ID: 791299
Sample Name: Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Cookbook: default.jbs
Time: 09:52:49
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

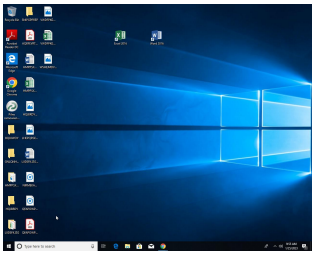
Windows Analysis Report

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

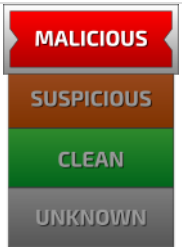
Overview

General Information

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



Detection



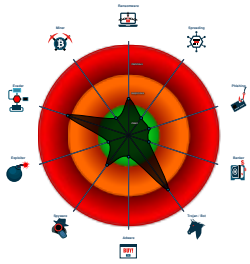
GuLoader

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Mass process execution to delay an…
- Obfuscated command line found
- Uses 32bit PE files
- PE file does not import any functions
- Sample file is different than original …
- Drops PE files
- Tries to load missing DLLs
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe (PID: 6056 cmdline: C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe MD5: 17388D36388D280C4E2D724C9AB58002)
  - cmd.exe (PID: 6104 cmdline: cmd.exe /c set /A "0x0E^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 6112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1116 cmdline: cmd.exe /c set /A "0x19^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5136 cmdline: cmd.exe /c set /A "0x05^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5352 cmdline: cmd.exe /c set /A "0x0E^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5348 cmdline: cmd.exe /c set /A "0x07^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5408 cmdline: cmd.exe /c set /A "0x78^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5516 cmdline: cmd.exe /c set /A "0x79^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4696 cmdline: cmd.exe /c set /A "0x71^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 3424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1400 cmdline: cmd.exe /c set /A "0x71^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 4912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4908 cmdline: cmd.exe /c set /A "0x08^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 1852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1556 cmdline: cmd.exe /c set /A "0x39^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 2360 cmdline: cmd.exe /c set /A "0x2E^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 3384 cmdline: cmd.exe /c set /A "0x2A^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1176 cmdline: cmd.exe /c set /A "0x3F^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 1540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 688 cmdline: cmd.exe /c set /A "0x2E^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5760 cmdline: cmd.exe /c set /A "0x0D^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- cmd.exe (PID: 5836 cmdline: cmd.exe /c set /A "0x22^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5860 cmdline: cmd.exe /c set /A "0x27^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4964 cmdline: cmd.exe /c set /A "0x2E^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5808 cmdline: cmd.exe /c set /A "0x0A^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5884 cmdline: cmd.exe /c set /A "0x63^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5448 cmdline: cmd.exe /c set /A "0x26^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5452 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5736 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5928 cmdline: cmd.exe /c set /A "0x39^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 6136 cmdline: cmd.exe /c set /A "0x7F^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 684 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5360 cmdline: cmd.exe /c set /A "0x67^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5316 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5412 cmdline: cmd.exe /c set /A "0x22^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5456 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4228 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5008 cmdline: cmd.exe /c set /A "0x33^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 2056 cmdline: cmd.exe /c set /A "0x73^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4556 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 496 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1296 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3092 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3236 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5872 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4988 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4920 cmdline: cmd.exe /c set /A "0x67^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5484 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5908 cmdline: cmd.exe /c set /A "0x22^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5732 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5768 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 2576 cmdline: cmd.exe /c set /A "0x67^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 6112 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5164 cmdline: cmd.exe /c set /A "0x3B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5152 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5344 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5436 cmdline: cmd.exe /c set /A "0x67^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5380 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1768 cmdline: cmd.exe /c set /A "0x22^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- cmd.exe (PID: 4252 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 576 cmdline: cmd.exe /c set /A "0x7F^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1412 cmdline: cmd.exe /c set /A "0x67^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3988 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5752 cmdline: cmd.exe /c set /A "0x22^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4852 cmdline: cmd.exe /c set /A "0x6B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5760 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4984 cmdline: cmd.exe /c set /A "0x33^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4976 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5860 cmdline: cmd.exe /c set /A "0x73^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4956 cmdline: cmd.exe /c set /A "0x7B^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5808 cmdline: cmd.exe /c set /A "0x67^75" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5896 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
00000000.00000002.514197554.0000000000613000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	
Process Memory Space: Pilne zamowienie nr5363582 U TECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe PID: 6056	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Data Obfuscation

