MALWARE-TRAFFIC-ANALYSIS.NET

2021-02-25 - TA551 (SHATHAK) BACK TO PUSHING ICEDID (BOKBOT)

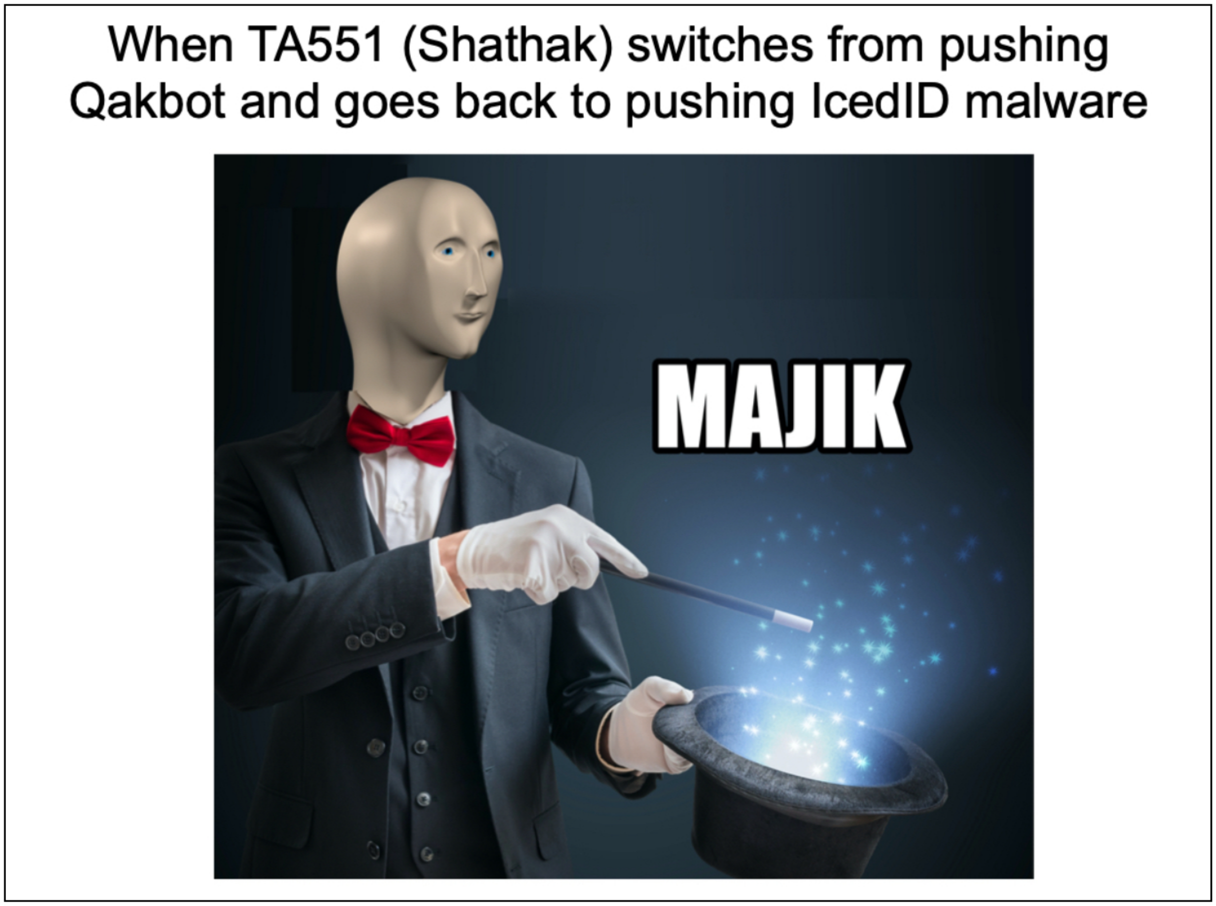
ASSOCIATED FILES:

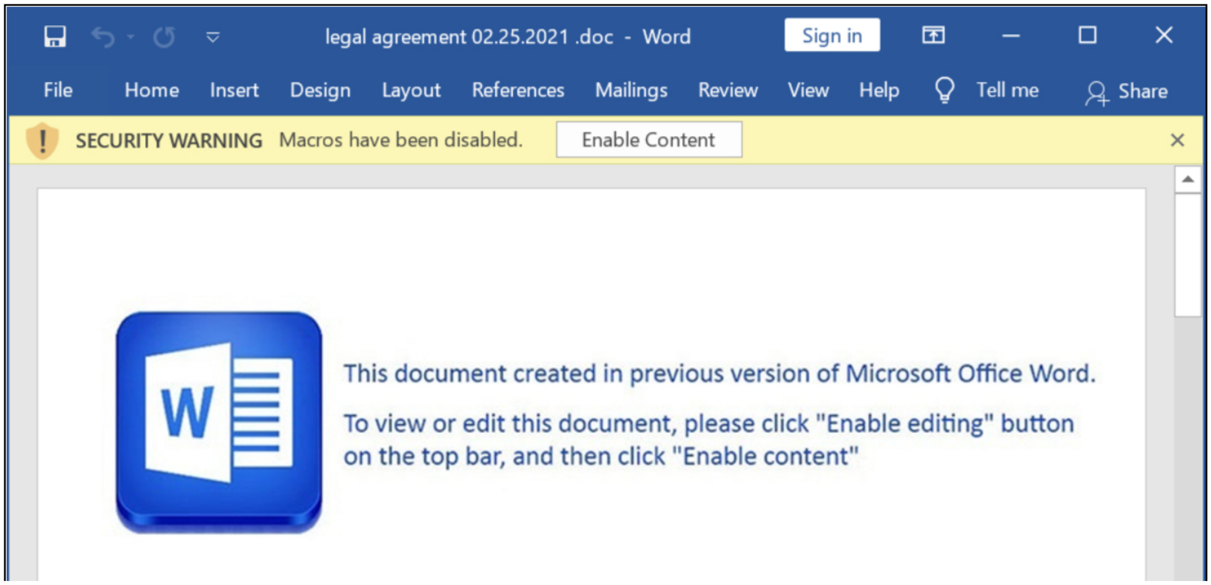
- **2021-02-25-IOCs-for-IcedID-from-TA551.txt.zip** 3.6 kB (3,622 bytes)
- **2021-02-25-TA551-IcedID-infection-traffic.pcap.zip** 8.0 MB (7,979,570 bytes)
- **2021-02-25-Word-docs-and-installer-DLL-files.zip** 15.4 MB (15,382,175 bytes)
- **2021-02-25-malware-and-artifacts-from-an-infection.zip** 9.4 MB (9,415,415 bytes)

NOTES:

- From 2021-01-22 through at least 2021-02-05, the TA551 (Shathak) campaign was pushing Qakbot (Qbot) malware. Today it returned to pushing IcedID (Bokbot).
- All zip archives on this site are password-protected. If you don't know the password, see the "about" page of this website.

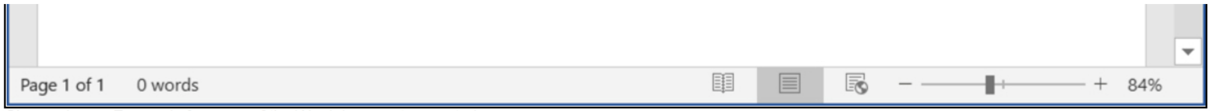
IMAGES


When TA551 (Shathak) switches from pushing Qakbot and goes back to pushing IcedID malware

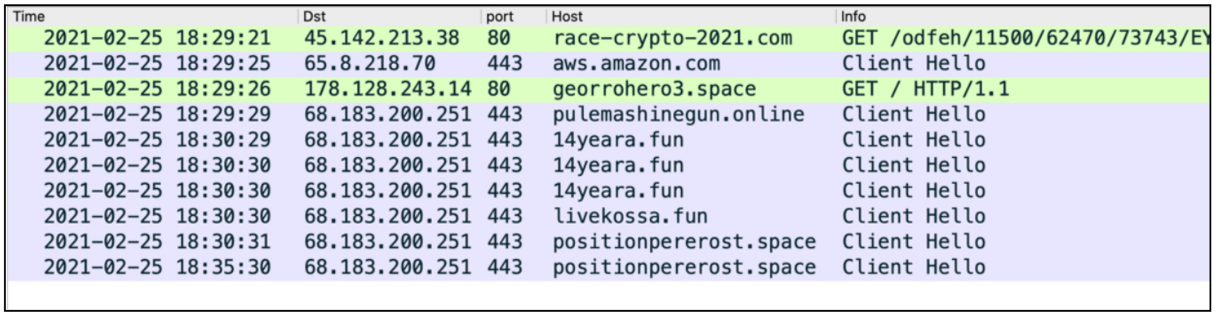


This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"



Shown above: Exeample from one of the Word documents seen today.



Time	Dst	port	Host	Info
2021-02-25 18:29:21	45.142.213.38	80	race-crypto-2021.com	GET /odfeh/11500/62470/73743/EY
2021-02-25 18:29:25	65.8.218.70	443	aws.amazon.com	Client Hello
2021-02-25 18:29:26	178.128.243.14	80	georrohero3.space	GET / HTTP/1.1
2021-02-25 18:29:29	68.183.200.251	443	pulemashinegun.online	Client Hello
2021-02-25 18:30:29	68.183.200.251	443	14yeara.fun	Client Hello
2021-02-25 18:30:30	68.183.200.251	443	14yeara.fun	Client Hello
2021-02-25 18:30:30	68.183.200.251	443	14yeara.fun	Client Hello
2021-02-25 18:30:30	68.183.200.251	443	livekossa.fun	Client Hello
2021-02-25 18:30:31	68.183.200.251	443	positionpererost.space	Client Hello
2021-02-25 18:35:30	68.183.200.251	443	positionpererost.space	Client Hello

Shown above: Traffic from an infection filtered in Wireshark.

Click here to return to the main page.