonsági incidens bekövetkezése esetén az NBSZ NKI javasolja:

- Az érintett eszköz **hálózatról** történő **leválasztás**át.
- Az érintett adathordozók helyreállítása előtt **bitazonos másolat készítését.**
- **Incidens bejelentését** az NBSZ NKI részére a cert@govcert.hu e-mail címen.

Az esettel kapcsolatos további információk:

- https://www.fortinet.com/blog/threat-research/dharma-ransomware--what-it-s-teaching-us.html
- https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-15th-2019-stop-decryptors-and-more/

Kérjük, továbbítsa a tájékoztatót a háttérintézményei felé.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@govcert.hu