2022-08-03 (WEDNESDAY) - ICEDID (BOKBOT) INFECTION WITH COBALT STRIKE

REFERENCE:

- **https://twitter.com/Unit42_Intel/status/1555255274897801216**

NOTES:

- Zip files are password-protected. If you don't know the password, see the "about" page of this website.

ASSOCIATED FILES:

- **2022-08-03-IOCs-for-IcedID-and-Cobalt-Strike.txt.zip** 1.9 kB (1,877 bytes)
- **2022-08-03-IcedID-malspam-1707-UTC.eml.zip** 126 kB (126,334 bytes)
- **2022-08-03-IcedID-with-Cobalt-Strike.pcap.zip** 6.7 MB (6,665,170 bytes)
- **2022-08-03-IcedID-and-Cobalt-Strike-malware-and-artifacts.zip** 3.2 MB (3,220,741 bytes)

Click here to return to the main page.