2021-06-02 (WEDNESDAY) - TA551 (SHATHAK) WORD DOCS PUSH ICEDID (BOKBOT)

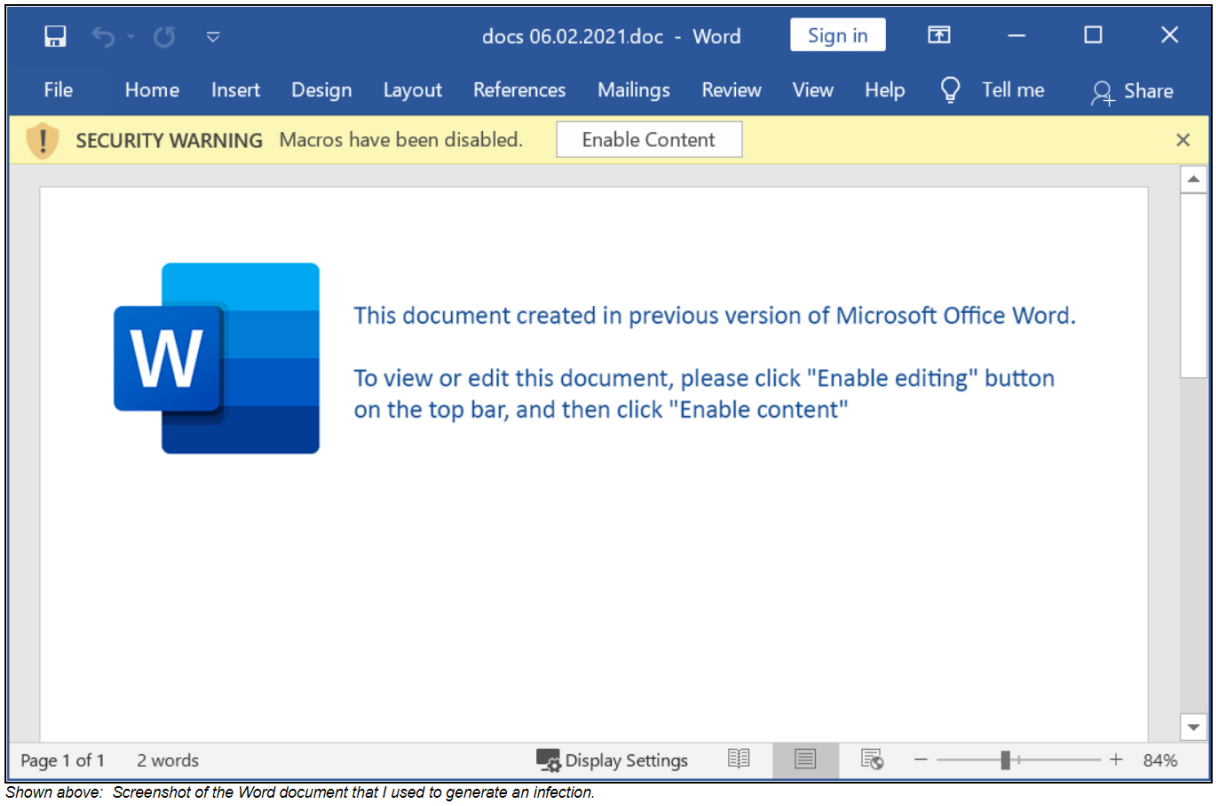
ASSOCIATED FILES:

- **2021-06-02-TA551-IOCs-for-IcedID.txt.zip** 4.4 kB (4,376 bytes)
- **2021-06-02-TA551-Word-docs-14-examples.zip** 523 kB (522,802 bytes)
- **2021-06-02-TA551-HTA-and-DLL-files.zip** 1.8 MB (1,803,122 bytes)
- **2021-06-02-IcedID-infection-traffic.pcap.zip** 3.4 MB (3,442,315 bytes)
- **2021-06-02-malware-and-artifacts-from-TA551-IcedID-infection.zip** 1.6 MB (1,603,767 bytes)

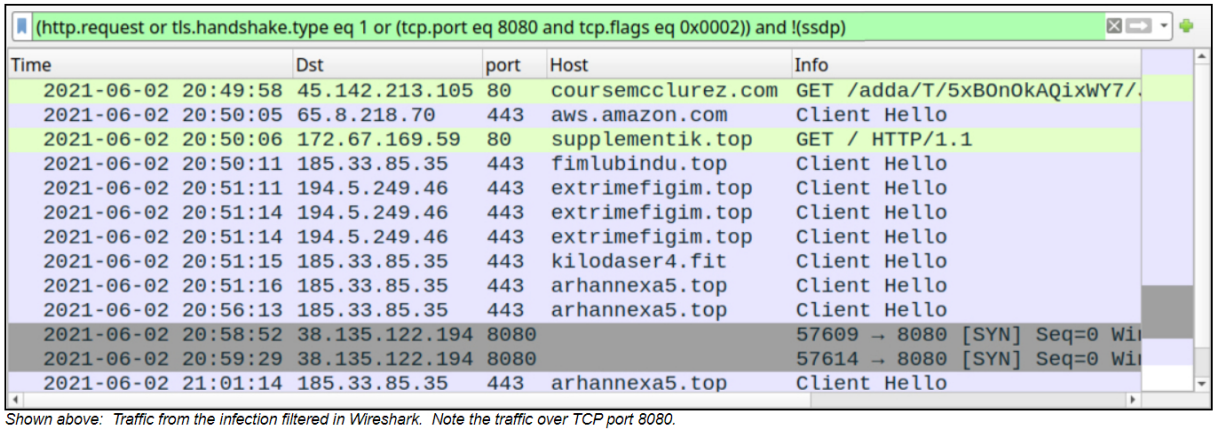
NOTES:

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

IMAGES



Shown above: Screenshot of the Word document that I used to generate an infection.



Time	Dst	port	Host	Info
2021-06-02 20:49:58	45.142.213.105	80	coursemcclurez.com	GET /adda/T/5xBOnOkAQixWY7/
2021-06-02 20:50:05	65.8.218.70	443	aws.amazon.com	Client Hello
2021-06-02 20:50:06	172.67.169.59	80	supplementik.top	GET / HTTP/1.1
2021-06-02 20:50:11	185.33.85.35	443	fimlubindu.top	Client Hello
2021-06-02 20:51:11	194.5.249.46	443	extrimefigim.top	Client Hello
2021-06-02 20:51:14	194.5.249.46	443	extrimefigim.top	Client Hello
2021-06-02 20:51:14	194.5.249.46	443	extrimefigim.top	Client Hello
2021-06-02 20:51:15	185.33.85.35	443	kilodaser4.fit	Client Hello
2021-06-02 20:51:16	185.33.85.35	443	arhannexa5.top	Client Hello
2021-06-02 20:56:13	185.33.85.35	443	arhannexa5.top	Client Hello
2021-06-02 20:58:52	38.135.122.194	8080		57609 → 8080 [SYN] Seq=0 Wi
2021-06-02 20:59:29	38.135.122.194	8080		57614 → 8080 [SYN] Seq=0 Wi
2021-06-02 21:01:14	185.33.85.35	443	arhannexa5.top	Client Hello

Shown above: Traffic from the infection filtered in Wireshark. Note the traffic over TCP port 8080.

Click here to return to the main page.