2022-05-10 (TUESDAY) - TA578 CONTACT FORMS CAMPAIGN --> ICEDID (BOKBOT) --> COBALT STRIKE

REFERENCE:

- **https://twitter.com/Unit42_Intel/status/1524474195471745028**

ASSOCIATED FILES:

- **2022-05-10-IOCs-for-Contact-Forms-IcedID-with-Cobalt-Strike.txt.zip** 2.5 kB (2,450 bytes)
- **2022-05-10-Contact-Forms-IcedID-infection-with-Cobalt-Strike.pcap.zip** 6.8 MB (6,828,144 bytes)
- **2022-05-10-IcedID-malware-and-artifacts.zip** 2.3 MB (2,267,349 bytes)
- **2022-05-10-text-file-examples-of-HTTPS-traffic-for-ISO-download.zip** 417 kB (417,030 bytes)

NOTES:

- All zip archives on this site are password-protected. If you don't know the password, see the "about" page of this website.

Click here to return to the main page.