ID: 680567
Sample Name:
Gulvmaattens.exe
Cookbook: default.jbs
Time: 20:15:08
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

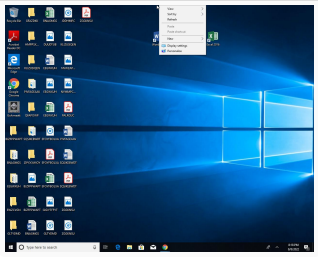
Windows Analysis Report

Gulvmaattens.exe

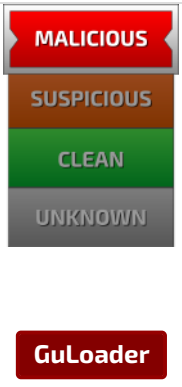
Overview

General Information

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



Detection



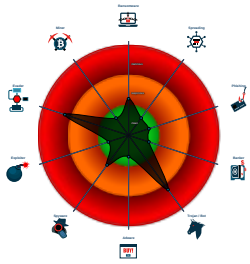
GuLoader

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Mass process execution to delay an…
- Obfuscated command line found
- Tries to detect virtualization through…
- Uses 32bit PE files
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- PE file contains sections with non-s…
- Binary contains a suspicious time s…
- Detected potential crypto function
- Too many similar processes found

Classification



Process Tree

- **System is w10x64**
- Gulvmaattens.exe (PID: 800 cmdline: "C:\Users\user\Desktop\Gulvmaattens.exe" MD5: AFA8D5C2F8F14ED458EA6D8547FE57A8)
  - cmd.exe (PID: 3556 cmdline: cmd.exe /c set /a "0x78^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 3028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4736 cmdline: cmd.exe /c set /a "0x76^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1212 cmdline: cmd.exe /c set /a "0x61^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 3064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 824 cmdline: cmd.exe /c set /a "0x7D^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 3304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1772 cmdline: cmd.exe /c set /a "0x76^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4388 cmdline: cmd.exe /c set /a "0x7F^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 2756 cmdline: cmd.exe /c set /a "0x00^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 1400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5444 cmdline: cmd.exe /c set /a "0x01^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 60 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6092 cmdline: cmd.exe /c set /a "0x09^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 3468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4432 cmdline: cmd.exe /c set /a "0x09^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 1820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1772 cmdline: cmd.exe /c set /a "0x70^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 3516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5872 cmdline: cmd.exe /c set /a "0x41^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4688 cmdline: cmd.exe /c set /a "0x56^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1400 cmdline: cmd.exe /c set /a "0x52^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 2756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4752 cmdline: cmd.exe /c set /a "0x47^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 1600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5416 cmdline: cmd.exe /c set /a "0x56^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1956 cmdline: cmd.exe /c set /a "0x75^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 1188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4736 cmdline: cmd.exe /c set /a "0x5A^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)

- Conhost.exe (PID: 3516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5876 cmdline: cmd.exe /c set /a "0x5F^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5444 cmdline: cmd.exe /c set /a "0x56^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 412 cmdline: cmd.exe /c set /a "0x72^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5140 cmdline: cmd.exe /c set /a "0x1B^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 804 cmdline: cmd.exe /c set /a "0x5E^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1956 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3276 cmdline: cmd.exe /c set /a "0x41^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5144 cmdline: cmd.exe /c set /a "0x07^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3304 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1008 cmdline: cmd.exe /c set /a "0x1F^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3284 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 2056 cmdline: cmd.exe /c set /a "0x5A^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1672 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1956 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4432 cmdline: cmd.exe /c set /a "0x4B^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5736 cmdline: cmd.exe /c set /a "0x0B^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5156 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5652 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3524 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5444 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1696 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3272 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5816 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4736 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3024 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3020 cmdline: cmd.exe /c set /a "0x1F^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5848 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5444 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4008 cmdline: cmd.exe /c set /a "0x5A^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3956 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5084 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5436 cmdline: cmd.exe /c set /a "0x1F^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 2512 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4764 cmdline: cmd.exe /c set /a "0x43^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3580 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5152 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3464 cmdline: cmd.exe /c set /a "0x1F^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3444 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3336 cmdline: cmd.exe /c set /a "0x5A^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5972 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1424 cmdline: cmd.exe /c set /a "0x07^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- cmd.exe (PID: 5392 cmdline: cmd.exe /c set /a "0x1F^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1324 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5836 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5484 cmdline: cmd.exe /c set /a "0x5A^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1544 cmdline: cmd.exe /c set /a "0x13^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5736 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5672 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3656 cmdline: cmd.exe /c set /a "0x4B^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 2028 cmdline: cmd.exe /c set /a "0x0B^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3252 cmdline: cmd.exe /c set /a "0x03^51" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.626525207.0000000000760000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Data Obfuscation

Yara detected GuLoader

Obfuscated command line found

Malware Analysis System Evasion

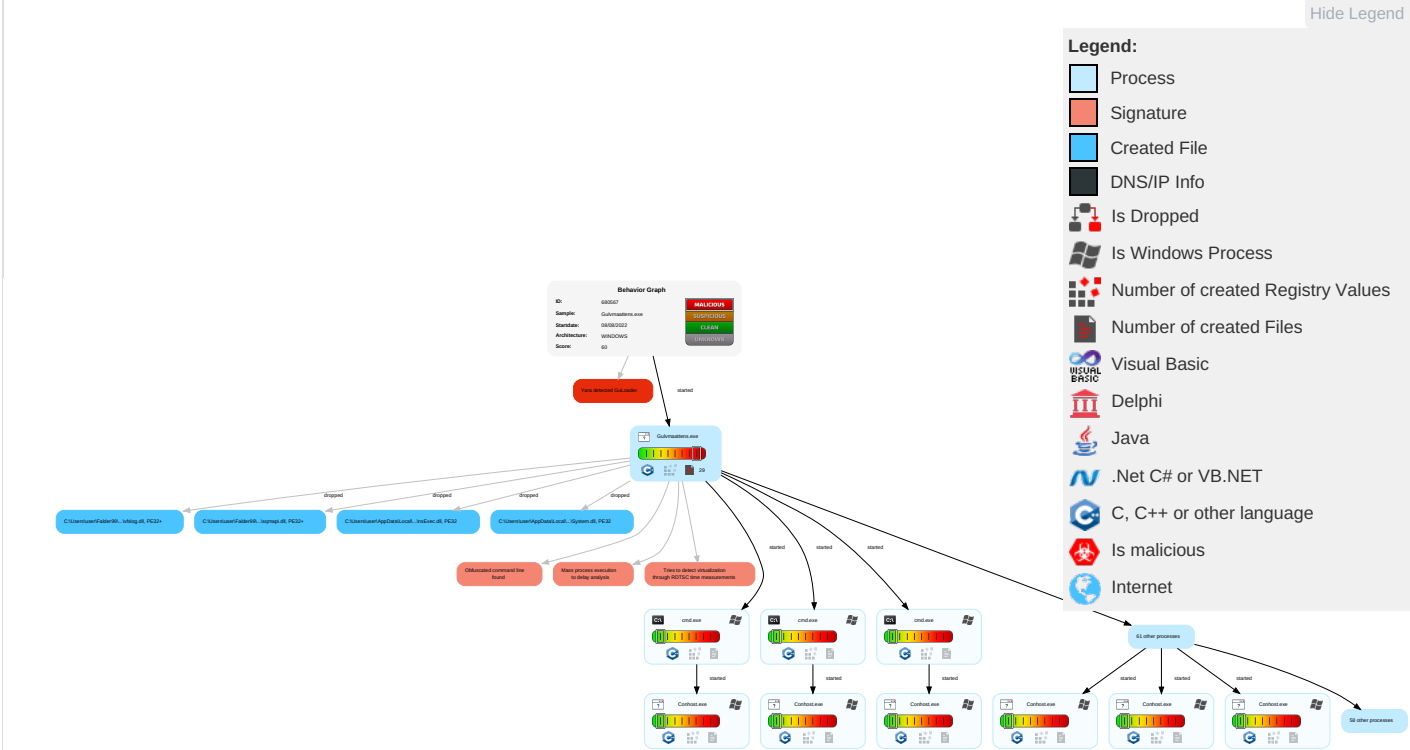
Mass process execution to delay analysis

Tries to detect virtualization through RDTSC time measurements

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	1 Command and Scripting Interpreter	Path Interception	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Access Token Manipulation	LSASS Memory	1 Time Based Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Time Based Evasion	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Timestomp	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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	3%	Virustotal		Browse
Gulvmaattens.exe	2%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nso786B.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nso786B.tmp\System.dll	4%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nso786B.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nso786B.tmp\nsExec.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nso786B.tmp\nsExec.dll	8%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nso786B.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://subca.ocsp-certum.com05	0%	URL Reputation	safe	
http://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.pl/ctnca2.crl0l	Gulvmaattens.exe	false		high
http://repository.certum.pl/ctnca2.cer09	Gulvmaattens.exe	false		high
http://crl.certum.pl/ctsca2021.crl0o	Gulvmaattens.exe	false		high
http://repository.certum.pl/ctnca.cer09	Gulvmaattens.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	Gulvmaattens.exe	false		high
http://repository.certum.pl/ctsca2021.cer0	Gulvmaattens.exe	false		high
http://crl.certum.pl/ctnca.crl0k	Gulvmaattens.exe	false		high
http://subca.ocsp-certum.com05	Gulvmaattens.exe	false	• URL Reputation: safe	unknown
http://www.certum.pl/CPS0	Gulvmaattens.exe	false		high
http://subca.ocsp-certum.com02	Gulvmaattens.exe	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com01	Gulvmaattens.exe	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680567
Start date and time: 08/08/202220:15:08	2022-08-08 20:15:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s
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 v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	148
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:	mal60.troj.evad.winEXE@412/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.6% (good quality ratio 61.1%) • Quality average: 88.1% • Quality standard deviation: 21.8%
HCA Information:	• Successful, ratio: 100% • 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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nso786B.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: Virustotal, Detection: 0%, Browse • 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\nso786B.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: Virustotal, Detection: 0%, Browse • 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+UItxzCyfw2ZLYQeQD5u
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:	A573ABCC7D3DFE8656C537F9E6C40AC6F20B388C623258B5D84D6896F6A3557DFE8E89953F7F5D8BFE786F1F88EB2077D8DF41E79021094CA7F66B7DBD8113 D
Malicious:	false
Preview:	8BADA3CD0CA9A9C5F29972F662F7EE72162D5B9C6B074DD2A4AA1C205FB4676D141C92F8F08065E612FDFC68E8921C12F356396296903CB92A9E9D9B E6E1006C6B2BF359513ABFE6D1BAA6F1F7C8479EA85D6802C3BBC589AED2669E4BF6F829725A13050E9D100DA41B530336B0D5D145E390952907843D E8C86D5112592FA679141E7891B3F6BE3941B0CE9D2A0075A9069124145AA17CF013656540B1FEEC0AEBABE47B070E59ECD408F4AA87160B6F5461A9 5B2213606259DCF1B3592724E8D1395E82D5B1F8AD6CD14F4898A3CEF097816C7ACEAD5A7C85C371257FD2319E4C8698B486959064928DE22A994436 58E1DB424450FB6E6A10AA43D0357678902A7FFD6A7F3EB6F91E7A34AB1EDAB7B4726C28EF0A44E2DADE4761AAA53AD216CF84B3149FAAF0C5CDD72F 1B246B29A0A7A21AB0F751843071C8BF8D8B106FA94A55F52F06987F275D3DF7CB6C1904FF3D45D3D83B858241F3DCCB1D48DC37333066E5627B763B E7BDB14771FFD0D9ACC4956ADB62EEFB7F464359BE5D40AE0176EB22F112AA3E2644139F0141F05A7ECE0C9F0B0B0FE2801C08FB57B993067067C355 0D229802BC5768BC1BEC762C6521B08130E8B4109B6861A7C31B64F8F176344C1DCF52358AF03845C4B9812BEE3C3ACE4D3F803D25B043D4BDC4275D 6116B505A86EEC034BA2955A66E8F542B0A3680C

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:	8F19B196EC5D282C28199AD0391B13C4977190B3AF5A6BB732DA8EFC24DE6AC5A0632D74209A8F5382F98F9FEBCFB619CEA006ECB682476B0FB10447A9BE8D 9A
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.A V...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+x4SekjRYJKRiISZ20pidakx9o9dAPkuFJI1PHdOC:Hf20wzjRuC0uaF9d8dFePHQ
MD5:	A5D6ECC292535D2C635EE25701238173
SHA1:	DE34B8248886E59AC72C5A1FDA9876F40312EC95
SHA-256:	E320356D53C168DB9080BB04D5E8F4CC16D66657DEEB063F9133EAC9381BDB1D
SHA-512:	E1CA3E6627C2C5D59F2EC931887F82514B850E567EF423D0F1CC763948A190ECBF0FEEC4F10FD697C35C252E56ACFC02BB7B163745946E791B11BAA467B00DF
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+hNPLutht2tJEFcRs/aP55+02MGH/WtSy4uh:STakO7te4NPwfOEEm65mgSHW
TLSH:	C67401B1DBF6D00BDAB2DA347C75530A7DEA5A62503257135305F8C8B8A22A36FCD790
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	• 8/8/2022 6:55:24 AM 8/7/2025 6:55:24 AM
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 00007FF438D5DD93h
push ebx
call 00007FF438D61081h
cmp eax, ebx
je 00007FF438D5DD89h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007FF438D60FFBh
push esi
call dword ptr [00408154h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FF438D5DD6Ch
push 0000000Bh
call 00007FF438D61054h
push 00000009h
call 00007FF438D6104Dh
push 00000007h
mov dword ptr [00434F04h], eax
call 00007FF438D61041h
cmp eax, ebx
je 00007FF438D5DD91h
push 0000001Eh
call eax
test eax, eax
je 00007FF438D5DD89h
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

