



**TLP: WHITE**

**Szabadon terjeszthető!**

## Tájékoztatás káros URL-t tartalmazó üzenetekkel kapcsolatban

(2022. november 09.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatást ad ki kéréstlen, URL-t tartalmazó üzenetek kapcsán. Az URL-ek megnyitására jellemzően egy videó megtekintésének lehetőségét ígérve próbálják meg rávenni az áldozatot a támadók. A letöltést kínáló URL-ek eddigi ismereteink alapján a [https://cdn\[.\]discordapp\[.\]com](https://cdn[.]discordapp[.]com) és a [https://workupload\[.\]com](https://workupload[.]com) oldalakon elhelyezett, különböző aloldalakra mutatnak.

A letöltendő káros kódot a vírusvédelmi eszközök nem ismerik fel, annak működése során a támadók érzékeny adatokhoz (pl.: mentett jelszavak) férhetnek hozzá.

**A káros csatolmányú levelek kiszűrése érdekében a Nemzeti Kibervédelmi Intézet az alább indikátorok tiltását, illetve szűrését javasolja:**

**Ip:** 185.199.109[.]133

**Url-ek:**

[hXXps://cdn\[.\]discordapp\[.\]com](https://cdn[.]discordapp[.]com) (lehetőség esetén)

[hXXps://workupload\[.\]co](https://workupload[.]co) (lehetőség esetén)

[raw\[.\]githubusercontent\[.\]com](https://raw[.]githubusercontent[.]com) (lehetőség esetén)

**hash-ek:**

sha256: 26afc0c80e175e238680e203b2d0c3dbf1d89f2a555aa5d782dd60e99d9a915e

sha256: 08E3EE95B3460C8EB88D85F6AE3311DB3695EB25D932D8C33E3927778105921C

A fenti indikátorok szűrésén túl javasolt a fenti indikátorok tekintetében hálózati forgalomellenőrzés végrehajtása 60 napra visszamenően. Amennyiben a forgalomelemzés pozitív találatot ad, kérjük lépjen kapcsolatba Intézetünkkel!

**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**