Yara detected GuLoader

Obfuscated command line found

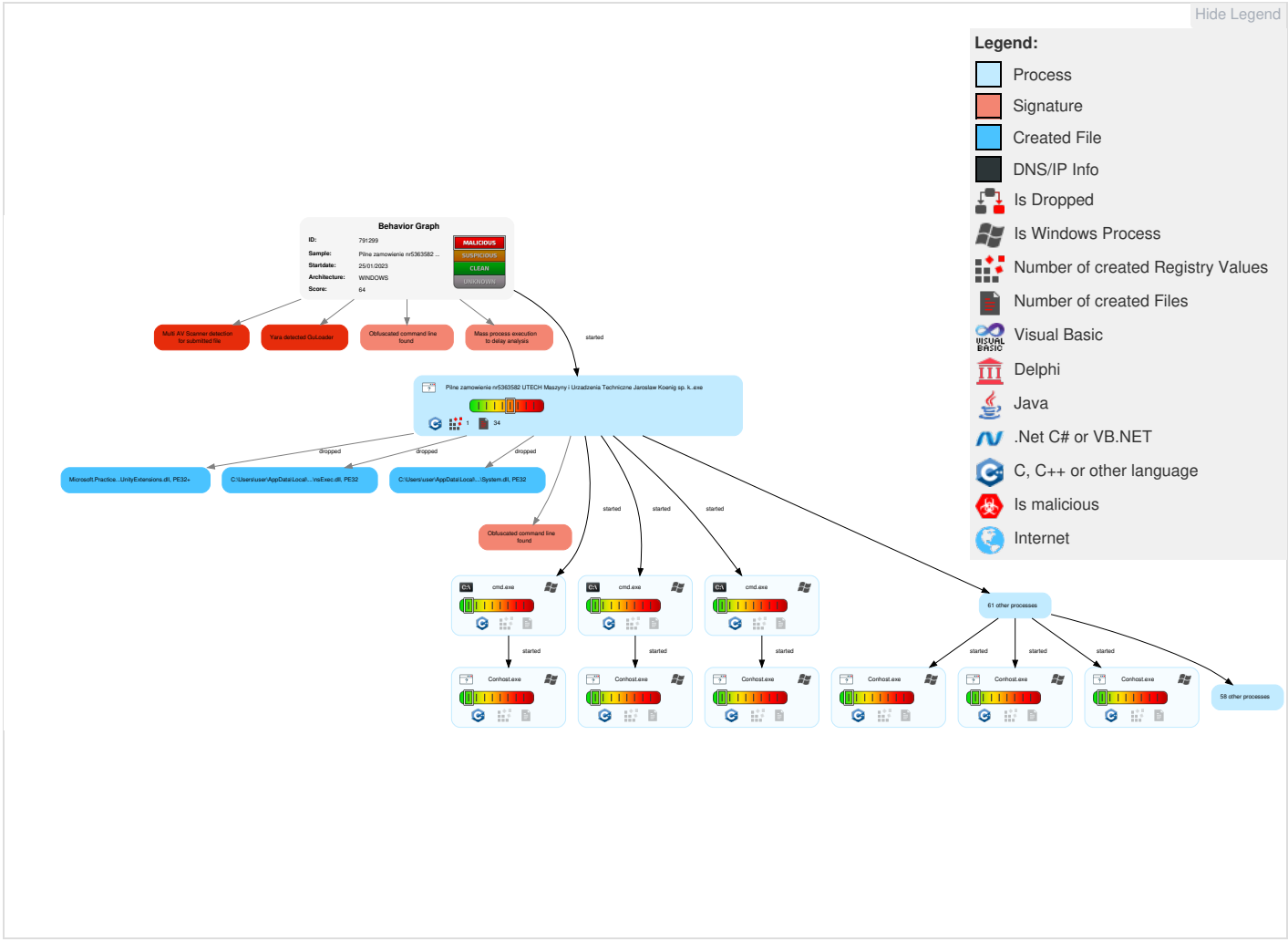
Malware Analysis System Evasion

Mass process execution to delay analysis

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	1 DLL Side-Loading	1 Access Token Manipulation	1 1 Masquerading	OS Credential Dumping	1 Time Based Evasion	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	2 File and Directory Discovery	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)	1 DLL Side-Loading	1 1 Process Injection	Security Account Manager	3 System Information 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	System Network Configuration 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 Obfuscated Files or Information	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
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

