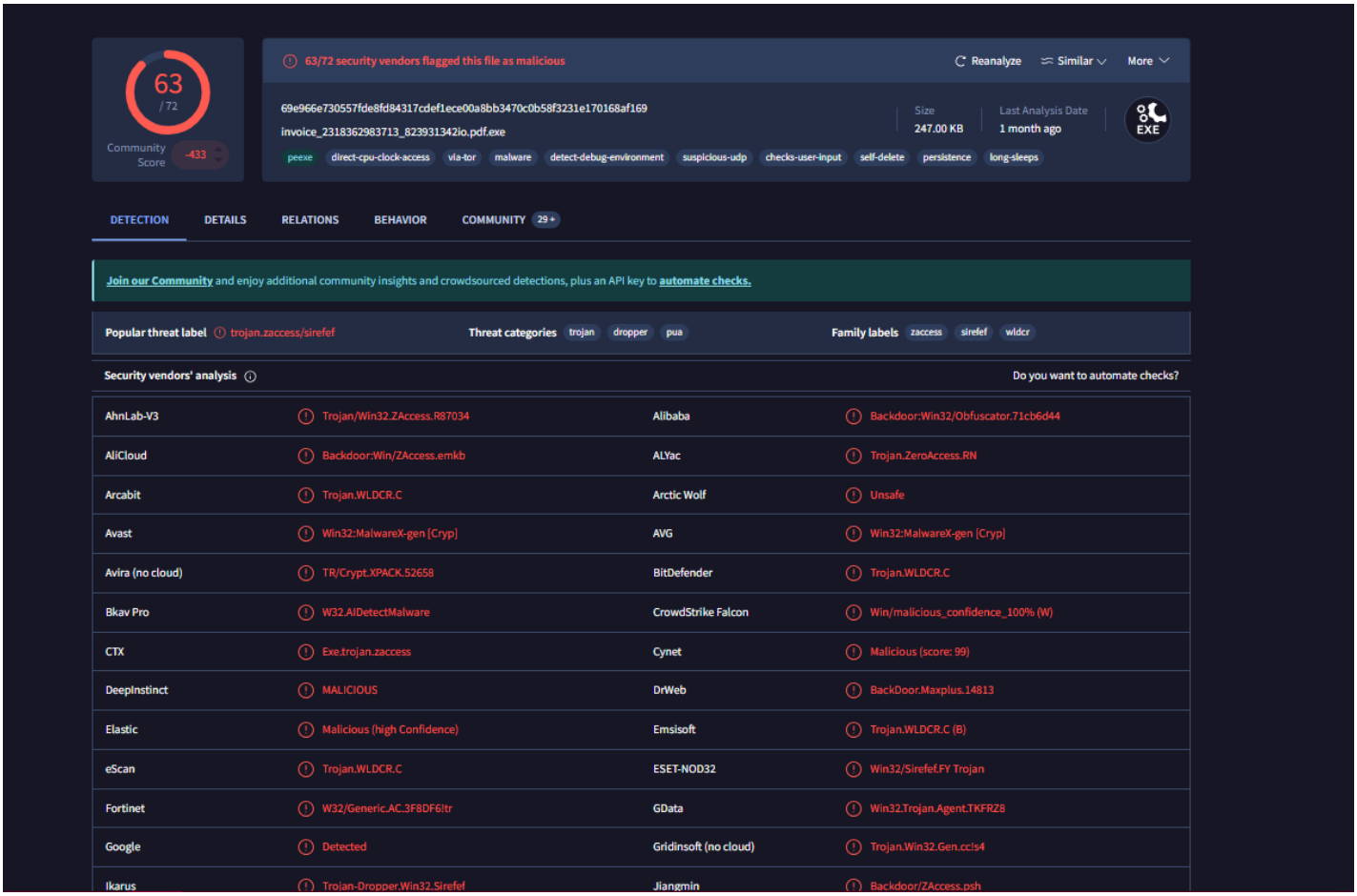
Analysis of Zeus Banking Trojan

Fingerprint:

VirusTotal output:



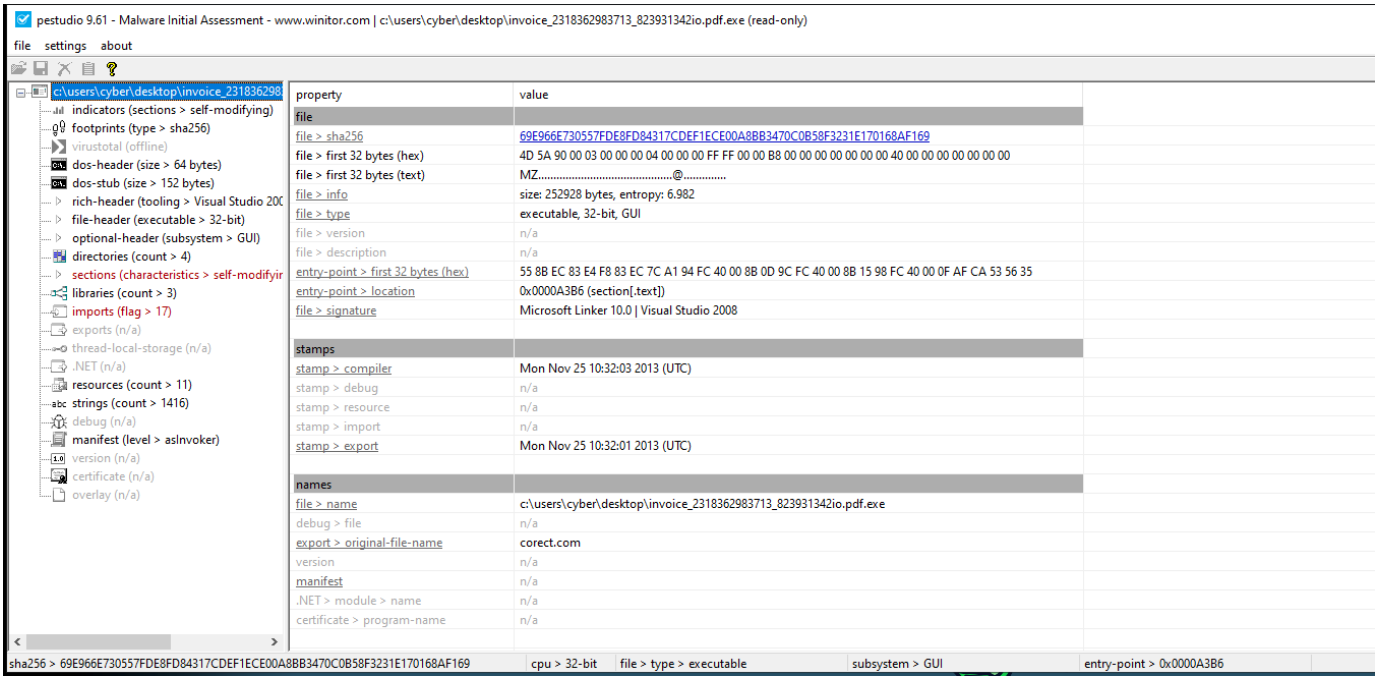
Hashes:
sha256:69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169
md5:459E320C8A8F7E7049FF769CD123FD31

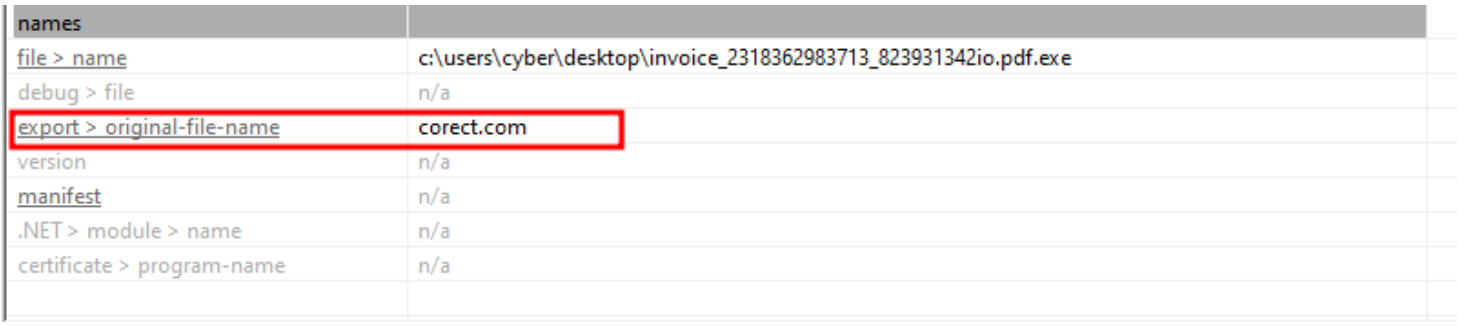
File Name:invoice_2318362983713_823931342io.pdf.exe

file > first 32 bytes (text),MZ.....@.....

