Microsoft opozorilo - Malware campaign IcedID

Microsoft opozarja na trenutno aktivno kampanjo razširjanja malware imenovan IcedID.

Malware se razširja z inovativnimi načini zavajanja preko elektronke pošte in spletnega brskalnika, najbolj efektiven način je preko elektronske pošte.

Uporabnik prejme »legitimno« pravno opozorilo ali grozilno pismo o kršenju spletnih vsebin/objavljenih slik. Z željo po ureditvi se uporabnika naproša, da vnaša lastne informacije v formo. Sporočila so lahko prevedena tudi v lokalni jezik (SI, IT, DE). Iz forme se potem namesti malware na lokalni računalnik.

Ostali načini namestitve malware obsegajo še:

- COVID19 tematska sporočila z Excel datoteko pripeto z makro ukazi.
- Okužene priponke z geslom, ki je pripeto dokumentu.

Potrebno je biti pazljivi na sporočila, ki zgledajo legitimna.

Za več tehničnih podrobnosti preberite:
https://www.microsoft.com/security/blog/2021/04/09/investigating-a-unique-form-of-email-delivery-for-icedid-malware/