Instruction
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	
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

Name	RVA	Size	Type	Language	Country
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
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

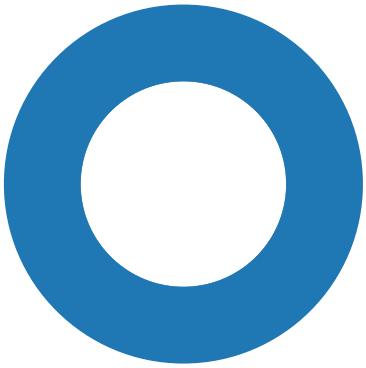
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- 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

Click to jump to process

System Behavior

Analysis Process: Gulvmaattens.exe PID: **800**, Parent PID: **5748**

General

Target ID:	0
Start time:	20:16:14
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: 00000000.00000002.626525207.0000000000760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4059D1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsp6DDB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405F75	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4059D1	CreateDirectoryW

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	3	4059D1	CreateDirectoryW
C:\Users\user\Falder99	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4059D1	CreateDirectoryW
C:\Users\user\Falder99\Interelectrode	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4059D1	CreateDirectoryW
C:\Users\user\Falder99\Interelectrode\Overvejendes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4059D1	CreateDirectoryW
C:\Users\user\Falder99	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4059D1	CreateDirectoryW
C:\Users\user\Falder99\Interelectrode	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4059D1	CreateDirectoryW
C:\Users\user\Falder99\Interelectrode\Overvejendes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4059D1	CreateDirectoryW
C:\Users\user\Falder99\Interelectrode\Overvejendes\Pleasurelessly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4059D1	CreateDirectoryW
C:\Users\user\Falder99\Interelectrode\Overvejendes\Pleasurelessly\Anodiserende.opa	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\Falder99\Interelectrode\Overvejendes\Airplane_2.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\Falder99\Interelectrode\Overvejendes\Dystomic.Bel	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\Falder99\Interelectrode\Overvejendes\english.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\Falder99\Interelectrode\Overvejendes\sqmapi.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\Falder99\Interelectrode\Overvejendes\vfslog.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\AppData\Local\Temp\nso786B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405F75	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4059D1	CreateDirectoryW

