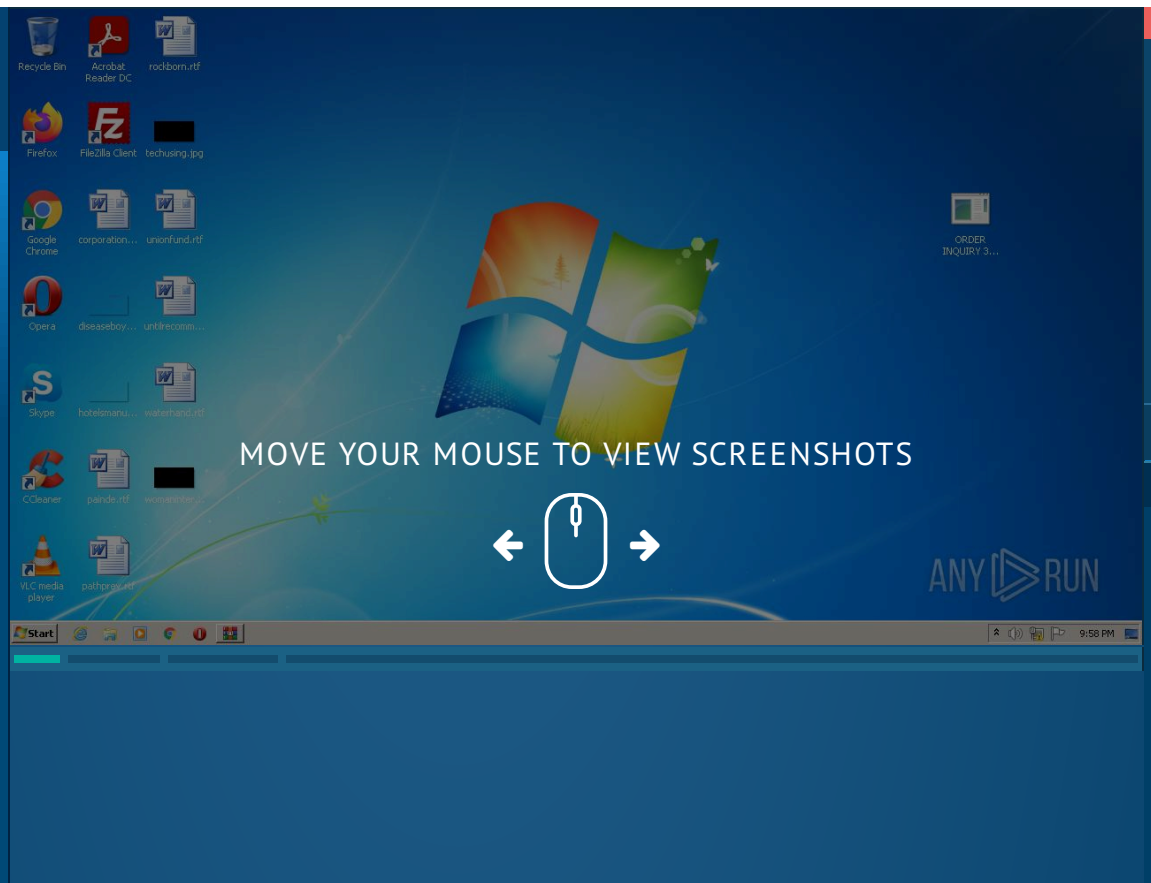

Malicious activity

3bb13a710b3a58dd9b170bf858347f00a...

MD5: CE1034A9CCAC25FAEAB4BDCBB6331E5E

Start: 23.02.2022, 22:57 Total time: 180 s

Win7 32 bit Complete

trojan formbook stealer

Indicators: Tracker: Formbook, Stealer, 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

584 SUS Explorer.EXE formbook 1k 1k 201

3848 WinRAR.exe "C:\Users\admin\AppData\Local\Temp\3bb13a7... 1k 1k 90

3996 ORDER INQUIRY 3756653.exe PE 997 332 66

3516 schtasks.exe /Create /TN "Updates\QgFSIRJE" /XML "C:... 88 14 23

3860 ORDER INQUIRY 3756653.exe PE "{path}" 37 5 14

2584 wscript.exe 41 9 28

HTTP Requests 15 | Connections 15 | DNS Requests 25 | Threats 62 | Filter by PID, name or url | PCAP

NETWORK FILES DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
58520 ms	GET | 404: Not Found	?	584	Explorer.EXE		http://www.cacaolixir.com/nqni/?EHg4...	3
63620 ms	GET | 404: Not Found	?	584	Explorer.EXE		http://www.724ototamir.com/nqni/?EH...	3
68734 ms	GET | 404: Not Found	?	584	Explorer.EXE		http://www.mkbau-quickborn.com/nqni...	3
78945 ms	GET | 404: Not Found	?	584	Explorer.EXE	?	http://www.palmsugar.biz/nqni/?EHg4S...	3
89260 ms	GET | 404: Not Found	?	584	Explorer.EXE		http://www.moreosin.com/nqni/?EHg4...	3
99470 ms	GET | 404: Not Found	?	584	Explorer.EXE		http://www.webdesigncharlestonsc.co...	3
104.58 s	GET | 404: Not Found	?	584	Explorer.EXE		http://www.dbcvj.com/nqni/?EHg4Sz=...	3
109.68 s	GET | 404: Not Found	?	584	Explorer.EXE		http://www.apollorealtors.com/nqni/?E...	3

Danger [584] Explorer.EXE Connects to CnC server

Try community version for free! Register now