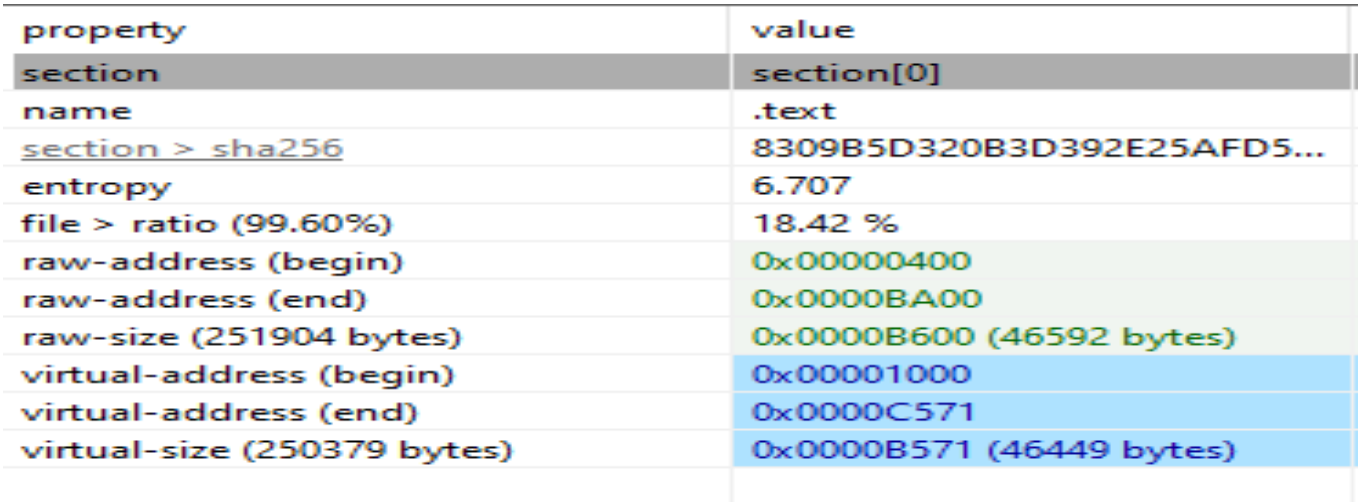
Basic Static Analysis

Pestudio output:

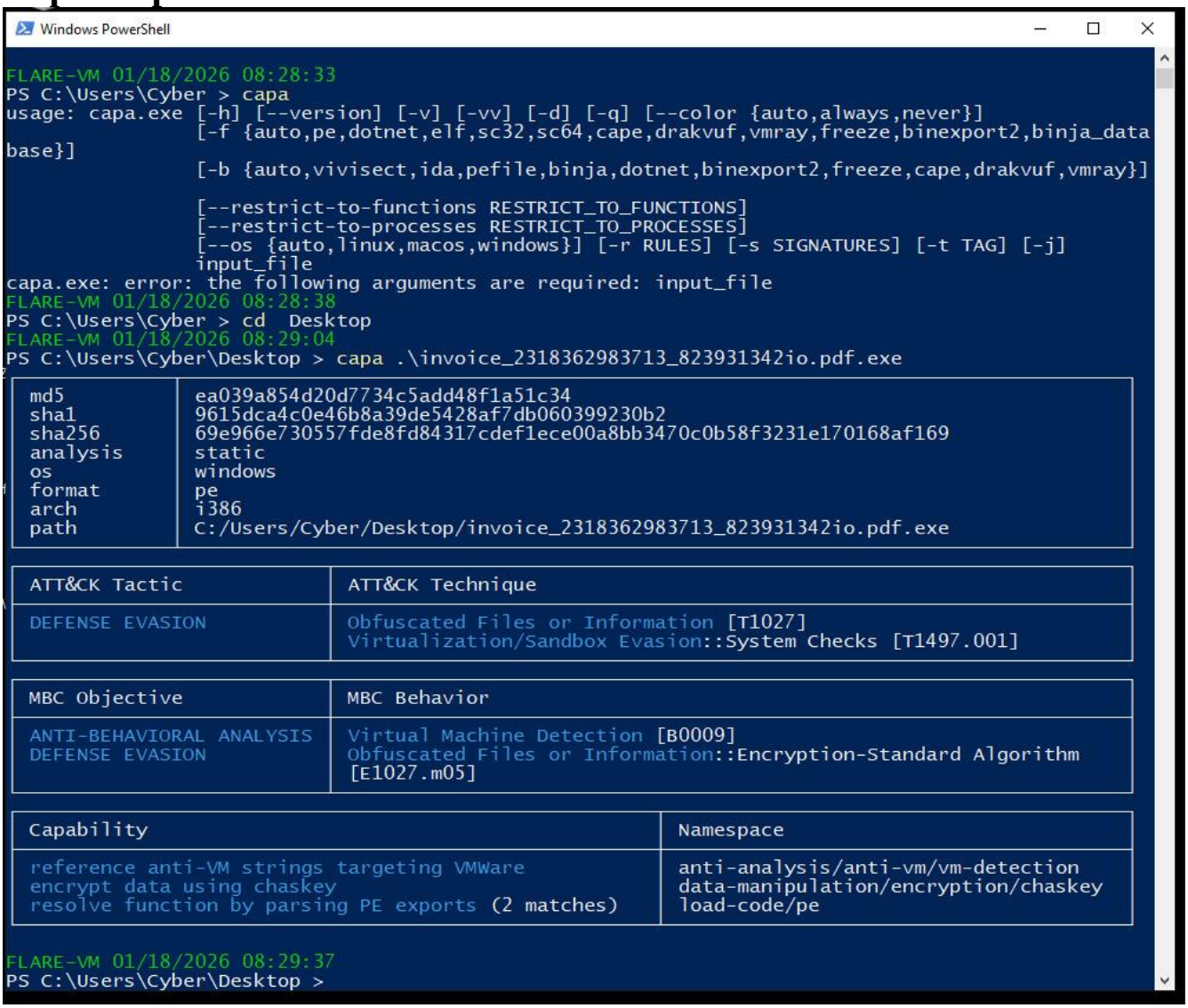




corect.com yielded no interesting results.