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	4059D1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4059D1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4059D1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4059D1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nso786B.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405991	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nso786B.tmp\nsExec.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\AppData\Local\Temp\nso786B.tmp\nsExec.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	295	405F33	CreateFileW
C:\Users\user\AppData\Local\Temp\nso786B.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\AppData\Local\Temp\nso786B.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405F33	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsp6DDB.tmp	success or wait	1	403774	DeleteFileW
C:\Users\user\AppData\Local\Temp\nso786B.tmp	success or wait	1	405B52	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Falder99\Interelectrode\Overvejendes\Pleasurelessly\Anodiserende.opa	0	22330	fd 74 fd 1c fd fd 41 59 4d fd 47 5b 5d 0b 58 fd fd 10 fd 5b 22 07 fd fd fd 57 fd 38 fd fd 5e 7e 28 23 25 30 7f fd fd f4 0f 60 fd 23 16 fd 1f fd 0b 50 7e 09 fd 31 fd 7b fd fd 19 fd 4f 47 fd fd 7d fd fd fd 4d 5a 4e fd fd 3e 31 1a fd 38 fd 1c 4e 55 fd fd fd ec fd 08 53 fd 0c fd 23 c6 73 fd 09 fd fd 4c fd 4a 0f fd 5e fd 76 fd 17 38 fd fd 7b fd 76 5e 2a fd fd fd 5b fd 0e 4a fd fd 39 fd fd fd 29 54 02 fd 05 6d fd fd 6a fd 56 fd 3b fd fd 26 fd fd 37 fd 5a fd 61 42 fd 8e 0c 5b 36 7e 75 0a 7e 62 d7 fd fd fd fd 72 06 fd 59 5b 0e 4d fd fd fd 00 4d fd fd 04 78 fd fd 31 fd 41 56 fd 13 1f 4f fd 36 fd 7f 0d fd fd fd fd 73 1d 43 21 3d fd fd 56 fd 6f fd 0f fd fd 00 42 51 58 fd 04 02 fd 0f 2a 10 fd 19 fd 41 fd 23 fd fd fd 50 fd 3e fd 00	tAYMG[]X["W8^~(#%0`#P~1{OG}ZN>18NUS#sLJ^v8{v^*[J9)TmjV;&7ZaB[6~u~brY[MMx1AVO6sC!=VoBQX*A#P>	success or wait	6	405FD3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Falder99\Interelectrode\Overvejendes\Airplane_2.bmp	0	8416	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00	JFIFdd:ExifMM*QQaQaCCnn"	success or wait	1	405FD3	WriteFile
C:\Users\user\Falder99\Interelectrode\Overvejendes\Dystomic.Bel	0	28195	38 42 41 44 41 33 43 44 30 43 41 39 41 39 43 35 46 32 39 39 37 32 46 36 36 32 46 37 45 45 37 32 31 36 32 44 35 42 39 43 36 42 30 37 34 44 44 32 41 34 41 41 31 43 32 30 35 46 42 34 36 37 36 44 31 34 31 43 39 32 46 38 46 30 38 30 36 35 45 36 31 32 46 44 46 43 36 38 45 38 39 32 31 43 31 32 46 33 35 36 33 39 36 32 39 36 39 30 33 43 42 39 32 41 39 45 39 44 39 42 45 36 45 31 30 30 36 43 36 42 32 42 46 33 35 39 35 31 33 41 42 46 45 36 44 31 42 41 41 36 46 31 46 37 43 38 34 37 39 45 41 38 35 44 36 38 30 32 43 33 42 42 43 35 38 39 41 45 44 32 36 36 39 45 34 42 46 36 46 38 32 39 37 32 35 41 31 33 30 35 30 45 39 44 31 30 30 44 41 34 31 42 35 33 30 33 33 36 42 30 44 35 44 31 34 35 45 33 39 30 39 35 32 39 30 37 38 34 33 44 45 38 43 38 36 44 35 31 31 32 35 39 32 46 41	8BADA3CD0CA9A9C5F29972F662F7EE72162D5B9C6B074DD2A4AA1C205FB4676D141C92F8F08065E612FDFC68E8921C12F356396296903CB92A9E9D9BE6E1006C6B2BF359513ABFE6D1BAA6F1F7C8479EA85D6802C3BBC589AED2669E4BF6F829725A13050E9D100DA41B530336B0D5D145E390952907843DE8C86D5112592FA	success or wait	2	405FD3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Falder99\Interelectrode\Overvejendes\english.txt	0	13116	61 62 61 6e 64 6f 6e 0a 61 62 69 6c 69 74 79 0a 61 62 6c 65 0a 61 62 6f 75 74 0a 61 62 6f 76 65 0a 61 62 73 65 6e 74 0a 61 62 73 6f 72 62 0a 61 62 73 74 72 61 63 74 0a 61 62 73 75 72 64 0a 61 62 75 73 65 0a 61 63 63 65 73 73 0a 61 63 63 69 64 65 6e 74 0a 61 63 63 6f 75 6e 74 0a 61 63 63 75 73 65 0a 61 63 68 69 65 76 65 0a 61 63 69 64 0a 61 63 6f 75 73 74 69 63 0a 61 63 71 75 69 72 65 0a 61 63 72 6f 73 73 0a 61 63 74 0a 61 63 74 69 6f 6e 0a 61 63 74 6f 72 0a 61 63 74 72 65 73 73 0a 61 63 74 75 61 6c 0a 61 64 61 70 74 0a 61 64 64 0a 61 64 64 69 63 74 0a 61 64 64 72 65 73 73 0a 61 64 6a 75 73 74 0a 61 64 6d 69 74 0a 61 64 75 6c 74 0a 61 64 76 61 6e 63 65 0a 61 64 76 69 63 65 0a 61 65 72 6f 62 69 63 0a 61 66 66 61 69 72 0a 61 66 66 6f 72 64 0a 61 66 72 61 69	abandonabilityableaboutaboveabsentabsorbabstractabsurdabuseaccessaccidentaccountaccuseachieveacidacousticacquireacrossactactionactoractressactualadaptaddaddictaddressadjustadmitadultadvanceadviceaerobicaffairaffordafrai	success or wait	1	405FD3	WriteFile
C:\Users\user\Falder99\Interelectrode\Overvejendes\sqmapi.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 0f fd fd fd 6e fd fd fd 6e fd fd fd 6e fd fd fd 05 6d fd fd 6e fd fd fd 05 fd fd fd 6e fd fd fd 05 fd fd fd 6e fd fd fd 6e fd fd 76 6e fd fd fd 05 fd fd fd 6e fd fd fd 05 fd fd fd 6e fd fd fd 05 fd fd fd 6e fd fd fd 05 fd fd fd 6e fd fd fd 05 6f fd fd 6e fd fd fd 05 fd fd fd 6e fd fd 52 69 63 68 fd 6e fd fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 fd 62 fd fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$nnnmnnnnvnnnnnonnRichnPEdb	success or wait	3	405FD3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Falder99\Interelectrode\Overvejendes\vfslog.dll	0	30459	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 13 00 73 4c fd 60 00 fd 03 00 54 06 00 00 fd 00 26 20 0b 02 02 24 00 fd 00 00 00 fd 00 00 00 0c 00 00 50 13 00 00 00 10 00 00 00 00 65 01 02 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 04 00 00 06 00 00 60 fd 04 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdsL`T& $Pe``	success or wait	12	405FD3	WriteFile
C:\Users\user\AppData\Local\Temp\nso786B.tmp\nsExec.dll	0	7168	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2c fd fd fd fd fd fb ef fd fd fd fd 10 1b fd fd fd fd 52 69 63 68 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd 24 5f 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 00 0e 00 00 00 0e 00 00 00 00 00 00 fd 10 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$,RichPEL$_.!	success or wait	1	405FD3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nso786B.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd 24 5f 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 fd 29 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPEL$_.!")	success or wait	1	405FD3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Gulvmaattens.exe	unknown	512	success or wait	156	405FA4	ReadFile
C:\Users\user\Desktop\Gulvmaattens.exe	unknown	4	success or wait	2	405FA4	ReadFile
C:\Users\user\Desktop\Gulvmaattens.exe	unknown	4	success or wait	24	405FA4	ReadFile
C:\Users\user\Falder99\Interelectrode\Overvejendes\Dystomic.Bel	unknown	2	success or wait	1023	402756	ReadFile
C:\Users\user\Desktop\Gulvmaattens.exe	unknown	4	success or wait	2	405FA4	ReadFile
C:\Users\user\Desktop\Gulvmaattens.exe	unknown	4	success or wait	2	405FA4	ReadFile

