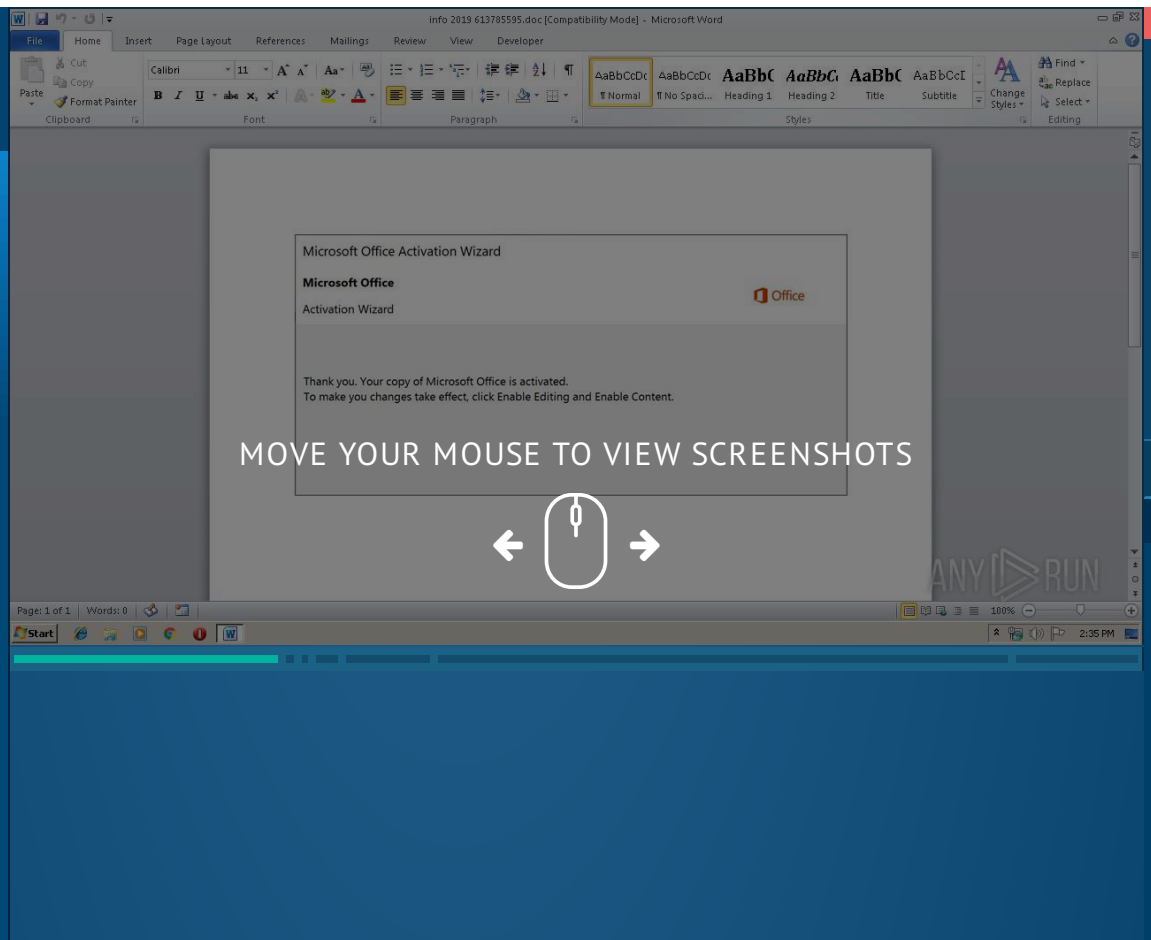

Malicious activity

info 2019 613785595.doc

MD5: 9600328A14AB247BBE1B1BA6B543E2E3

Start: 30.09.2019, 15:35 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

2936	WINWORD.EXE	/n "C:\Users\admin\AppData\Local\Temp\info 201...	4k	1k	106
3596	WMI powershell.exe	-enco PAAjACAAaAB0AHQAcABzADoALwAvA...	1k	547	230
2924	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 [3596] powershell.exe Executes application which crashes

Try community version for free! Register now