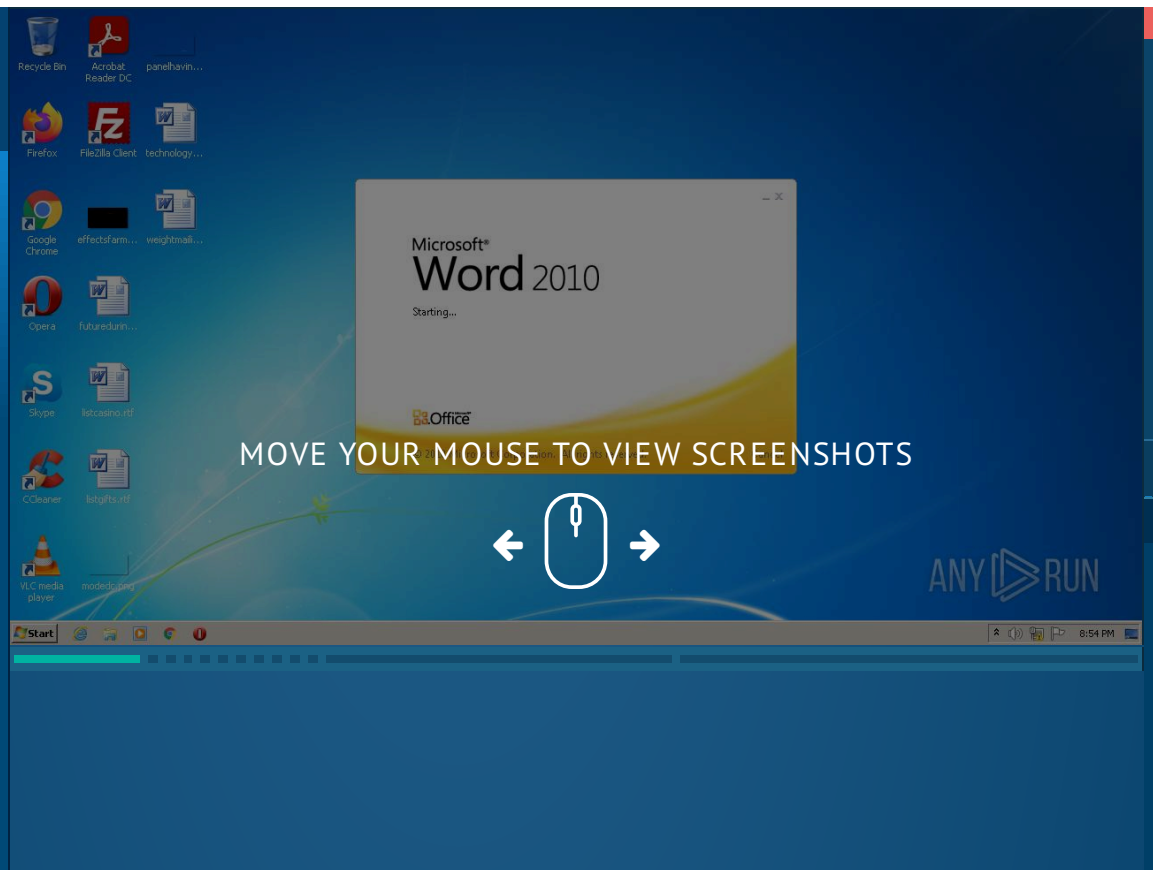

Malicious activity

download(1).doc

MD5: 14F4C470C207E22C3B0A4EFA7B4200E8
Start: 04.06.2022, 21:54 Total time: 60 s

Win7 32 bit
Complete

macros | ole-embedded | macros-on-open | maldoc-57 | generated-doc | evasion | trojan | hancitor

Indicators:

Tracker: Hancitor, Trojan

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes | Filter by PID or name | Only important

3040 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\downlo... 5k 3k 120

1816 rundll32.exe CFG c:\users\admin\appdata\roaming\micros... hancitor 375 308 74

NETWORK | FILES | DEBUG

HTTP Requests 3 | Connections 4 | DNS Requests 4 | Threats 3 | Filter by PID, name or url | PCAP

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
5706 ms	GET | 200: OK	?	1816	rundll32.exe		http://api.ipify.org/	1
9793 ms	POST | No Response	?	1816	rundll32.exe		http://euvereginumet.ru/8/forum.php	11
9801 ms	POST | No Response	?	1816	rundll32.exe		http://rhopulforopme.ru/8/forum.php	11

Pricing | Contacts | FAQ | Sign In

Danger [1816] rundll32.exe HANCITOR detected by memory dumps

Try community version for free! Register now