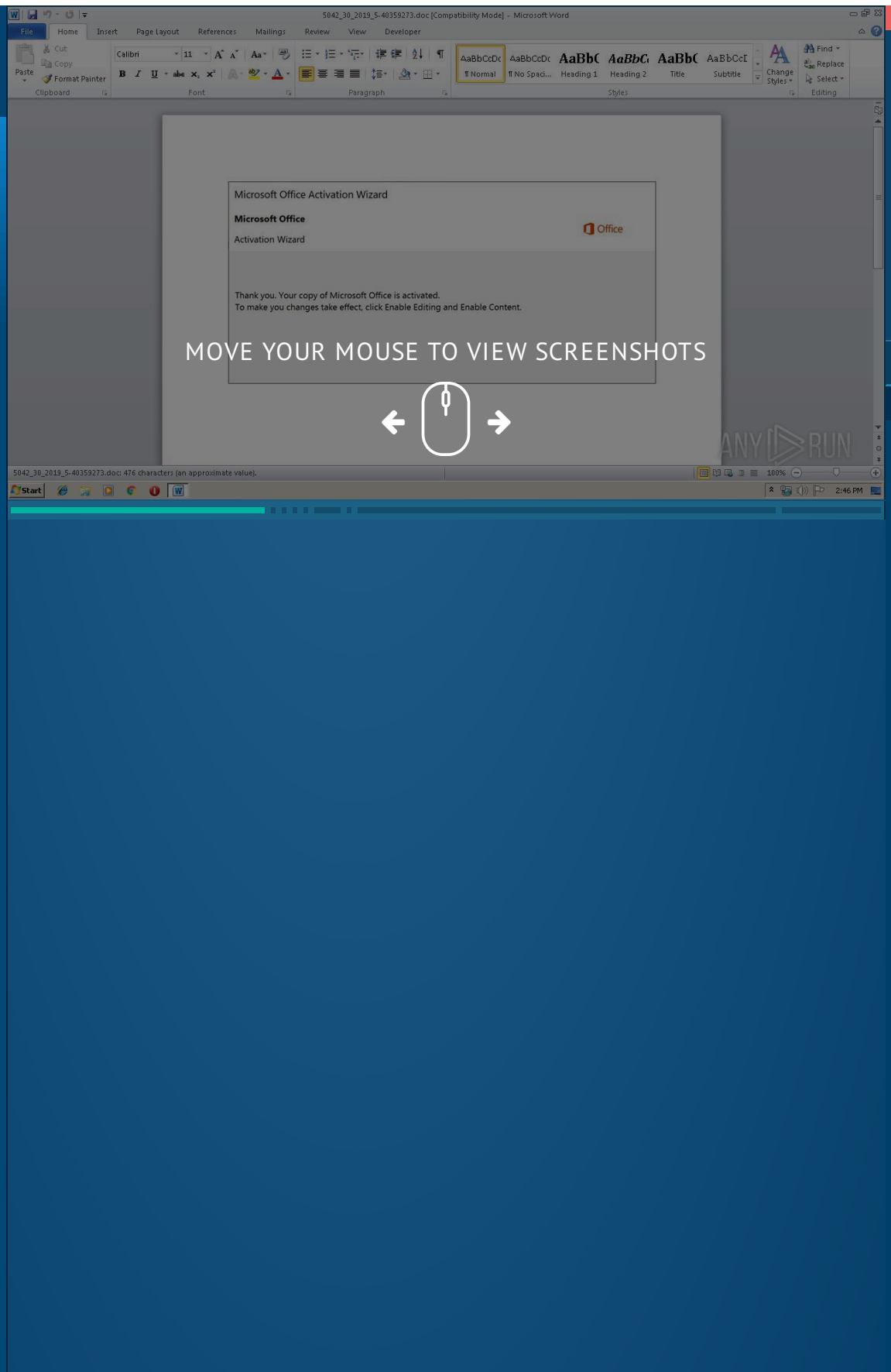

Malicious activity

5042_30_2019_5-40359273.doc

MD5: 9600328A14AB247BBE1B1BA6B543E2E3

Start: 30.09.2019, 15:46 Total time: 60 s

Win7 32 bit Complete

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

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

2800 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\5042_3... 3k 1k 116

3100 WMI powershell.exe -enco PAAjACAAaAB0AHQAcABzADoALwAvA... 1k 556 230

4012 ntvdm.exe -i1 436 0 50

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

NETWORK | FILES | DEBUG

Timeshift | Headers | Rep | PID | Process name | CN | URL | Content

No data

Warning [3100] powershell.exe Executes application which crashes

Try community version for free! Register now