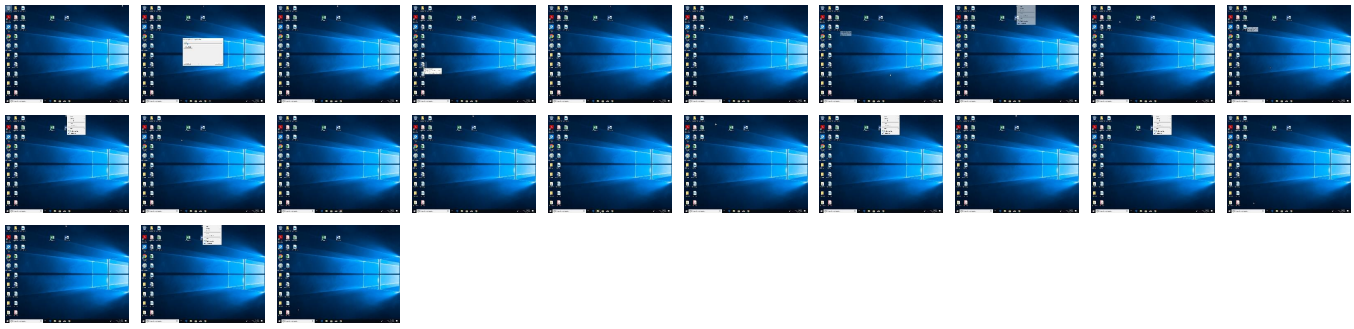
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\nsExec.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\nsExec.dll	1%	Virustotal		Browse
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaiblean ir\Nodebilledet\Microsoft.Practices.Composite.UnityExtensions.dll	0%	ReversingLabs		
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaiblean ir\Nodebilledet\Microsoft.Practices.Composite.UnityExtensions.dll	0%	Virustotal		Browse

Unpacked PE Files

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

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

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe, 00000000.00000003.248538306.000000002890000.00000004.00000020.00020000.00000000.sdmp, default.css.0.dr	false		high
http://creativecommons.org/licenses/by-sa/4.0/	application-x-executable.png.0.dr	false		high
http://nsis.sf.net/NSIS_Error	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	false		high
http://nsis.sf.net/NSIS_ErrorError	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	false		high
http://mozilla.org/MPL/2.0/.	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe, 00000000.00000003.248538306.000000002890000.00000004.00000020.00020000.00000000.sdmp, default.css.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791299
Start date and time:	2023-01-25 09:52:49 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	161
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:	mal64.troj.evad.winEXE@410/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63% (good quality ratio 61.6%) • Quality average: 88.6% • Quality standard deviation: 21.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 13.107.5.88, 13.107.42.16, 40.126.31.69, 20.190.159.23, 20.190.159.2, 20.190.159.0, 20.190.159.68, 20.190.159.4, 40.126.31.67, 20.190.159.73, 131.253.33.200, 13.107.22.200
- Excluded domains from analysis (whitelisted): ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, config.edge.skype.com.trafficmanager.net, eudb.ris.api.iris.microsoft.com, e-0009.e-msedge.net, arc.msn.com, prda.aadg.msidentity.com, config-edge-skype.l-0007.l-msedge.net, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, l-0007.l-msedge.net, config.edge.skype.com, storeedgefd.dsx.mp.microsoft.com, www.bing.com, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, ctldl.windowsupdate.com, www.tm.a.prd.aadg.akadns.net, www-www.bing.com.trafficmanager.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, dual-a-0001.dc-msedge.net, store-images.s-microsoft.com, l-0007.config.skype.com, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:53:43	API Interceptor	1x Sleep call for process: Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\System.dll

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.770803561213006
Encrypted:	false
SSDEEP:	192:vPtkumJX7zB22kGwfy0mtVgkCPOsE1un:k702k5qpdsEQn
MD5:	2AE993A2FFEC0C137EB51C8832691BCB
SHA1:	98E0B37B7C14890F8A599F35678AF5E9435906E1
SHA-256:	681382F3134DE5C6272A49DD13651C8C201B89C247B471191496E7335702FA59
SHA-512:	2501371EB09C01746119305BA080F3B8C41E64535FF09CEE4F51322530366D0BD5322EA5290A466356598027E6CDA8AB360CAEF62DCAF560D630742E2DD9BCD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j.9..i....I....I.Richm.....PE..L...tc.W.. .....!.....'.....0.....`.....2.....0..P.....P.....0..X.....text...O..... ..... ..`.rdata..S....0....."....@..@.data...h....@.....&.....@....reloc..`....P.....(.....@..B.....