Analysis Process: cmd.exe PID: **3556**, Parent PID: **800**

General

Target ID:	3
Start time:	20:16:18
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Conhost.exe PID: **3028**, Parent PID: **3556**

General

Target ID:	4
Start time:	20:16:18
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **4736**, Parent PID: **800**

General

Target ID:	5
Start time:	20:16:18
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Conhost.exe PID: **5724**, Parent PID: **4736**

General

Target ID:	6
Start time:	20:16:18
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **1212**, Parent PID: **800**

General

Target ID:	8
Start time:	20:16:19
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	

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

Analysis Process: Conhost.exe PID: **3064**, Parent PID: **1212**

General	
Target ID:	9
Start time:	20:16:19
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **824**, Parent PID: **800**

General	
Target ID:	10
Start time:	20:16:19
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Conhost.exe PID: **3304**, Parent PID: **824**

General	
Target ID:	11
Start time:	20:16:20
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **1772**, Parent PID: **800**

General	
Target ID:	12
Start time:	20:16:20
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5140**, Parent PID: **1772**

General	
Target ID:	13
Start time:	20:16:20
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4388**, Parent PID: **800**

General	
Target ID:	14
Start time:	20:16:20
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5920**, Parent PID: **4388**

General	
Target ID:	16
Start time:	20:16:21
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2756**, Parent PID: **800**

General

Target ID:	17
Start time:	20:16:21
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1400**, Parent PID: **2756**

General

Target ID:	18
Start time:	20:16:21
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5444**, Parent PID: **800**

General

Target ID:	19
Start time:	20:16:22
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **60**, Parent PID: **5444**

General	
Target ID:	20
Start time:	20:16:22
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6092**, Parent PID: **800**

General	
Target ID:	21
Start time:	20:16:22
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3468**, Parent PID: **6092**

General	
Target ID:	22
Start time:	20:16:23
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4432**, Parent PID: **800**

General	
Target ID:	23
Start time:	20:16:23
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1820**, Parent PID: **4432**

General	
Target ID:	24
Start time:	20:16:23
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1772**, Parent PID: **800**

General	
Target ID:	25
Start time:	20:16:24
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3516**, Parent PID: **1772**

General	
Target ID:	26
Start time:	20:16:24
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5872**, Parent PID: **800**

General	
Target ID:	27
Start time:	20:16:24
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **244**, Parent PID: **5872**

General	
Target ID:	28
Start time:	20:16:24
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4688**, Parent PID: **800**

General	
Target ID:	29
Start time:	20:16:25
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5844**, Parent PID: **4688**

General	
Target ID:	30
Start time:	20:16:25

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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1400**, Parent PID: **800**

General

Target ID:	31
Start time:	20:16:25
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **2756**, Parent PID: **1400**

General

Target ID:	32
Start time:	20:16:26
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4752**, Parent PID: **800**

General

Target ID:	33
Start time:	20:16:26
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	

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

Analysis Process: Conhost.exe PID: **1600**, Parent PID: **4752**

General	
Target ID:	34
Start time:	20:16:26
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5416**, Parent PID: **800**

General	
Target ID:	35
Start time:	20:16:26
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5036**, Parent PID: **5416**

General	
Target ID:	36
Start time:	20:16:27
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1956**, Parent PID: **800**

General	
Target ID:	37

Start time:	20:16:27
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1188**, Parent PID: **1956**

General

Target ID:	38
Start time:	20:16:27
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4736**, Parent PID: **800**

General

Target ID:	39
Start time:	20:16:28
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3516**, Parent PID: **4736**

General

Target ID:	40
Start time:	20:16:28
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: cmd.exe PID: **5876**, Parent PID: **800**

General	
Target ID:	42
Start time:	20:16:29
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5300**, Parent PID: **5876**

General	
Target ID:	43
Start time:	20:16:32
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5444**, Parent PID: **800**

General	
Target ID:	44
Start time:	20:16:32
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4040**, Parent PID: **5444**

General

Target ID:	45
Start time:	20:16:32
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **412**, Parent PID: **800**

General	
Target ID:	46
Start time:	20:16:33
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4724**, Parent PID: **412**

General	
Target ID:	47
Start time:	20:16:33
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5140**, Parent PID: **800**

General	
Target ID:	48
Start time:	20:16:33
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:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5660**, Parent PID: **5140**

General	
Target ID:	49
Start time:	20:16:33
Start date:	08/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff726010000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **804**, Parent PID: **800**

General	
Target ID:	50
Start time:	20:16:34
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **2024**, Parent PID: **804**

General	
Target ID:	51
Start time:	20:16:34
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1956**, Parent PID: **800**

General	
Target ID:	52
Start time:	20:16:34
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5432**, Parent PID: **1956**

General	
Target ID:	53
Start time:	20:16:34
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3276**, Parent PID: **800**

General	
Target ID:	54
Start time:	20:16:35
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1104**, Parent PID: **3276**

General	
Target ID:	55
Start time:	20:16:35
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5144**, Parent PID: **800**

General	
Target ID:	56
Start time:	20:16:35
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5844**, Parent PID: **5144**

General	
Target ID:	57
Start time:	20:16:36
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3304**, Parent PID: **800**

General	
Target ID:	58
Start time:	20:16:36
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3196**, Parent PID: **3304**

General	
Target ID:	59
Start time:	20:16:36
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1008**, Parent PID: **800**

General	
Target ID:	60
Start time:	20:16:37
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5848**, Parent PID: **1008**

General	
Target ID:	61
Start time:	20:16:37
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3284**, Parent PID: **800**

General	
Target ID:	63
Start time:	20:16:37
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4764**, Parent PID: **3284**

General

Target ID:	64
Start time:	20:16:37
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2056**, Parent PID: **800**

General

Target ID:	65
Start time:	20:16:38
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6076**, Parent PID: **2056**

General

Target ID:	66
Start time:	20:16:38
Start date:	08/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1672**, Parent PID: **800**

General	
Target ID:	67
Start time:	20:16:38
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **2904**, Parent PID: **1672**

General	
Target ID:	68
Start time:	20:16:39
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1956**, Parent PID: **800**

General	
Target ID:	69
Start time:	20:16:39
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1700**, Parent PID: **1956**

General	
Target ID:	70
Start time:	20:16:39
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4432**, Parent PID: **800**

General	
Target ID:	72
Start time:	20:16:40
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4428**, Parent PID: **4432**

General	
Target ID:	73
Start time:	20:16:40
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5736**, Parent PID: **800**

General	
Target ID:	74
Start time:	20:16:40
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3580**, Parent PID: **5736**

General	
Target ID:	75
Start time:	20:16:40
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5156**, Parent PID: **800**

General	
Target ID:	76
Start time:	20:16:41
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4388**, Parent PID: **5156**

General	
Target ID:	77
Start time:	20:16:41
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5652**, Parent PID: **800**

General	
Target ID:	78
Start time:	20:16:42

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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5504**, Parent PID: **5652**

General	
Target ID:	79
Start time:	20:16:42
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3524**, Parent PID: **800**

General	
Target ID:	80
Start time:	20:16:42
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5444**, Parent PID: **3524**

General	
Target ID:	81
Start time:	20:16:43
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	

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

Analysis Process: cmd.exe PID: **1696**, Parent PID: **800**

General	
Target ID:	82
Start time:	20:16:43
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4724**, Parent PID: **1696**

General	
Target ID:	83
Start time:	20:16:43
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3272**, Parent PID: **800**

General	
Target ID:	84
Start time:	20:16:44
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **772**, Parent PID: **3272**

General	
Target ID:	85

Start time:	20:16:44
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5816**, Parent PID: **800**

General	
Target ID:	86
Start time:	20:16:44
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4736**, Parent PID: **5816**

General	
Target ID:	87
Start time:	20:16:45
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3024**, Parent PID: **800**

