MALWARE-TRAFFIC-ANALYSIS.NET

2022-07-25 (MONDAY) - ICEDID (BOKBOT) INFECTION WITH COBALT STRIKE

REFERENCE:

- **https://twitter.com/Unit42_Intel/status/1551968860756217856**

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:

- **2022-07-25-IOCs-for-IcedID-with-Cobalt-Strike.txt.zip**   1.7 kB   (1,657 bytes)
- **2022-07-25-IcedID-with-Cobalt-Strike-carved.pcap.zip**   4.3 MB   (4,323,467 bytes)
- **2022-07-25-IcedID-and-Cobalt-Strike-malware-and-artifacts.zip**   2.5 MB   (2,521,213 bytes)

Click here to return to the main page.