TLP:WHITE
Szabadon terjeszthető!

Riasztás
DeadBolt zsarolóvírus terjedéséről
(2022. február 07.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **riasztást** ad ki a **DeadBolt ransomware terjedésével kapcsolatban**. Az NBSZ NKI tapasztalatai alapján a zsarolóvírus terjedése az elmúlt időszakban fokozódó jelenlétet mutat. A hazai és nemzetközi partnerektől származó információk alapján a zsarolóvírus elsődleges célpontjai a **QNAP** által gyártott **NAS eszközök**.

A QNAP NAS-okat célzó DeadBolt zsarolóvírus támadások a legtöbb esetben

- **nyitott**, vagy nem biztonságos **távoli asztali kapcsolaton keresztül** (RDP, TCP/UDP 3389-es alapértelmezett port);
- vagy **adathalász e-mailek** segítségével történnek.

A sikeres támadások megelőzése érdekében ─ kiemelt figyelemmel a távoli asztali elérést biztosító szolgáltatásokra ─ az NBSZ NKI az alábbi kockázatcsökkentő / megelőző intézkedések mihamarabbi megtételét javasolja:

- A NAS felügyeleti szolgáltatás **Port Forwarding** funkció **tiltása** (alapértelmezés szerint a 8080-as és a 443-as port).
- A myQNAPcloud menüjében, az „**Auto Router Configuration**” menüpontban „**Enable UPnP Port forwarding**” jelölőnégyzetének törlése.
- A NAS-on használt szoftverek mielőbbi **frissítése** a legújabb verziókra.
- Felhasználói **fiókok zárolására vonatkozó házirend kialakítása.**
- **Megfelelő biztonsági mentési és visszaállítási stratégia kidolgozása.**
- **Katasztrófa utáni helyreállítási terv kidolgozása.**
- **Amennyiben lehetséges, többfaktoros azonosítás engedélyezése az RDP bejelentkezéshez.**
- **A nyitott portok alapértelmezett értékeinek megváltoztatása megnehezíti az automatákkal végzett letapogatást, így a szolgáltatás támadásokkal szembeni kitettsége is csökkenthető.**
- **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.**
- **Alkalmazások és operációs rendszerek naprakészen tartása.**
- **Határvédelmi eszközök feketelistájának frissítése** (több gyártó rendelkezik nyilvánosan elérhető listákkal pl.: Cisco), ezáltal csökkentve a támadás kockázatát.
- A **szükségtelen felhasználói fiókok felfüggesztése**, a távoli eléréssel rendelkező felhasználók számának minimalizálása, a **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 CSIRT@nki.gov.hu e-mail címen.

A fentiekben megfogalmazott javaslatok végrehajtása nem csak a DeadBolt ransomware, hanem minden olyan zsarolóvírus esetében jelentősen csökkentik a biztonsági esemény bekövetkeztét, amelyeket RDP segítségével juttatnak a támadók a rendszerbe.

További hivatkozások:

- Közigazgatási Kibervédelmi Eszköztár
- Levélfejléc kinyerése
- Zsarolóvírusok
- Adathalászat
- Adatbiztonság a munkahelyen
- Biztonságos internethasználat
- Megszemélyesítéses támadások
- Pszichológiai befolyásolás
- Biztonsági mentés

TLP:WHITE
Szabadon terjeszthető!

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu