2022-01-06 (THURSDAY) - TA551 (SHATHAK) PUSHES ICEDID (BOKBOT)

ASSOCIATED FILES:

- **2022-01-06-IOCs-for-TA551-IcedID.txt.zip** 3.5 kB (3,517 bytes)
- **2022-01-06-TA551-IcedID-infection.pcap.zip** 2.7 MB (2,691,671 bytes)
- **2022-01-06-TA551-IcedID-malware-and-artifacts.zip** 1.3 MB (1,273,331 bytes)

NOTES:

- This is the second day in a row for TA551 activity.
- Today's Word docs use and English template, but they have mostly Italian file names.

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

IMAGES

(http.request or tls.handshake.type eq 1) and !(ssdp) and !(ip.addr eq 52.109.0.0/16) and !(ip.addr eq 52.183.0.0/16)

Time	Dst	port	Host	Info
2022-01-06 23:19:28	80.71.157.216	80	thompsonstorages.com	GET /vcnh/31815/15915/Ebkqanyvr/o4Esy
2022-01-06 23:20:28	13.249.195.74	443	aws.amazon.com	Client Hello
2022-01-06 23:20:31	194.147.115.14	80	joikarendal.com	GET / HTTP/1.1
2022-01-06 23:21:01	5.181.80.225	443	upperdown.eu	Client Hello
2022-01-06 23:22:01	94.140.112.43	443	landofrayz.com	Client Hello
2022-01-06 23:22:02	94.140.112.43	443	landofrayz.com	Client Hello
2022-01-06 23:22:02	94.140.112.43	443	landofrayz.com	Client Hello
2022-01-06 23:22:02	5.181.80.225	443	upperdown.eu	Client Hello
2022-01-06 23:27:02	94.140.112.43	443	landofrayz.com	Client Hello

Shown above: Screenshot of the infection traffic filtered in Wireshark.

Click here to return to the main page.