TLP:WHITE
Szabadon terjeszthető!

Tájékoztatás

PLAY ransomware-rel kapcsolatban

(2022. augusztus 12.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **tájékoztató**t ad ki a **PLAY ransomware-rel kapcsolatban.** A hazai partnerektől származó információk alapján a zsarolóvírus elsődleges célpontja a kis- és középvállalatok.

A PLAY ransomware működése:

A számítógépen tárolt adatfájlok **titkosítása után** az említett *„.txt”* formátum mellett egy *„.play”* kiterjesztésű adatfájl, valamint egy másik **szöveges dokumentum is létrejön** a felhasználó asztalán, ami egy **e-mail címet tartalmaz.**

A zsarolóvírus viszonylag agresszívan terjed belső hálózaton, miután az **internetről nyitott SSH, RDP vagy FTP kapcsolaton keresztül betöltődik az adott rendszerbe**, illetve nem megfelelő védelemmel ellátott, **gyenge jelszóval védett szolgáltatásokat vesz célpontba**, amikbe beletartoznak a webszerverek, az OWA és az Exchange kiszolgáló rendszerei. A **rendszer infekciója** a jellemzően **e-mail csatolmányban** elhelyezett gyanús fájlon keresztül vagy az internetről letöltött **nem hivatalos oldalról beszerzett ismert programcsomaggal történik** meg (Skype, Teams, Chrome, Firefox…).

Az elsődleges információk alapján a fertőzés elsősorban Microsoft Office és Open Office dokumentumokat, PDF és TXT fájlokat, adatbázis fájlokat, valamint fotó, zene és videófájlokat enkriptál. A fertőzött állományt az asztali ikonokon kívül a \Desktop\ -> \User_folders\ -> \%TEMP%\ -> könyvtáron belül helyezi el a kártevő programkód.

Biztonsági szempontból elsődleges feladat, hogy a vírussal detektált és megfertőzött számítógépet minél előbb izolálják a hálózatról, ezzel megelőzve a kártevő további terjedését. A nagyobb vírusdetektáló cégek még nem adtak ki megfelelő eszközt a vírus visszafejtéséhez, ezért a titkosított adatokat jelenleg nem lehet dekódolni.

A nevezett ransomware vizsgálatát követően megállapítást nyert, hogy a zsarolóvírust több vírusvédelmi rendszer már ismeri, ezért annak használatát javasoljuk.

Jelenleg az esettel összefüggésbe hozható rendelkezésre álló indikátor:

sha256: 7d14b98cdc1b898bd0d9be80398fc59ab560e8c44e0a9dedac8ad4ece3d450b0

TLP:WHITE
Szabadon terjeszthető!

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.

Hivatkozások:

- **https://malwarefixes.com/play-ransomware/**
- **https://nologs-nobreach.com/2022/07/24/play-ransomware/**
- **https://www.bleepingcomputer.com/forums/t/773651/play-ransomware-play-support-topic/**
- **https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-zsarolovirus-ransomware-tamadasokkal-kapcsolatban/**
- **https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-nyitott-rdp-port-biztonsagi-kockazatai/**

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