

2021-05-24 (MONDAY) - TA551 (SHATHAK) WORD DOCS PUSH ICEDID (BOKBOT)

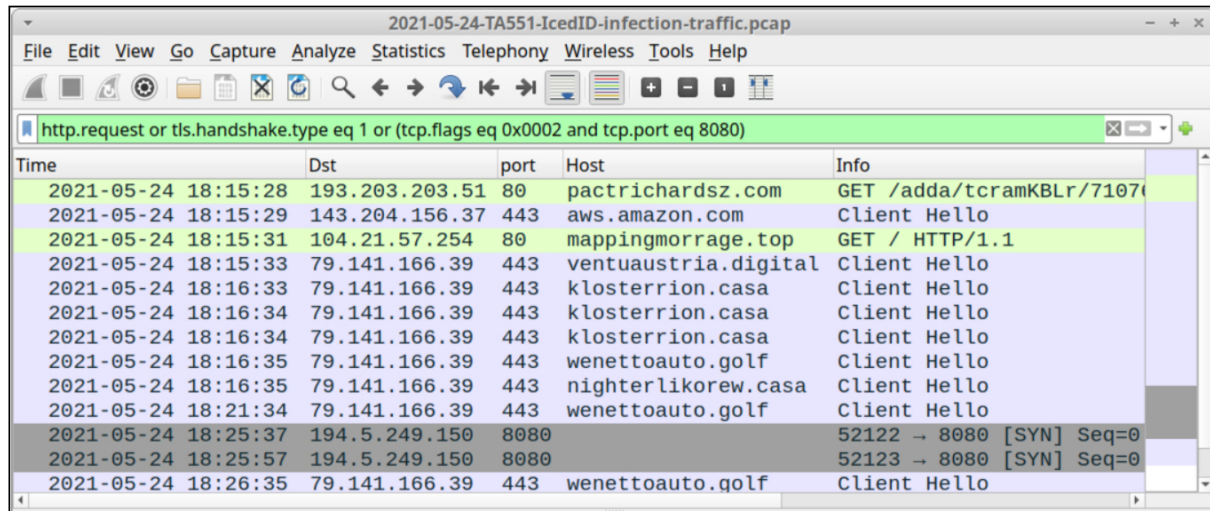
ASSOCIATED FILES:

- 2021-05-24-TA551-IOCs-for-IcedID.txt.zip 3.6 kB (3,578 bytes)
- 2021-05-24-TA551-malspam-1418-UTC.eml.zip 79.2 kB (79,249 bytes)
- 2021-05-24-TA551-IcedID-malware-and-artifacts.zip 1.4 MB (1,425,721 bytes)
- 2021-05-24-TA551-IcedID-infection-traffic.pcap.zip 3.9 MB (3,873,519 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.

IMAGES



Time	Dst	port	Host	Info
2021-05-24 18:15:28	193.203.203.51	80	pactrichardsz.com	GET /adda/tcramKBLr/71070
2021-05-24 18:15:29	143.204.156.37	443	aws.amazon.com	Client Hello
2021-05-24 18:15:31	104.21.57.254	80	mappingmorrage.top	GET / HTTP/1.1
2021-05-24 18:15:33	79.141.166.39	443	ventuaustria.digital	Client Hello
2021-05-24 18:16:33	79.141.166.39	443	klosterrion.casa	Client Hello
2021-05-24 18:16:34	79.141.166.39	443	klosterrion.casa	Client Hello
2021-05-24 18:16:34	79.141.166.39	443	klosterrion.casa	Client Hello
2021-05-24 18:16:35	79.141.166.39	443	wenettoauto.golf	Client Hello
2021-05-24 18:16:35	79.141.166.39	443	nighterlikorew.casa	Client Hello
2021-05-24 18:21:34	79.141.166.39	443	wenettoauto.golf	Client Hello
2021-05-24 18:25:37	194.5.249.150	8080		52122 → 8080 [SYN] Seq=0
2021-05-24 18:25:57	194.5.249.150	8080		52123 → 8080 [SYN] Seq=0
2021-05-24 18:26:35	79.141.166.39	443	wenettoauto.golf	Client Hello

Shown above: Traffic from an infection filtered in Wireshark.

[Click here](#) to return to the main page.