C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\nsExec.dll

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	4.994861218233575
Encrypted:	false
SSDEEP:	96:U7GUxNkO6GR0t9GKKr1Zd8NHYVVHp4dEeY3kRnHdMqqyVgNN3e:mXhHR0aTQN4gRHdMqJVgNE
MD5:	B648C78981C02C434D6A04D4422A6198
SHA1:	74D99EED1EAE76C7F43454C01CDB7030E5772FC2
SHA-256:	3E3D516D4F28948A474704D5DC9907DBE39E3B3F98E7299F536337278C59C5C9
SHA-512:	219C88C0EF9FD6E3BE34C56D8458443E695BADD27861D74C486143306A94B8318E6593BF4DA81421E88E4539B238557DD4FE1F5BEDF3ECEC59727917099E90D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2% • Antivirus: Virustotal, Detection: 1%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d..7..7..7..7..7,..7..7..7..7..7..7Rich..7.....PE..L...rc.W.....!..... ....P.....$..I.... ..P.....@..... .....text..... ..`. rdata...,.... .....@..@.data.....0.....@....reloc.....@.....@..B..... ....

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

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	18048
Entropy (8bit):	5.781710632242959
Encrypted:	false
SSDEEP:	384:PDNDRvozv1hgXptjLrzs4AvgWOMrq0eMDl/:ZRvA4r77ARg/
MD5:	270209B12F7C117C539F574CE2576C0A
SHA1:	184B447F6364FA0760F862B84CBC6E717C9F5C3D
SHA-256:	C5DB3358A184147D6FFB41F05BBF9BA9356038A0867A783F266EA62813EF6CF4
SHA-512:	BB062EF832EB2B477D92FDF71C0B6B30AA590A735DEC1920400C3DA74EC07FF1F1DBF9E50E63EE2FDD68E9E48FC39F5522DFF0A029E47658A41F88EEC9FD25 0A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..d...W..S.........." .....0.............. .....@..... ....@...@......@............... ....`...............8.............dM............................................................. ..H...........text...6.... ...0................. ..`.rsrc........`.......2...... ........@..@.reloc..............8.............@..BH........*..\#..........`&..{....*"..}....*..{....*"..(....*...0...........}.....o......-.(....s....z.r...p..o......o....(.....(....-. (....s....z.r3..p..o.....(....o...+&.o.....r_..p..o.....o....&.o....&.o.....r...p..o.....o......,...(....o...+(....(.....r...p..o.....o.....r...p..o....*..(...(....(.....+...(....(.....,...(....(....*2.(....o...+*...0..%......... (.....o....o...+&.o......,..(.....o...+&.{....9......-...(.........(.

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

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	ASCII text, with very long lines (50244), with no line terminators
Category:	dropped
Size (bytes):	50244
Entropy (8bit):	3.999625167208849
Encrypted:	false
SSDEEP:	768:4Kt0hO4obUZX9nvBHp7RJ+CqqSK0haV6RTFA9yu7m1HK0TWgKL383w6gW:81oq9nvjqqSiUu9yu7m1HzT4L38AhW
MD5:	21337BAB1F65E60A88523B4DDB961E52
SHA1:	AD9C448F53AB48C3110D25650BACFE44C1988D51
SHA-256:	E2565D3B49D70ACDAD0AB4162BA0FBF738F227A0EC224982A813E874C46C0FCE
SHA-512:	A6DAE16844C6A433AFF4EDE77F0E77984073CEC0E38D439B57144670EE0F4034BD5F2FFCB6647010F6717A7F39928A6F04E7F05BA9511745F38CF6A49891FFDA
Malicious:	false
Preview:	56E3E082070CC707B0B701B836A6FEDCB0D7E6E50989CF2DA81B4311EF928EBF02F09C7EB977BC9031BA864CC44F17929BE2524D78FC507F411DCBC9 1BE502D51D27CA45924DFC91765F6EB7845C91C0D665E583A8AD0203D0E4E6E6CD17355A6BEE2CB460D8FEE6D05422DDF5EE3A100E5B5DF7E16AF5EE 06574C03F45CF5AB392237D86BD7BA856648AFC8934A58C5CB26436F55DDADFBBF10B9B4879334CB8EC34E3188C13AB624B5BD476E64AE8E29F5D01B 1F4990A3C97BFCFF07D4B1C9164FF864EC64F66817B8CB32DEDF9FCDD8BFEA77F0E8FA2FF734E9693AB8DB0E567BF76D363F5446629BF43E8658F94A 657CA3A4E1F8CBE2A0DF2079A857E95B935916B09270CBD505DC004B5398C830A48C5BEC0BF51F45B3CF8B5BB54C379E941830FBE112B9AA311E3DDC B33515B088213DF149B237AA4C2FDEF37D6456FA22C12527A4B8369506B1AD0523F47A8479C3F96173652E3E9D10BC37BBDA514166816FEB43067D30 B2F3AF7514968878341027AC20B0A426E2E7C25DCBA0B6FED381151DDA1B09092FF33782B8325E6B87234F9652F4DB96B3783CDA3D515E98CEDAACDB A19D8B6F8900215829145E262A081177B80AA3834EDBFF2F96C95ED77E31546A6F59C87BE0A467B5CF31606F7D2E6453A34C7B7AF3DAFCFB71E6B577 0C2B1BC25C472C3653338393230C4F9FFB4398AD

