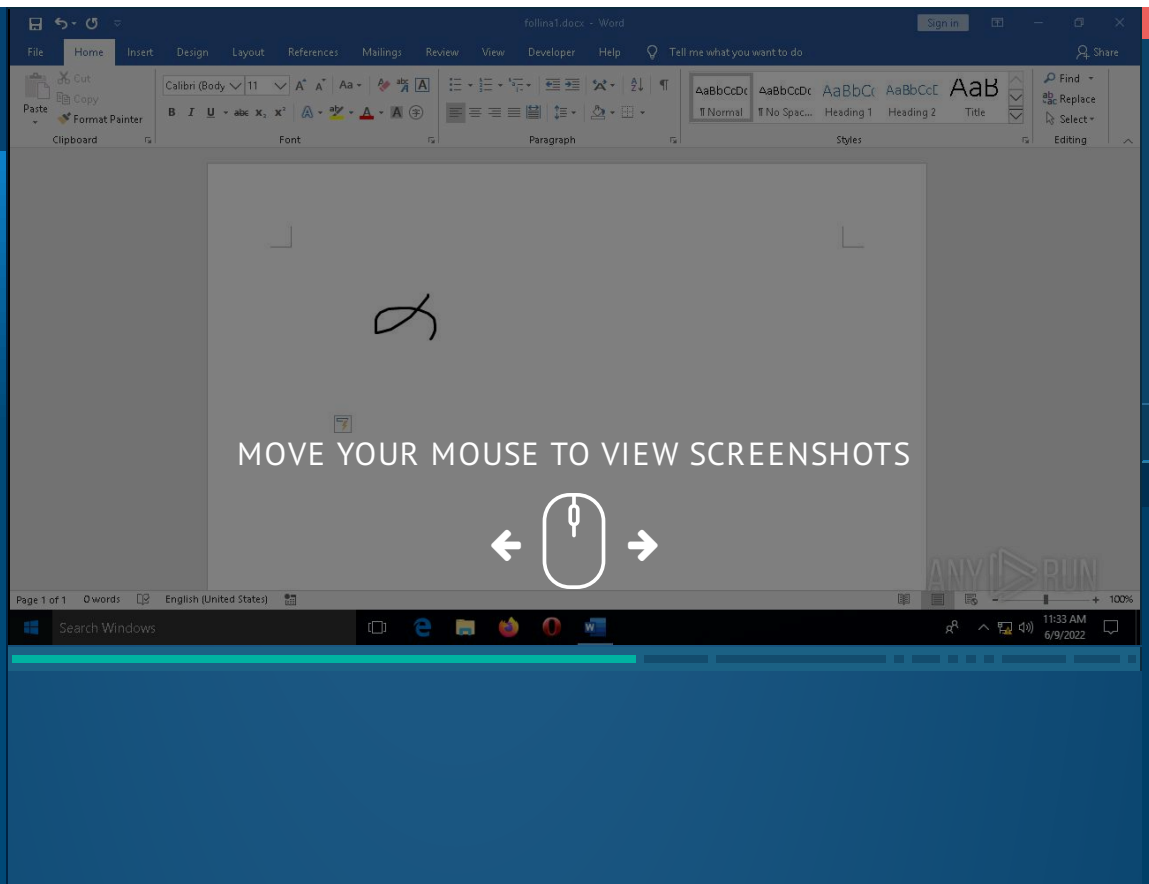

Malicious activity

follina1.docx

MD5: 046AE2440E0808BC2EEC9B72DA015981

Start: 09.06.2022, 13:32 Total time: 60 s

Win10 64 bit
Complete

generated-doc | cve-2022-30190 | exploit

Indicators:

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes | Filter by PID or name | Only important

1416	WINWORD.EXE	/n "C:\Users\admin\AppData\Local\Temp\follina1....	8k	4k	187
3628	msdt.exe	ms-msdt:/id PCWDiagnostic /skip force /param "IT...	1k	2k	70
3028	COM sdiagnhost.exe	-Embedding	4k	1k	112
3572	conhost.exe	0xffffffff -ForceV1	136	52	31
4644	csc.exe	/noconfig /fullpaths @"C:\Users\admin\AppData\Loc...	385	1k	34
308	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OUT:C...	69	16	14
692	csc.exe	/noconfig /fullpaths @"C:\Users\admin\AppData\Local...	381	1k	34
1320	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OUT:...	69	16	14
68	csc.exe	/noconfig /fullpaths @"C:\Users\admin\AppData\Local\...	380	1k	34
1928	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OUT:...	69	16	14
3076	calc.exe		316	192	50
4420	csc.exe	/noconfig /fullpaths @"C:\Users\admin\AppData\Loc...	381	1k	34
1656	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OUT:...	69	16	14
68	COM OpenWith.exe	-Embedding	539	293	76

HTTP Requests 4 | Connections 11 | DNS Requests 7 | Threats 0 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
27553 ms	GET | 200: OK	?	1416	WINWORD.EXE		http://ocsp.digicert.com/MFEwTzBNM...	47
27566 ms	GET | 200: OK	?	1416	WINWORD.EXE		http://x1.c.lencr.org/	71
27589 ms	GET | 200: OK	?	1416	WINWORD.EXE	?	http://r3.o.lencr.org/MFMwUTBPME0w...	50
28551 ms	GET | 200: OK	?	1416	WINWORD.EXE	?	http://r3.o.lencr.org/MFMwUTBPME0w...	50

Warning [4420] csc.exe Drops a file with a compile date too recent

Try community version for free! Register now