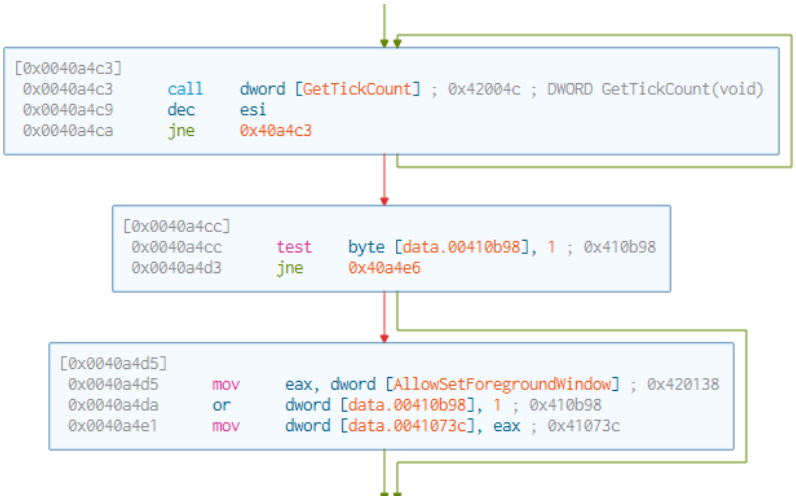
Capa output:



Advanced Static Analysis:

this is an order of execution

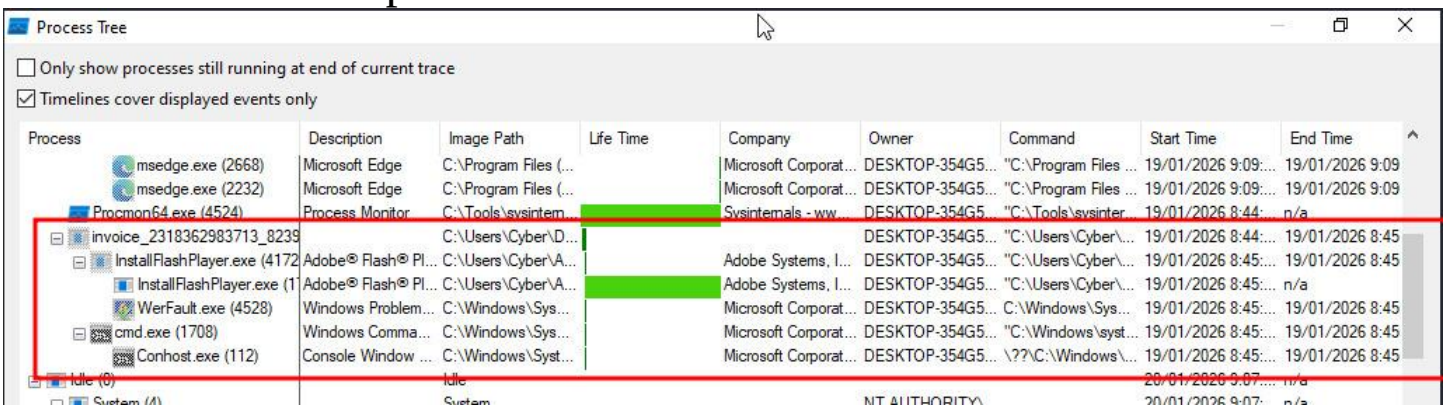
Used cutter tool

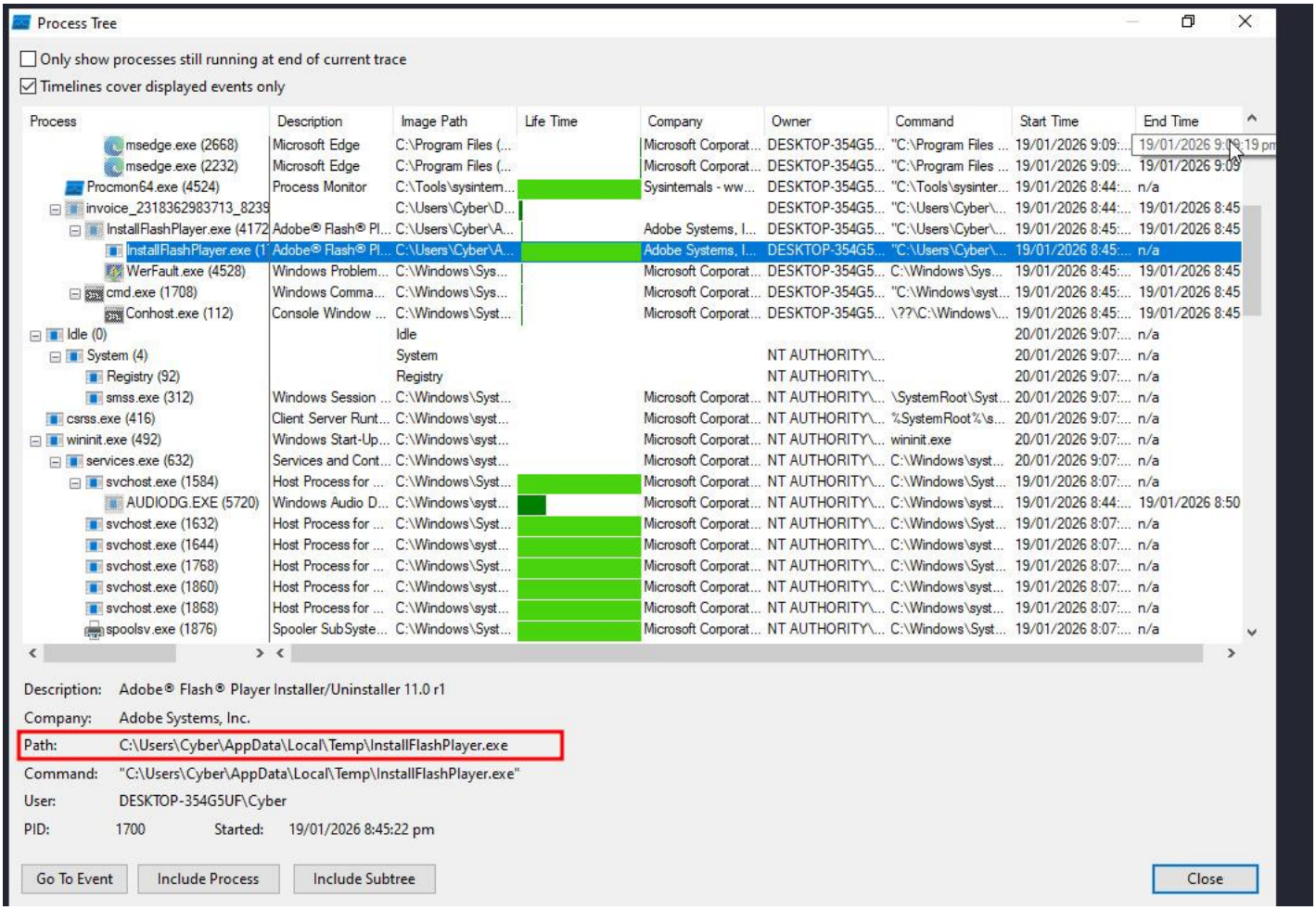


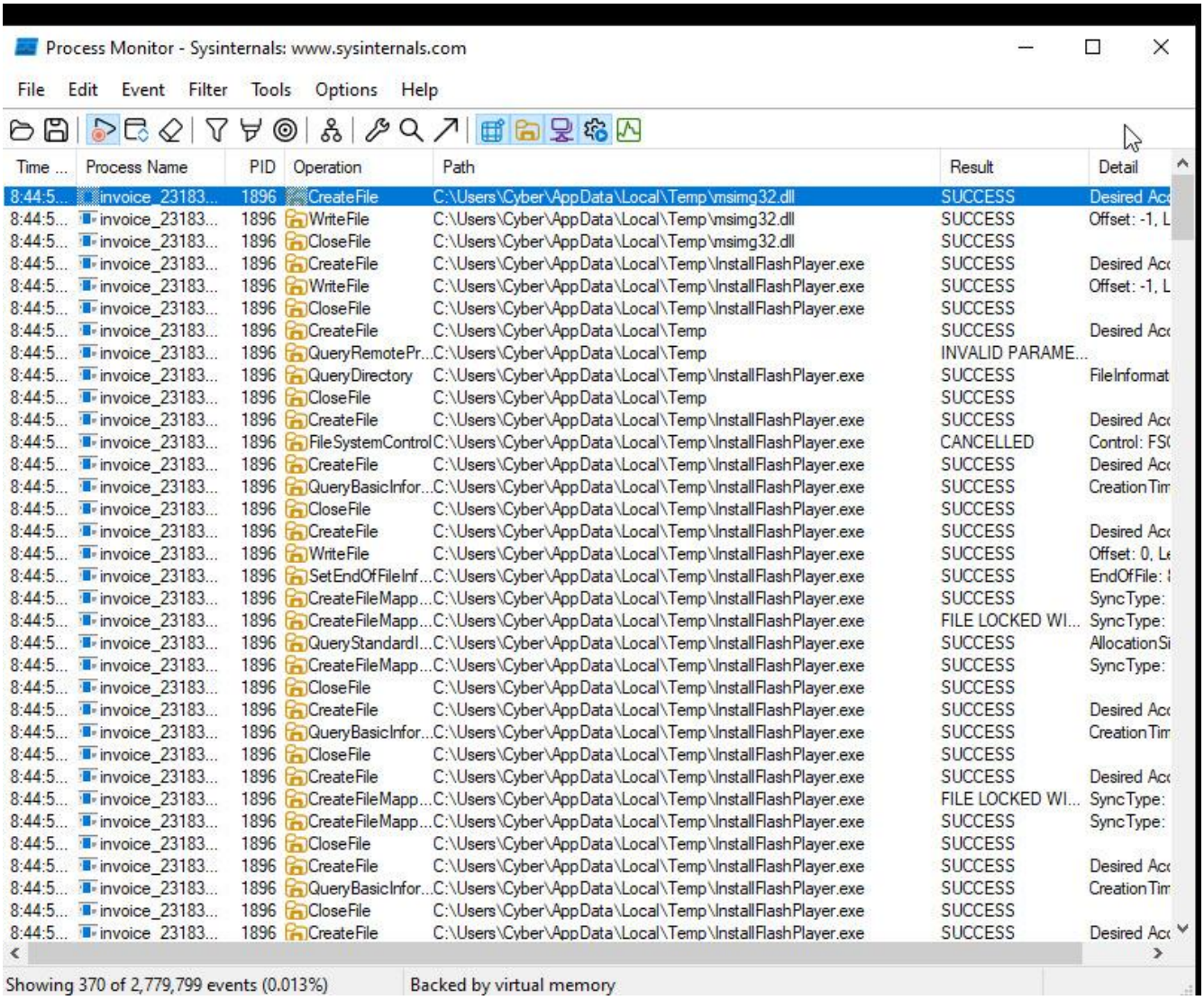
gettickcount is an api call function that tels how long the machine is powered up

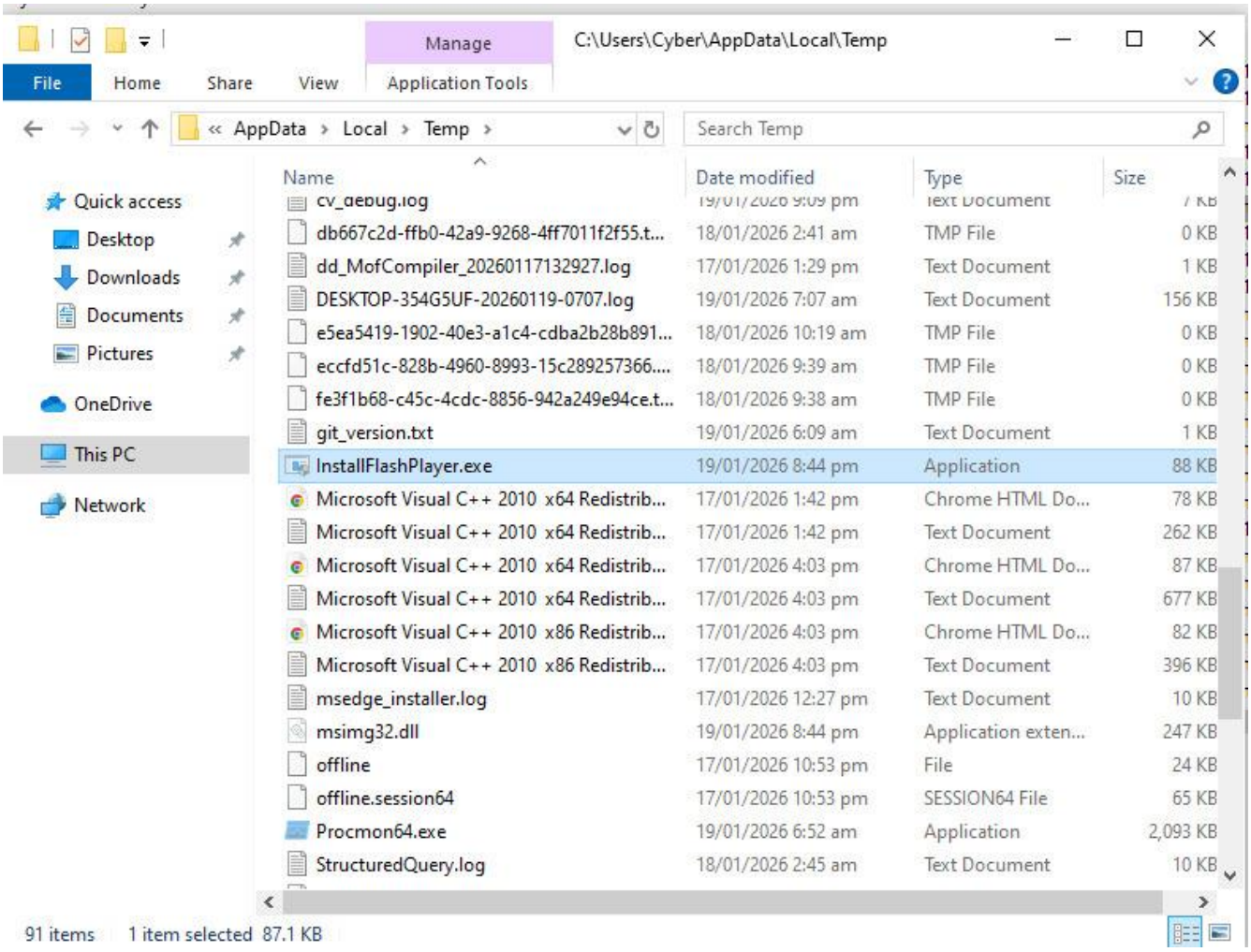
Basic Dynamic Analysis

Process Monitor procmon.

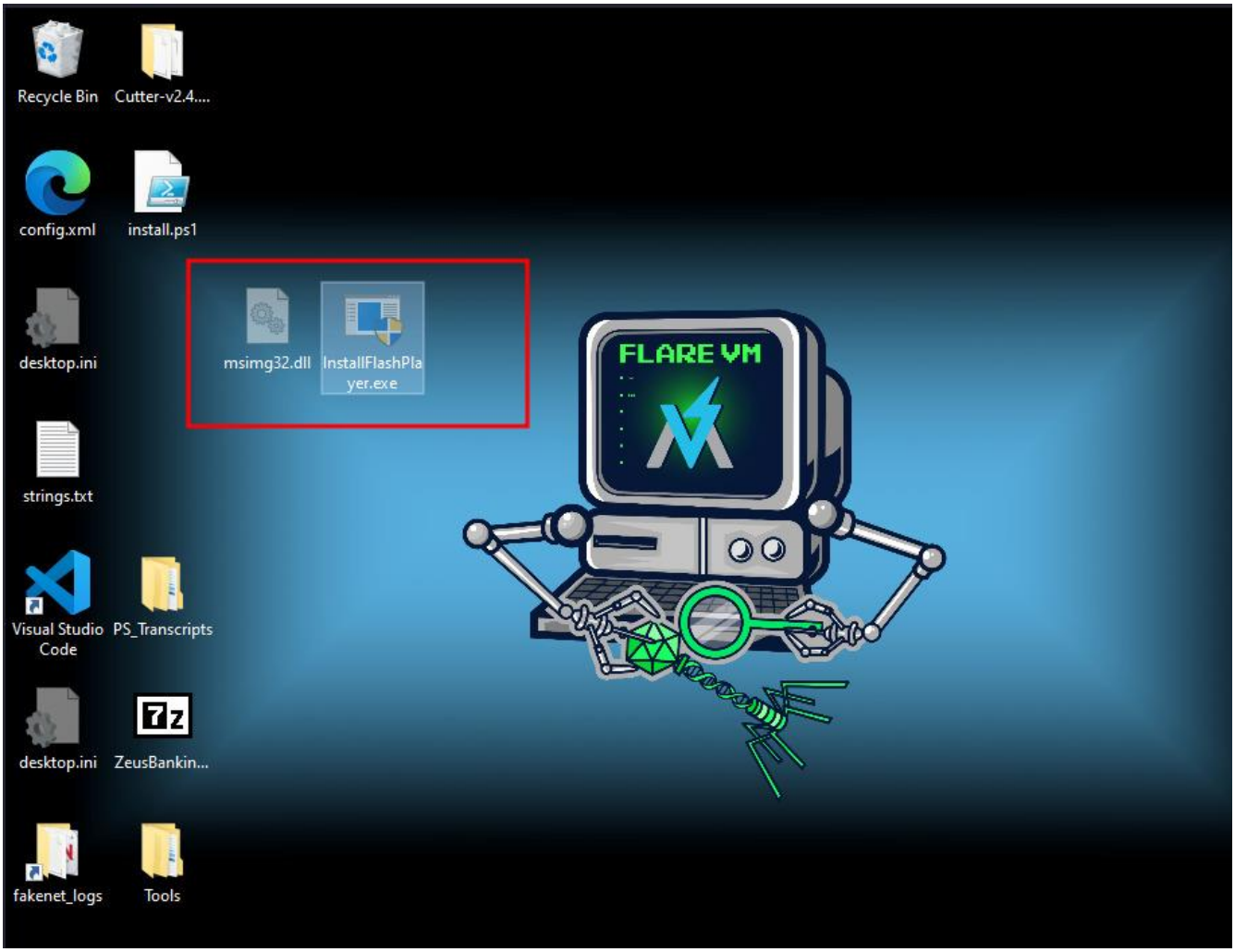


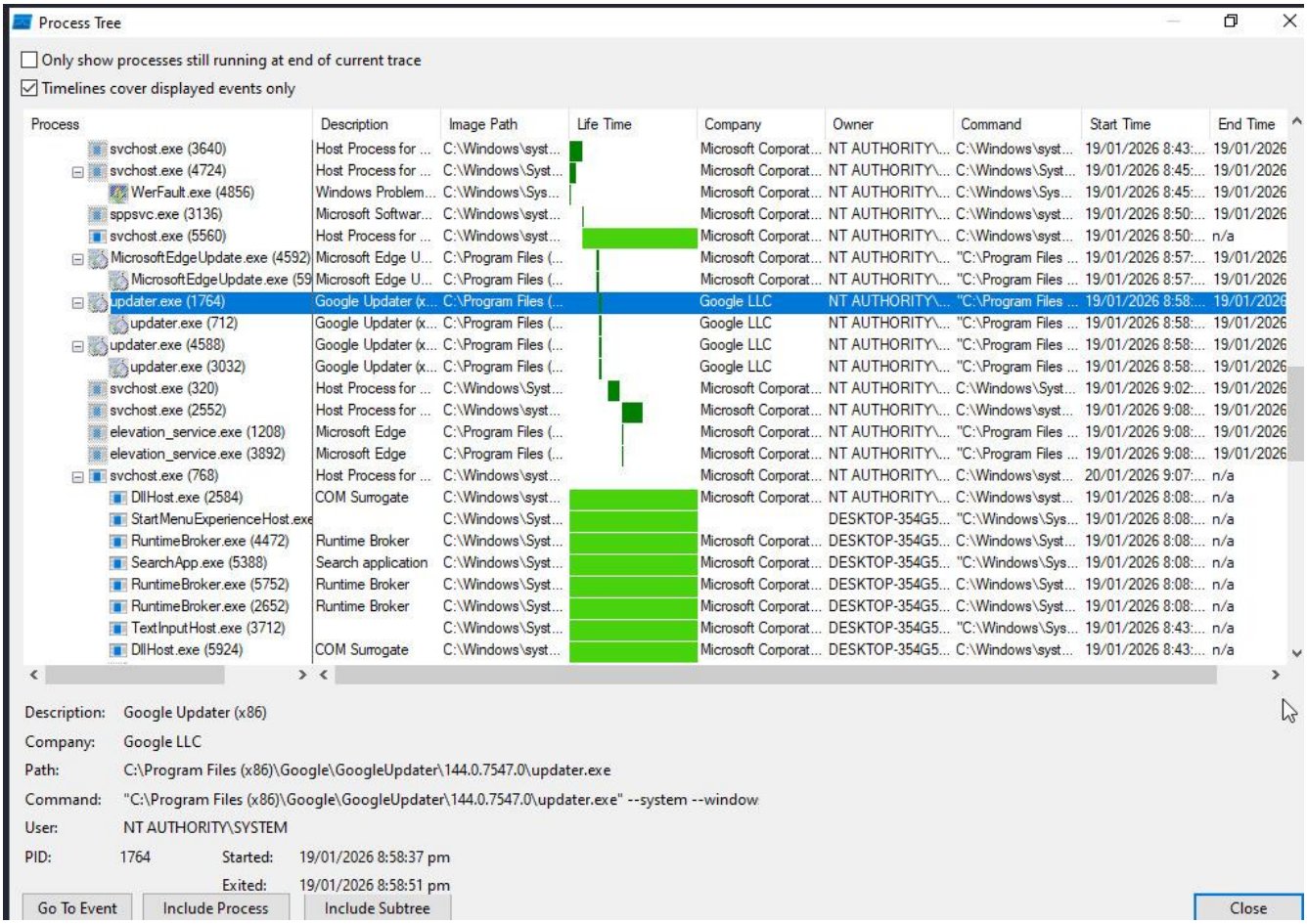

Process Tree
Only show processes still running at end of current trace
Timelines cover displayed events only
Process
Description
Image Path
Life Time
Company
Owner
Command
Start Time
End Time
msedge.exe (2668) Microsoft Edge C:\Program Files (... Microsoft Corporat... DESKTOP-354G5... "C:\Program Files ... 19/01/2026 9:09:... 19/01/2026 9:09:19 pm
msedge.exe (2232) Microsoft Edge C:\Program Files (... Microsoft Corporat... DESKTOP-354G5... "C:\Program Files ... 19/01/2026 9:09:... 19/01/2026 9:09
Procmon64.exe (4524) Process Monitor C:\Tools\sysintem... Sysinternals - ww... DESKTOP-354G5... "C:\Tools\sysinter... 19/01/2026 8:44:... n/a
invoice_2318362983713_8239 C:\Users\Cyber\D... DESKTOP-354G5... "C:\Users\Cyber\... 19/01/2026 8:44:... 19/01/2026 8:45
InstallFlashPlayer.exe (4172 Adobe® Flash® Pl... C:\Users\Cyber\A... Adobe Systems, I... DESKTOP-354G5... "C:\Users\Cyber\... 19/01/2026 8:45:... 19/01/2026 8:45
InstallFlashPlayer.exe (1 Adobe® Flash® Pl... C:\Users\Cyber\A... Adobe Systems, I... DESKTOP-354G5... "C:\Users\Cyber\... 19/01/2026 8:45:... n/a
WerFault.exe (4528) Windows Problem... C:\Windows\Sys... Microsoft Corporat... DESKTOP-354G5... C:\Windows\Sys... 19/01/2026 8:45:... 19/01/2026 8:45
cmd.exe (1708) Windows Comma... C:\Windows\Sys... Microsoft Corporat... DESKTOP-354G5... "C:\Windows\syst... 19/01/2026 8:45:... 19/01/2026 8:45
Conhost.exe (112) Console Window ... C:\Windows\Syst... Microsoft Corporat... DESKTOP-354G5... \??\C:\Windows\... 19/01/2026 8:45:... 19/01/2026 8:45
Idle (0) Idle 20/01/2026 9:07:... n/a
System (4) System NT AUTHORITY\... 20/01/2026 9:07:... n/a
Registry (92) Registry NT AUTHORITY\... 20/01/2026 9:07:... n/a
smss.exe (312) Windows Session ... C:\Windows\Syst... Microsoft Corporat... NT AUTHORITY\... \SystemRoot\Syst... 20/01/2026 9:07:... n/a
csrss.exe (416) Client Server Runt... C:\Windows\syst... Microsoft Corporat... NT AUTHORITY\... %SystemRoot%\s... 20/01/2026 9:07:... n/a
wininit.exe (492) Windows Start-Up... C:\Windows\syst... Microsoft Corporat... NT AUTHORITY\... wininit.exe 20/01/2026 9:07:... n/a
services.exe (632) Services and Cont... C:\Windows\syst... Microsoft Corporat... NT AUTHORITY\... C:\Windows\syst... 20/01/2026 9:07:... n/a
svchost.exe (1584) Host Process for ... C:\Windows\Syst... Microsoft Corporat... NT AUTHORITY\... C:\Windows\Syst... 19/01/2026 8:07:... n/a
AUDIODG.EXE (5720) Windows Audio D... C:\Windows\syst... Microsoft Corporat... NT AUTHORITY\... C:\Windows\syst... 19/01/2026 8:44:... 19/01/2026 8:50
svchost.exe (1632) Host Process for ... C:\Windows\Syst... Microsoft Corporat... NT AUTHORITY\... C:\Windows\Syst... 19/01/2026 8:07:... n/a
svchost.exe (1644) Host Process for ... C:\Windows\syst... Microsoft Corporat... NT AUTHORITY\... C:\Windows\syst... 19/01/2026 8:07:... n/a
svchost.exe (1768) Host Process for ... C:\Windows\Syst... Microsoft Corporat... NT AUTHORITY\... C:\Windows\Syst... 19/01/2026 8:07:... n/a
svchost.exe (1860) Host Process for ... C:\Windows\syst... Microsoft Corporat... NT AUTHORITY\... C:\Windows\syst... 19/01/2026 8:07:... n/a
svchost.exe (1868) Host Process for ... C:\Windows\syst... Microsoft Corporat... NT AUTHORITY\... C:\Windows\syst... 19/01/2026 8:07:... n/a
spoolsv.exe (1876) Spooler SubSyste... C:\Windows\Syst... Microsoft Corporat... NT AUTHORITY\... C:\Windows\Syst... 19/01/2026 8:07:... n/a
Description: Adobe® Flash® Player Installer/Uninstaller 11.0 r1
Company: Adobe Systems, Inc.
Path: C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe
Command: "C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe"
User: DESKTOP-354G5UF\Cyber
PID: 1700 Started: 19/01/2026 8:45:22 pm
Go To Event
Include Process
Include Subtree
Close


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp\msimg32.dll SUCCESS Desired Acc
8:44:5... invoice_23183... 1896 WriteFile C:\Users\Cyber\AppData\Local\Temp\msimg32.dll SUCCESS Offset: -1, L
8:44:5... invoice_23183... 1896 CloseFile C:\Users\Cyber\AppData\Local\Temp\msimg32.dll SUCCESS
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Desired Acc
8:44:5... invoice_23183... 1896 WriteFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Offset: -1, L
8:44:5... invoice_23183... 1896 CloseFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp SUCCESS Desired Acc
8:44:5... invoice_23183... 1896 QueryRemotePr... C:\Users\Cyber\AppData\Local\Temp INVALID PARAME...
8:44:5... invoice_23183... 1896 QueryDirectory C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS FileInformat
8:44:5... invoice_23183... 1896 CloseFile C:\Users\Cyber\AppData\Local\Temp SUCCESS
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Desired Acc
8:44:5... invoice_23183... 1896 FileSystemControl C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe CANCELLED Control: FS
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Desired Acc
8:44:5... invoice_23183... 1896 QueryBasicInfor... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS CreationTim
8:44:5... invoice_23183... 1896 CloseFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Desired Acc
8:44:5... invoice_23183... 1896 WriteFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Offset: 0, Le
8:44:5... invoice_23183... 1896 SetEndOfFileInf... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS EndOfFile:
8:44:5... invoice_23183... 1896 CreateFileMapp... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS SyncType:
8:44:5... invoice_23183... 1896 CreateFileMapp... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe FILE LOCKED WI... SyncType:
8:44:5... invoice_23183... 1896 QueryStandardI... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS AllocationSi
8:44:5... invoice_23183... 1896 CreateFileMapp... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS SyncType:
8:44:5... invoice_23183... 1896 CloseFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Desired Acc
8:44:5... invoice_23183... 1896 QueryBasicInfor... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS CreationTim
8:44:5... invoice_23183... 1896 CloseFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Desired Acc
8:44:5... invoice_23183... 1896 CreateFileMapp... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe FILE LOCKED WI... SyncType:
8:44:5... invoice_23183... 1896 CreateFileMapp... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS SyncType:
8:44:5... invoice_23183... 1896 CloseFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Desired Acc
8:44:5... invoice_23183... 1896 QueryBasicInfor... C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS CreationTim
8:44:5... invoice_23183... 1896 CloseFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
8:44:5... invoice_23183... 1896 CreateFile C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS Desired Acc
Showing 370 of 2,779,799 events (0.013%)
Backed by virtual memory



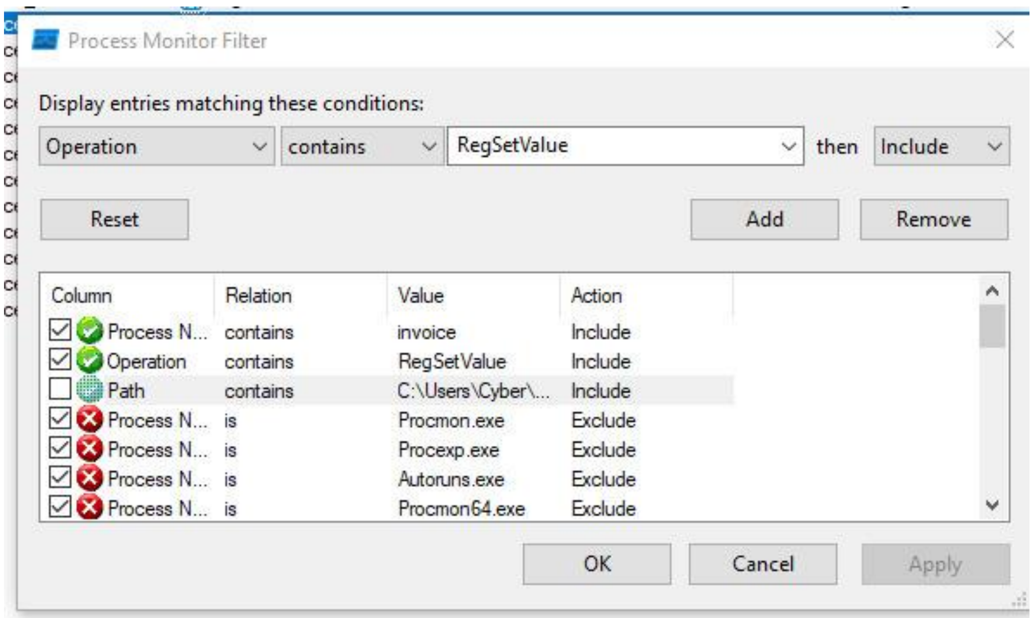
Invoice is downloading some different programs .
Specifically install adobe flashplayer

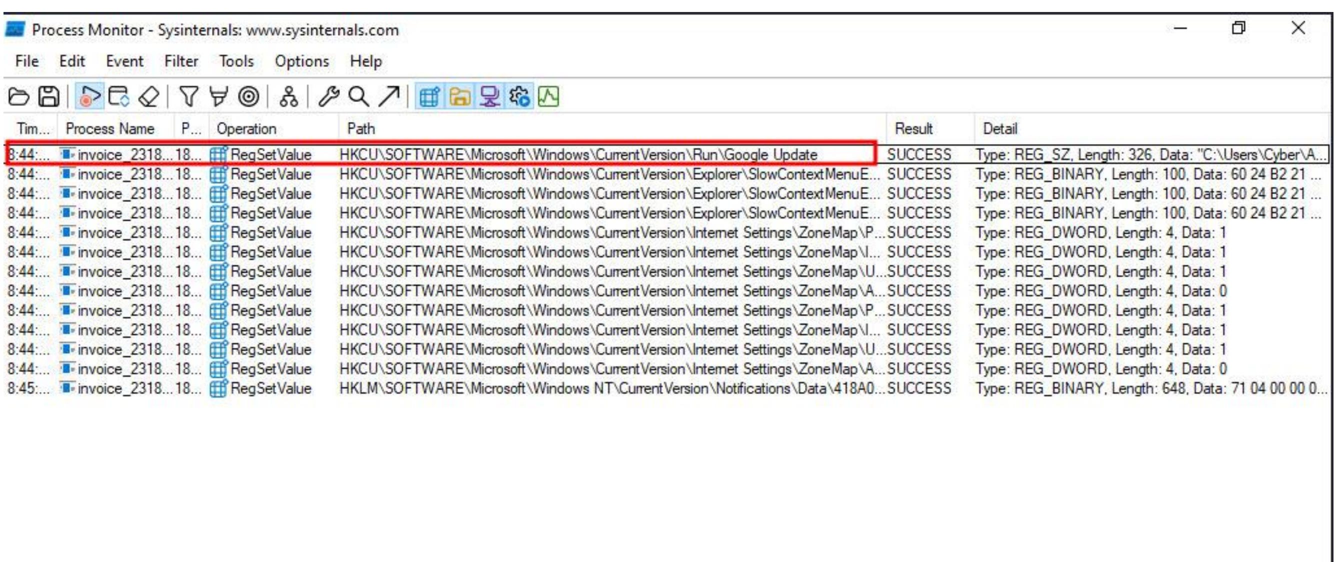

Recycle Bin
Cutter-v2.4....
config.xml
install.ps1
desktop.ini
msimg32.dll
InstallFlashPlayer.exe
strings.txt
Visual Studio Code
PS_Transcripts
desktop.ini
ZeusBankin...
fakenet_logs
Tools
FLARE VM



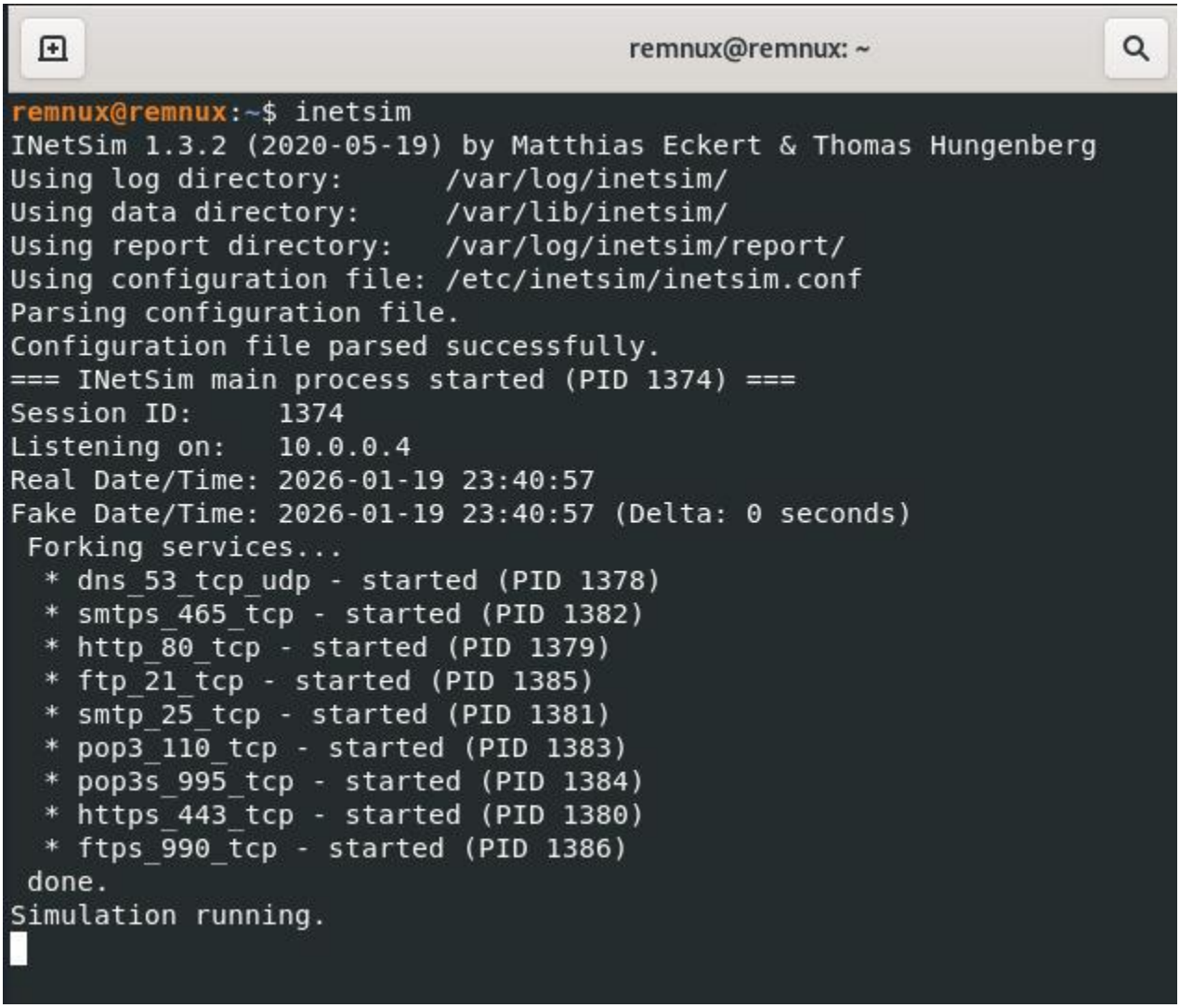
every time the google chrome is updated the binary executable will be executed.

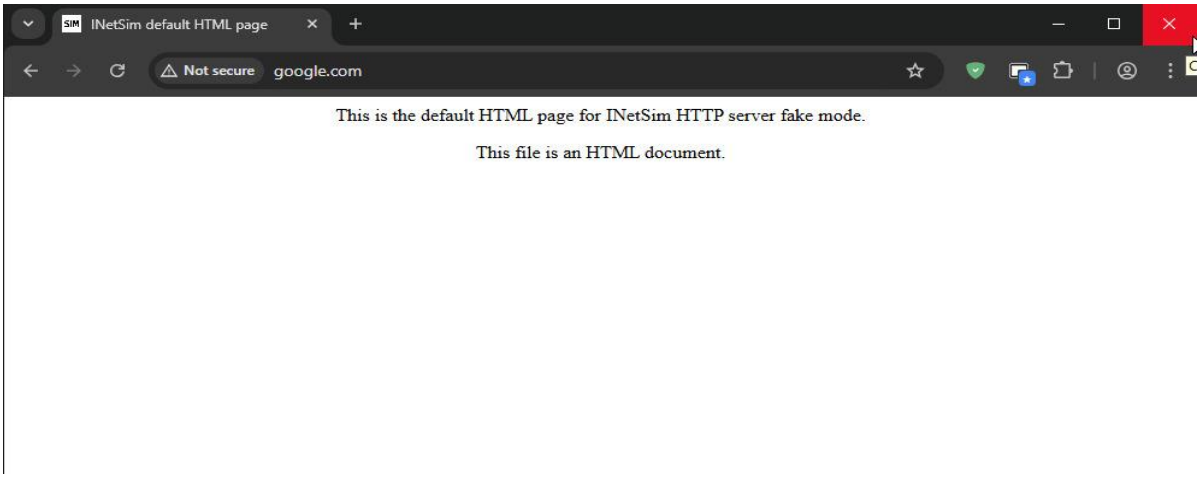
Registery Keys:



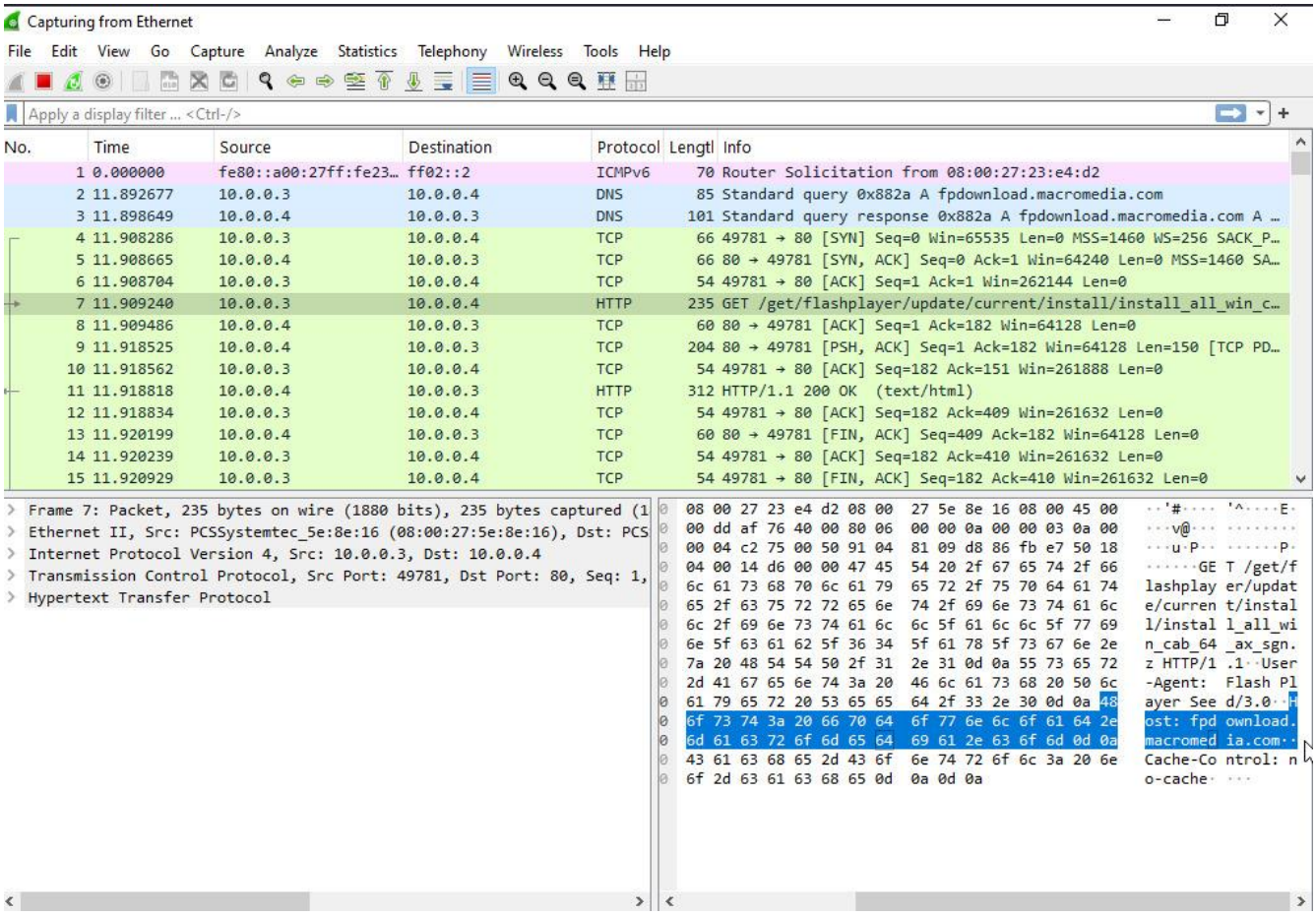


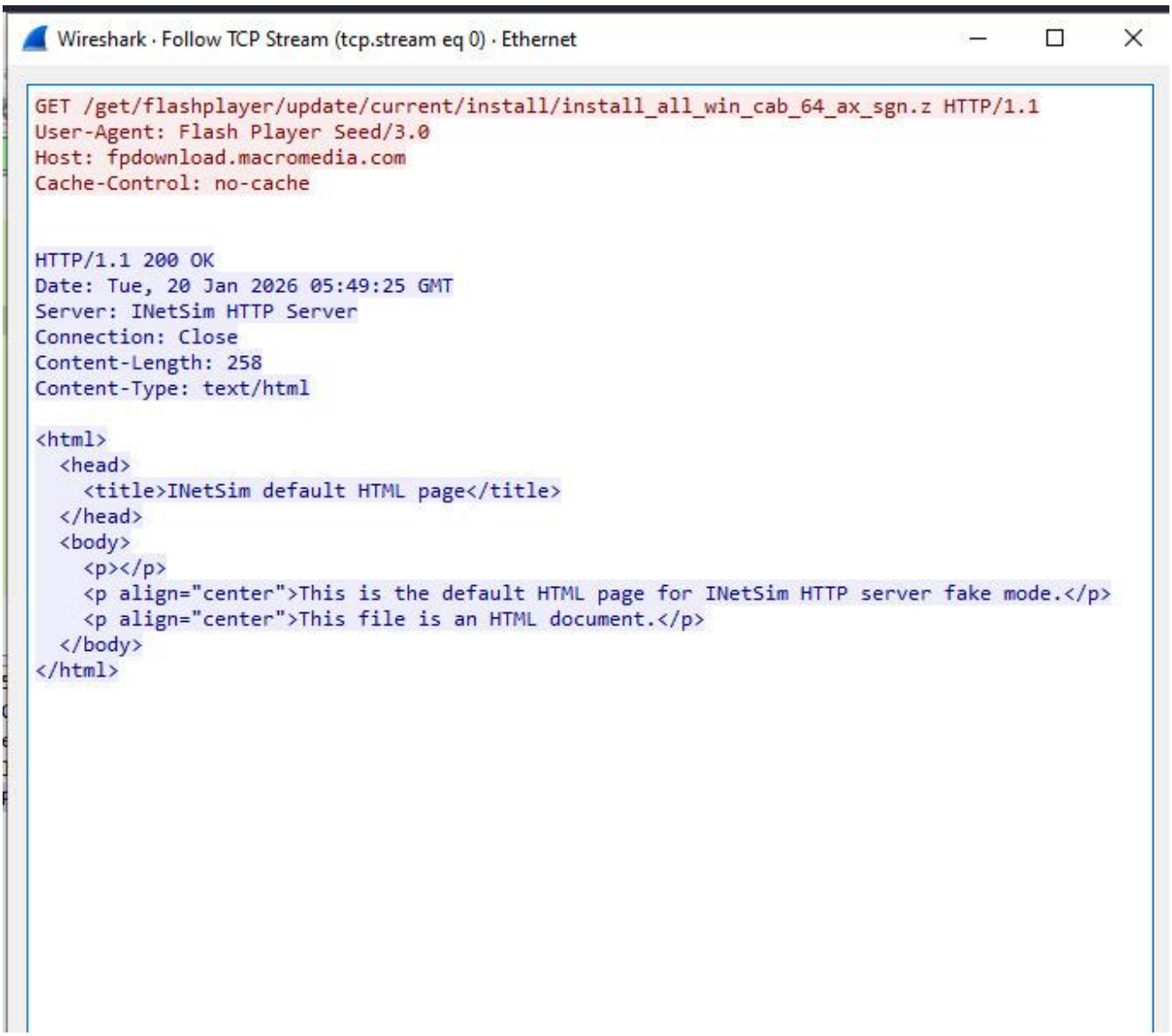
Remnux as a DNS Server:





Network Based Indicators
Wireshark:




Wireshark · Follow TCP Stream (tcp.stream eq 0) · Ethernet
GET /get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z HTTP/1.1
User-Agent: Flash Player Seed/3.0
Host: fpdownload.macromedia.com
Cache-Control: no-cache
HTTP/1.1 200 OK
Date: Tue, 20 Jan 2026 05:49:25 GMT
Server: INetSim HTTP Server
Connection: Close
Content-Length: 258
Content-Type: text/html
<html>
<head>
<title>INetSim default HTML page</title>
</head>
<body>

This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
</body>
</html>