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

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

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

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	Unicode text, UTF-8 text
Category:	dropped
Size (bytes):	19729
Entropy (8bit):	4.854870578875106
Encrypted:	false
SSDEEP:	384:SfWIec2c8Fn9khSO774VZE+HDxYADgab6YDrvCEE5c:SfWpc8Fn9khSO3yZE+HFYADJv/E5c
MD5:	A9006B652EBD39E033121BBAD1D45AC9
SHA1:	A9A681BD5801984388334C85B8E09561A21913FF
SHA-256:	E84FAFC9058C23AD27C2BE6BB8ED9CAC9AAC1744376330D53D7D531C1EA3EABE
SHA-512:	0B2F899C1FB7030F5ACA15E4F23F250CC62D5014ECBAE0E5CE738F9172895AB82C2B93693F3A078EC3642B3549355E25DA16834A9714CCF8B33087ED3BACAF B

Malicious:	false
Preview:	/*. * This file is part of the LibreOffice project.. *. * This Source Code Form is subject to the terms of the Mozilla Public. * License, v. 2.0. If a copy of the MPL was not distr ibuted with this. * file, You can obtain one at http://mozilla.org/MPL/2.0/.. *. * This file incorporates work covered by the following license notice:. *. * Licensed to the Apac he Software Foundation (ASF) under one or more. * contributor license agreements. See the NOTICE file distributed. * with this work for additional information regardi ng copyright. * ownership. The ASF licenses this file to you under the Apache. * License, Version 2.0 (the "License"); you may not use this file. * except in compliance with the License. You may obtain a copy of. * the License at http://www.apache.org/licenses/LICENSE-2.0 .. */./*.++ ++++++++++++++++++++++++++++++.+ LIBREOFFICE HELP IN BROWSER +.+ DEFAULT STYLE

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

Process:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	660
Entropy (8bit):	4.929915592008811
Encrypted:	false
SSDEEP:	12:t4CDqaZnoUJgiCydrkeYRAerAFFLAmLRHGdK5D9DME:t4C9ZoUJyyKbRAecFxfRHGMRtME
MD5:	96756F6658DD20BCB387DECC6C2FB720
SHA1:	42E06BBF711B5F71D07B965A0654AFF6249B99D6
SHA-256:	C15238E9B65995BDADC206340B33E7B7E50EF00031F5B61DF9700BBB5350F635
SHA-512:	F64F1B4C96611ADF276F87F242501534DA8D9D2A17A00749A4FE05DE051DA5CAEDF545D39D574BB7E6447CC272C5F9BF2E8B0EE88B277EDDB46D1E263C08FA 1B
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M8 4v11h3V4zm4-3v14h3V1zM4 7v8h3V7zm-4 3v5h3v-5z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation :auto;mix-blend-mode:normal" overflow="visible" opacity=".35" color="#000" font-weight="400" font-family="sans-serif" fill="#474747" fill-rule="evenodd"/></svg>

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

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.874744026790643
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
File size:	669600
MD5:	17388d36388d280c4e2d724c9ab58002
SHA1:	ee660100dfbad59a2796244514bff64c66cd0ca7
SHA256:	5f20a33e263b8b8f5388b8e2512d0678312257b8fdf592b8a83aa481076048ca
SHA512:	b49d055149f26ce72cd04ecd6fd581523fdeaf7f3234e8b547fa0fedbaf52aae6b408480c4cebdb7359422d9ae7664dcd8a083d99f13d9fbc1692d4914895ce4

SSDEEP:	12288:Pkvld8NVtfkug41IDHQ215k5P5x2/dKRy6i5y:PeHiMrQ2HkLI/ki5y
TLSH:	40E4F6527059808AE8A738F3685FC07014A02EAD92EDD25E66F67B2645F2313CC5FF9D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (...F...F...F.*.....F...G.v.F.*.....F...v...F...@...F.Rich..F.....PE..L....c.W.....^.....

