2022-07-06 (WEDNESDAY) - TA578 "STOLEN IMAGES EVIDENCE" --> ICEDID (BOKBOT) --> DARK VNC & COBALT STRIKE

REFERENCE:

- **https://twitter.com/Unit42_Intel/status/1544820768256786433**

NOTES:

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

ASSOCIATED FILES:

- **2022-07-06-IOCs-for-TA578-contact-forms-IcedID-with-DarkVNC-and-Cobalt-Strike.txt.zip** 2.3 kB (2,288 bytes)
- **2022-07-06-TA578-Contact-Forms-IcedID-with-DarkVNC-and-Cobalt-Strike.pcap.zip** 18.5 MB (18,521,372 bytes)
- **2022-07-06-TA578-IcedID-malware-and-artifacts.zip** 3.4 MB (3,444,568 bytes)

Click here to return to the main page.