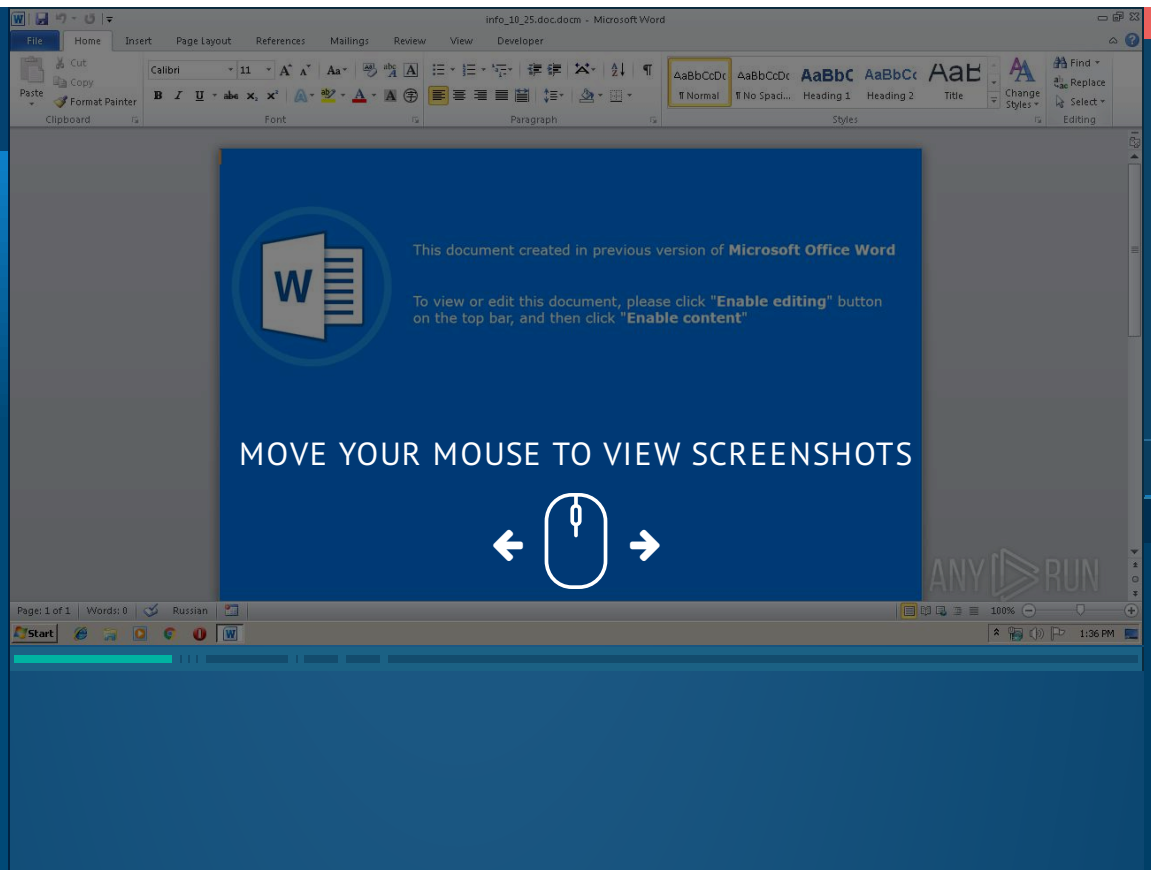

Malicious activity

info_10_25.doc

MD5: 83B97B809764B91B56EBD91D336BCAAE

Start: 25.10.2019, 14:36 Total time: 120 s

Win7 32 bit Complete

macros | macros-on-open | maldoc-3 | generated-doc | gozi | ursnif

Indicators: Tracker: Ursnif

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes Filter by PID or name Only important

1764 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\info_10... 5k 2k 218

2308 WMIC.exe process list /format:"C:\Users\admin\AppData\Lo... ursnif 513 79 138

3252 explorer.exe 183 26 80

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

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
4669 ms	GET | 404: Not Found	?	2308	WMIC.exe	?	http://bullisworg.com/minsee/ragaba.p...	

Info [3252] explorer.exe Manual execution by user

Try community version for free! Register now