File Icon

Icon Hash:	3319396623190917

Static PE Info

General

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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Dictatorialism, OU="Innervational Chloropal Stald ", E=Covalency@Bedrveligheds.Sl, O=Dictatorialism, L=Tarrant Rushton, S=England, C=GB
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 1/24/2023 12:31:02 AM 1/23/2026 12:31:02 AM
Subject Chain	• CN=Dictatorialism, OU="Innervational Chloropal Stald ", E=Covalency@Bedrveligheds.Sl, O=Dictatorialism, L=Tarrant Rushton, S=England, C=GB
Version:	3
Thumbprint MD5:	7F1F45BD7FCC95B4458C5EC8BFA17430
Thumbprint SHA-1:	31BE90317316BB6D5DBEDE711C3E03BCD2EF533A
Thumbprint SHA-256:	801CB0CF2041D9240AC71DE2FCEEC2FA0C23383EF6BEA436ECE5CCF3C1CB066D
Serial:	E5205A57DA732B09

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004070A8h]
call dword ptr [004070A4h]
cmp ax, 00000006h

Instruction
je 00007FF410ED2933h
push ebx
call 00007FF410ED58A1h
cmp eax, ebx
je 00007FF410ED2929h
push 00000C00h
call eax
mov esi, 00407298h
push esi
call 00007FF410ED581Dh
push esi
call dword ptr [004070A0h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FF410ED290Dh
push ebp
push 00000009h
call 00007FF410ED5874h
push 00000007h
call 00007FF410ED586Dh
mov dword ptr [00423704h], eax
call dword ptr [00407044h]
push ebx
call dword ptr [00407288h]
mov dword ptr [004237B8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041ECC8h
call dword ptr [00407174h]
push 00409188h
push 00422F00h
call 00007FF410ED5497h
call dword ptr [0040709Ch]
mov ebp, 00429000h
push eax
push ebp
call 00007FF410ED5485h
push ebx
call dword ptr [00407154h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7428	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3e000	0x5aec8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xa3078	0x728	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c5b	0x5e00	False	0.6603640292553191	data	6.411456379497882	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1246	0x1400	False	0.42734375	data	5.005029341587408	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1a7f8	0x400	False	0.6376953125	data	5.108396988130901	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x24000	0x1a000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3e000	0x5aec8	0x5b000	False	0.23903245192307693	data	5.402063687419607	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

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

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableA, Sleep, GetTickCount, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, GetFileAttributesA, SetFileAttributesA, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, ExitProcess, GetFullPathNameA, GlobalLock, CreateThread, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, ReadFile, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, CloseHandle, SetCurrentDirectoryA, MoveFileA, CompareFileTime, GetShortPathNameA, SearchPathA, lstrcmpiA, SetFileTime, lstrcmpA, ExpandEnvironmentStringsA, GlobalUnlock, GetDiskFreeSpaceA, GlobalFree, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, GetPrivateProfileStringA, FindClose, MultiByteToWideChar, FreeLibrary, MulDiv, WritePrivateProfileStringA, LoadLibraryExA, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, GlobalAlloc

DLL	Import
USER32.dll	ScreenToClient, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, PostQuitMessage, GetWindowRect, EnableMenuItem, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, GetDC, CreateDialogParamA, SetTimer, GetDlgItem, SetWindowLongA, SetForegroundWindow, LoadImageA, IsWindow, SendMessageTimeoutA, FindWindowExA, OpenClipboard, TrackPopupMenu, AppendMenuA, EndPaint, DestroyWindow, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegDeleteKeyA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, AdjustTokenPrivileges, RegOpenKeyExA, RegEnumValueA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

