2022-07-21 (THURSDAY) - ICEDID (BOKBOT) INFECTION WITH DARK VNC AND COBALT STRIKE

REFERENCE:

- **https://twitter.com/Unit42_Intel/status/1550582228119420928**

NOTES:

- Zip files are password-protected. If you don't know the password, see the "about" page of this website.
- Traffic was generated in the evening at my location and started on Friday 2022-07-22 in UTC time.

ASSOCIATED FILES:

- **2022-07-22-IOCs-for-IcedID-with-DarkVNC-and-Cobalt-Strike.txt.zip** 1.7 kB (1,749 bytes)
- **2022-07-22-IcedID-with-DarkVNC-and-Cobalt-Strike.pcap.zip** 7.1 MB (7,140,812 bytes)
- **2022-07-22-IcedID-malware-and-artifacts.zip** 1.1 MB (1,109,852 bytes)

Click here to return to the main page.

Copyright © 2022 | Malware-Traffic-Analysis.net