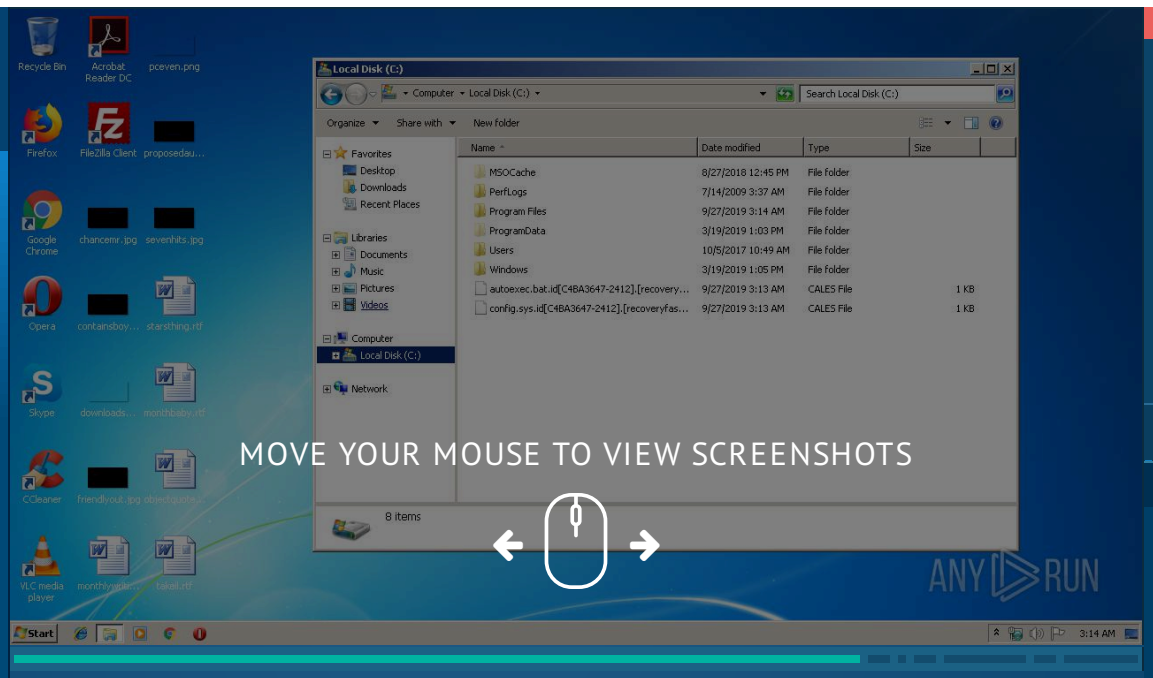

Malicious activity

svchost.exe

MD5: 1605DC744FE86B41F44C69A13AA092E9
Start: 27.09.2019, 04:13 Total time: 60 s

Win7 32 bit
Complete

ransomware

Indicators: Tracker: Ransomware

Get sample | IOC | MalConf | Restart

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

GPU RAM

Processes Filter by PID or name Only important

2948 svchost.exe PE — 481 5 39
3584 svchost.exe PE — 513 338 82
2812 svchost.exe PE — 159k 2 23
3200 cmd.exe — 154 6 26
3852 netsh.exe advfirewall set currentprofile state off — 623 60 252
2712 netsh.exe firewall set opmode mode=disable — 545 47 228
2732 explorer.exe — 184 26 80

HTTP Requests 0 | Connections 0 | 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

Info [2732] explorer.exe Manual execution by user

Try community version for free! Register now