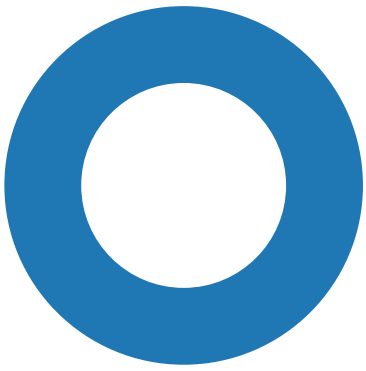
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



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

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

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

Click to jump to process

System Behavior

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

PID: **6056**, Parent PID: **3452**

General

Target ID:	0
Start time:	09:53:42
Start date:	25/01/2023
Path:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe
Imagebase:	0x400000
File size:	669600 bytes
MD5 hash:	17388D36388D280C4E2D724C9AB58002
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000000.00000002.514197554.0000000000613000.00000004.00000020.00020000.00000000.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	405461	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nswCDB0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4059CF	GetTempFileNameA
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	4	405461	CreateDirectoryA
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	4	405461	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Pacifisterne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer\Seacross.Him	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405998	CreateFileA
C:\Users\user\Pacifisterne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaibleanir	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaibleanir\Nodebilledet	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaibleanir\Nodebilledet\Microsoft.Practices.Composite.UnityExtensions.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405998	CreateFileA
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaibleanir\Nodebilledet\Reinspired.Aut	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405998	CreateFileA
C:\Users\user\Pacifisterne\Automatcafeer\Tubulating	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer\Tubulating\application-x-executable.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405998	CreateFileA
C:\Users\user\Pacifisterne\Automatcafeer\Syntaksgenkendelsernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405461	CreateDirectoryA
C:\Users\user\Pacifisterne\Automatcafeer\Syntaksgenkendelsernes\Temposkifterne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405461	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Pacifisterne\Automatcafeer\Syntaksgenkendelser nes\Temposkifterne\default.css	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405998	CreateFileA
C:\Users\user\Pacifisterne\Automatcafeer\Syntaksgenkendelser nes\Temposkifterne\network-cellular-signal-none-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405998	CreateFileA
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4059CF	GetTempFileNameA
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	405461	CreateDirectoryA
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	405461	CreateDirectoryA
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	405461	CreateDirectoryA
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	405461	CreateDirectoryA
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	405461	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsgFEE3.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	405421	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\nsExec.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405998	CreateFileA
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\nsExec.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	285	405998	CreateFileA
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405998	CreateFileA
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405998	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nswCDB0.tmp	success or wait	1	40332E	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp	success or wait	1	4055CA	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Pacifisterne\Automatcafeer\Seacross.Him	0	32768	58 58	XXXXXXXXXXXXXXXXX XXXXXXXXXXXXX XXXXXXXXXXXXXXXXX XXXXXXXXXXXXX XXXXXXXXXXXXXXXXX XXXXXXXXXXXXX XXXXXXXXXXXXXXXXX XXXXXXXXXXXXX XXXXXXXXXXXXXXXXX XXXXXXXXXXXXX XXXXXXXXXXXXXXXXX XXXXXXXXXXXXX XXXXXXXXXXXXXXXXX XXXXXXXXXXXXX XXXXXXXXXXXXXXXXX XXXXXXXXXXXXX XXXXXXXXXXXXXXX	success or wait	14	405A2D	WriteFile
