TLP: WHITE
Szabadon terjeszthető!

Riasztás
PHOBOS zsarolóvírus terjedéséről
(2020. február 29.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **riasztást** ad ki **PHOBOS ransomware megnövekedett terjedésével kapcsolatban**. Az NBSZ NKI tapasztalatai alapján a zsarolóvírus terjedése az elmúlt időszakban fokozódó jelenlétet mutat. Az hazai és nemzetközi partnerektől származó információk alapján a zsarolóvírus elsődleges célpontjai vállalatok és szervezetek, ugyanakkor a magánszemélyek érintettsége is növekvő tendenciát mutat.

A PHOBOS zsarolóvírus terjedésére vonatkozóan az alábbi módszerek ismertek:

- **Nyitott, vagy nem biztonságos távoli asztali kapcsolaton (RDP; port 3389) keresztül;**
- **RDP hitelesítő adatok brute-force támadásával;**
- **kiszivárgott, vagy megszerzett RDP hitelesítő adatok segítségével;**
- **valamint klasszikus és jól bevált adathalász technika segítségével.**

A támadások sikerességének csökkentése érdekében, kiemelt tekintettel a távoli asztali elérést biztosító szolgáltatásokra az NBSZ NKI az alábbi kockázatcsökkentő / megelőző intézkedések mihamarabbi megtételét javasolja:

- **Az RDP kiszolgáló beállítása, hogy publikus IP címekről tiltva legyen a TCP3389 port elérése.**
- Amennyiben szükséges **RDP** elérés, a **hozzáférés korlátozása** megadott **IP címekre**.
- **RDP** hozzáférés és hozzáférési kísérletek **naplózásának beállítása**.
- 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 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 CSIRT@nki.gov.hu e-mail címen.

A fentiekben megfogalmazott javaslatok végrehajtása nem csak a PHOBOS 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

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