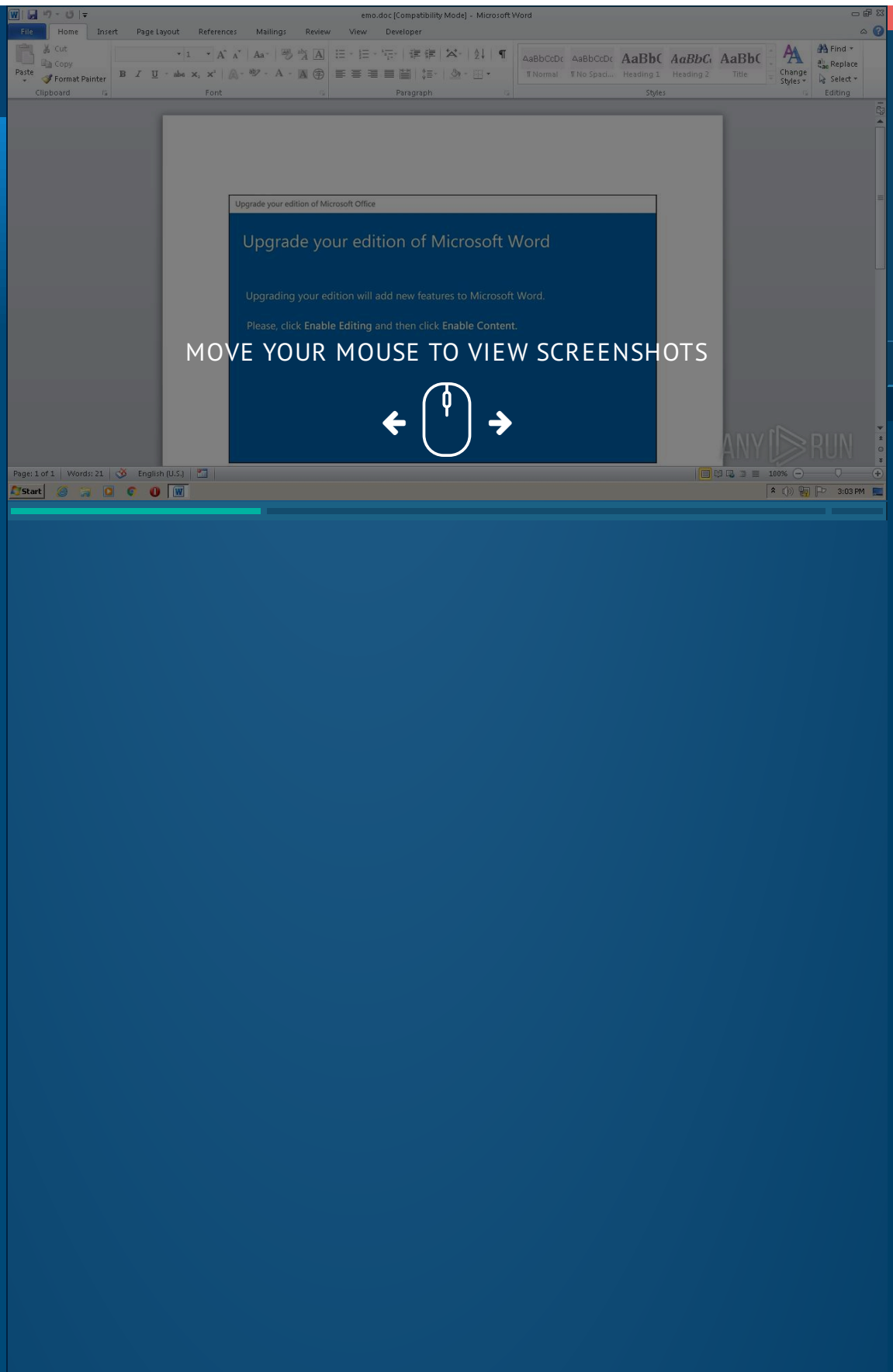

Malicious activity

emo.doc

MD5: 3079AF4D01EE6EC51BD3D9911DA7E23F
Start: 11.07.2022, 16:02 **Total time:** 60 s

Win7 32 bit
Complete

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

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

3060 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\emo.doc"
5k 3k 111

2120 WMI POwersheLL.exe -windowstyle hidden -ENCOD IABTAFYAIAA...
2k 922 84

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

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content

No data

Warning [2120] POwersheLL.exe Reads Environment values

Try community version for free! Register now