

## Riasztás

### AgentTesla malware kampánnyal összefüggésben

(2022. november 24.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **riasztást** ad ki **AgentTesla malware** egyes variánsainak **terjedésével kapcsolatban**.

Az NBSZ NKI tapasztalatai alapján a malware terjesztésére irányuló e-mail tevékenység az elmúlt időszakban ugrásszerűen megemelkedett. Az **AgentTesla** egy moduláris felépítésű trójai, amely 2014 óta van jelen. Elsősorban az áldozat eszközén begyűjthető személyes adatok megszerzésére tesz kísérletet, mint pl.: böngészőben mentett adatok, azonosítók. A káros kód emellett billentyűzetfigyelési (keylogger) funkcióval is rendelkezik.

Az **AgentTesla** terjesztése a jelenlegi kampány során jellemzően fertőzött Office dokumentumokkal történik.

Az NBSZ NKI az eset kapcsán **javasolja a kapcsolódó indikátorok tiltást a határvédelmi rendszeren**.

#### IoC:

- Fájl név: Kiemelkedő fizetés.exe
- MD5: FA4FFA1F263F5FC67309569975611640
- SHA1: C51ADF5382CEAC08BFD FE27CA98E22F3335472B9
- SHA256: CEFF897DF7716A8B4DFB91C0C40FF22958E23479B5AE96163F20BEF42EBB58CE
- Domain: [www\[.\]mediafire\[.\]com](http://www[.]mediafire[.]com)
- URL: [https://www\[.\]mediafire\[.\]com/file/a4wfhgxhrr7v79y/Kiemelkedő+fizetés.tgz/file](https://www[.]mediafire[.]com/file/a4wfhgxhrr7v79y/Kiemelkedő+fizetés.tgz/file)
- URL: [https://api\[.\]telegram\[.\]org/bot5954474519:AAEGnfW1mRvGRxq-zIAvwJfpKEbhLLiqVaM/](https://api[.]telegram[.]org/bot5954474519:AAEGnfW1mRvGRxq-zIAvwJfpKEbhLLiqVaM/)
- IP: 108.167.141[.]212
- Domain: [cents-ability\[.\]org](http://cents-ability[.]org)
- e-mail feladó: [ioan.brie@decorint\[.\]ro](mailto:ioan.brie@decorint[.]ro)
- e-mail tárgy: Tárgy: Kiemelkedő fizetés

**TLP:WHITE**

**Szabadon terjeszhető!**

További, kockázatcsökkentő / megelőző intézkedések:

- Excel VBA makrók automatikus futtatásának tiltása.
- Felhasználók tudatosítása, különös tekintettel, ha a beérkezett levél jóval korábbi (tavalyi) levelezésre érkezik válaszként.
- **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.
- Rendszeres online és **offline** (szalagos egység, külső merevlemez) **biztonsági mentés**, archiválás.

Biztonsági incidens bekövetkezése esetén az NBSZ NKI javasolja:

- Az érintett eszköz **hálózatról** történő **leválasztását**.
- Az érintett adathordozók helyreállítása előtt **bitazonos másolat készítését**.
- **Incidens bejelentését** az NBSZ NKI részére a [CSIRT@nki.gov.hu](mailto:CSIRT@nki.gov.hu) e-mail címen.

További hivatkozások:

- <https://nki.gov.hu/it-biztonsag/hirek/powerpoint-fajlokkal-terjesztik-a-tavoli-hozzaferest-biztosito-trojaiakat/>
- [https://malpedia.caad.fkie.fraunhofer.de/details/win.agent\\_tesla](https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla)
- [Közigazgatási Kibervédelmi Eszköztár](#)
- [Biztonsági mentés](#)

**Nemzetbiztonsági Szakszolgálat**

Nemzeti Kibervédelmi Intézet

Telefon: +36-1-336-4833

Fax: +36-1-336-4886

Incidensbejelentés: [csirt@nki.gov.hu](mailto:csirt@nki.gov.hu)

**TLP: WHITE**