2022-06-28 (TUESDAY) - TA578 ICEDID (BOKBOT) WITH DARKVNC AND COBALT STRIKE

REFERENCE:

- **https://twitter.com/Unit42_Intel/status/1541888192802181120**

NOTES:

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

ASSOCIATED FILES:

- **2022-06-28-IOCs-for-TA578-IcedID-Cobalt-Strike-and-DarkVNC.txt.zip** 1.6 kB (1,568 bytes)
- **2022-06-28-TA578-thread-hijacked-email-pushing-IcedID-155214-UTC.eml.zip** 285 kB (284,634 bytes)
- **2022-06-28-IcedID-malware-and-artifacts.zip** 2.2 MB (2,212,336 bytes)
- **2022-06-28-TA578-IcedID-with-DarkVNC-and-Cobalt-Strike.pcap.zip** 27.0 MB (26,951,407 bytes)

Click here to return to the main page.