General	
Target ID:	88
Start time:	20:16:45
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D

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

Analysis Process: Conhost.exe PID: **4428**, Parent PID: **3024**

General	
Target ID:	89
Start time:	20:16:45
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3020**, Parent PID: **800**

General	
Target ID:	90
Start time:	20:16:46
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1212**, Parent PID: **3020**

General	
Target ID:	91
Start time:	20:16:46
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5848**, Parent PID: **800**

General

Target ID:	93
Start time:	20:16:47
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5444**, Parent PID: **5848**

General	
Target ID:	95
Start time:	20:16:50
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4008**, Parent PID: **800**

General	
Target ID:	97
Start time:	20:16:51
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5808**, Parent PID: **4008**

General	
Target ID:	98
Start time:	20:16:52
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:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3956**, Parent PID: **800**

General	
Target ID:	99
Start time:	20:16:52
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c set /a "0x13^51"
Imagebase:	0x7ff7afe50000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1548**, Parent PID: **3956**

General	
Target ID:	100
Start time:	20:16:53
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5084**, Parent PID: **800**

General	
Target ID:	101
Start time:	20:16:54
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5000**, Parent PID: **5084**

General	
Target ID:	102
Start time:	20:16:54
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5436**, Parent PID: **800**

General	
Target ID:	103
Start time:	20:16:54
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4684**, Parent PID: **5436**

General	
Target ID:	104
Start time:	20:16:55
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2512**, Parent PID: **800**

General	
Target ID:	105
Start time:	20:16:55
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4360**, Parent PID: **2512**

General	
Target ID:	106
Start time:	20:16:55
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4764**, Parent PID: **800**

General	
Target ID:	107
Start time:	20:16:55
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5660**, Parent PID: **4764**

General	
Target ID:	108
Start time:	20:16:56
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3580**, Parent PID: **800**

General	
Target ID:	109
Start time:	20:16:56
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5872**, Parent PID: **3580**

General	
Target ID:	110
Start time:	20:16:56
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5152**, Parent PID: **800**

General	
Target ID:	111
Start time:	20:16:57
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1696**, Parent PID: **5152**

General	
Target ID:	112
Start time:	20:16:57
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3464**, Parent PID: **800**

General

Target ID:	113
Start time:	20:16:57
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5816**, Parent PID: **3464**

General

Target ID:	114
Start time:	20:16:58
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3444**, Parent PID: **800**

General

Target ID:	115
Start time:	20:16:58
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3432**, Parent PID: **3444**

General	
Target ID:	116
Start time:	20:16:58
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3336**, Parent PID: **800**

General	
Target ID:	117
Start time:	20:16:59
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1936**, Parent PID: **3336**

General	
Target ID:	118
Start time:	20:16:59
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5972**, Parent PID: **800**

General	
Target ID:	119
Start time:	20:16:59
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4068**, Parent PID: **5972**

General	
Target ID:	120
Start time:	20:17:00
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1424**, Parent PID: **800**

General	
Target ID:	121
Start time:	20:17:00
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5308**, Parent PID: **1424**

General	
Target ID:	122
Start time:	20:17:00
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5392**, Parent PID: **800**

General	
Target ID:	123
Start time:	20:17:01
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5384**, Parent PID: **5392**

General	
Target ID:	124
Start time:	20:17:01
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1324**, Parent PID: **800**

General	
Target ID:	125
Start time:	20:17:01
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5836**, Parent PID: **1324**

General	
Target ID:	126
Start time:	20:17:01

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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5484**, Parent PID: **800**

General	
Target ID:	127
Start time:	20:17:02
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5548**, Parent PID: **5484**

General	
Target ID:	128
Start time:	20:17:02
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1544**, Parent PID: **800**

General	
Target ID:	130
Start time:	20:17:02
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	

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

Analysis Process: Conhost.exe PID: **5736**, Parent PID: **1544**

General	
Target ID:	131
Start time:	20:17:03
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5672**, Parent PID: **800**

General	
Target ID:	132
Start time:	20:17:03
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5012**, Parent PID: **5672**

General	
Target ID:	133
Start time:	20:17:03
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3656**, Parent PID: **800**

General	
Target ID:	134

Start time:	20:17:04
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4756**, Parent PID: **3656**

General

Target ID:	135
Start time:	20:17:04
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2028**, Parent PID: **800**

General

Target ID:	136
Start time:	20:17:04
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **476**, Parent PID: **2028**

General

Target ID:	137
Start time:	20:17:04
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: cmd.exe PID: **3252**, Parent PID: **800**

General	
Target ID:	138
Start time:	20:17:05
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:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5660**, Parent PID: **3252**

General	
Target ID:	139
Start time:	20:17:05
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:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Disassembly

No disassembly