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaibleanir\Nodebilledet\Microsoft.Practices.Composite.UnityExtensions.dll	0	18048	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 02 00 57 fd 0d 53 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0b 00 00 30 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd fd 00 00 03 00 40 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdWS" 0 @ @@@	success or wait	1	405A2D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaibleanir\Nodebilledet\Reinspired.Aut	0	31324	35 36 45 33 45 30 38 32 30 37 30 43 43 37 30 37 42 30 42 37 30 31 42 38 33 36 41 36 46 45 44 43 42 30 44 37 45 36 45 35 30 39 38 39 43 46 32 44 41 38 31 42 34 33 31 31 45 46 39 32 38 45 42 46 30 32 46 30 39 43 37 45 42 39 37 37 42 43 39 30 33 31 42 41 38 36 34 43 43 34 34 46 31 37 39 32 39 42 45 32 35 32 34 44 37 38 46 43 35 30 37 46 34 31 31 44 43 42 43 39 31 42 45 35 30 32 44 35 31 44 32 37 43 41 34 35 39 32 34 44 46 43 39 31 37 36 35 46 36 45 42 37 38 34 35 43 39 31 43 30 44 36 36 35 45 35 38 33 41 38 41 44 30 32 30 33 44 30 45 34 45 36 45 36 43 44 31 37 33 35 35 41 36 42 45 45 32 43 42 34 36 30 44 38 46 45 45 36 44 30 35 34 32 32 44 44 46 35 45 45 33 41 31 30 30 45 35 42 35 44 46 37 45 31 36 41 46 35 45 45 30 36 35 37 34 43 30 33 46 34 35 43 46 35 41	56E3E082070CC707B0B701B836A6FEDCB0D7E6E50989CF2DA81B4311EF928EBF02F09C7EB977BC9031BA864CC44F17929BE2524D78FC507F411DCBC91BE502D51D27CA45924DFC91765F6EB7845C91C0D665E583A8AD0203D0E4E6E6CD17355A6BEE2CB460D8FEE6D05422DDF5EE3A100E5B5DF7E16AF5EE06574C03F45CF5A	success or wait	2	405A2D	WriteFile
C:\Users\user\Pacifisterne\Automatcafeer\Tubulating\application-x-executable.png	0	981	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 2b 0e 1b 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 77 77 77 2e 69 6e 6b 73 63 61 70 65 2e 6f 72 67 fd fd 3c 1a 00 00 00 1b 74 45 58 74 54 69 74 6c 65 00 41 64 77 61 69 74 61 20 49 63 6f 6e 20 54 65 6d 70 6c 61 74 65 fd fd fd 3f 00 00 00 18 74 45 58 74 41 75 74 68 6f 72 00 47 4e 4f 4d 45 20 44 65 73 69 67 6e 20 54 65 61 6d 60 fd 76 7e 00 00 00 52 74 45 58 74 43 6f 70 79 72 69 67 68 74 00 43 43 20 41 74 74 72 69 62 75 74 69 6f 6e 2d 53 68 61 72 65 41 6c 69 6b 65 20 68 74 74 70 3a 2f 2f 63 72 65 61 74 69 76 65 63 6f 6d 6d 6f 6e 73 2e 6f 72 67 2f 6c 69	PNGIHDRasBIT|dpHYs+tEXtSoftwarewww.inkscape.org<tEXtTitleAdwaita Icon Template?tEXtAuthorGNOME Design Team`v~RtEXtCopyrightCC Attribution-ShareAlike http://creativecommons.org/li	success or wait	1	405A2D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Pacifisterne\Automatcafeer\Syntaksgenkendelsernes\Temposkifterne\default.css	0	19729	2f 2a 0a 20 2a 20 54 68 69 73 20 66 69 6c 65 20 69 73 20 70 61 72 74 20 6f 66 20 74 68 65 20 4c 69 62 72 65 4f 66 66 69 63 65 20 70 72 6f 6a 65 63 74 2e 0a 20 2a 0a 20 2a 20 54 68 69 73 20 53 6f 75 72 63 65 20 43 6f 64 65 20 46 6f 72 6d 20 69 73 20 73 75 62 6a 65 63 74 20 74 6f 20 74 68 65 20 74 65 72 6d 73 20 6f 66 20 74 68 65 20 4d 6f 7a 69 6c 6c 61 20 50 75 62 6c 69 63 0a 20 2a 20 4c 69 63 65 6e 73 65 2c 20 76 2e 20 32 2e 30 2e 20 49 66 20 61 20 63 6f 70 79 20 6f 66 20 74 68 65 20 4d 50 4c 20 77 61 73 20 6e 6f 74 20 64 69 73 74 72 69 62 75 74 65 64 20 77 69 74 68 20 74 68 69 73 0a 20 2a 20 66 69 6c 65 2c 20 59 6f 75 20 63 61 6e 20 6f 62 74 61 69 6e 20 6f 6e 65 20 61 74 20 68 74 74 70 3a 2f 2f 6d 6f 7a 69 6c 6c 61 2e 6f 72 67 2f 4d 50 4c 2f 32 2e 30 2f	/* * This file is part of the LibreOffice project. * * This Source Code Form is subject to the terms of the Mozilla Public * License, v. 2.0. If a copy of the MPL was not distributed with this * file, You can obtain one at http://mozilla.org/MPL/2.0/	success or wait	1	405A2D	WriteFile
C:\Users\user\Pacifisterne\Automatcafeer\Syntaksgenkendelsernes\Temposkifterne\network-cellular-signal-none-symbolic.svg	0	660	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 70 61 74 68 20 64 3d 22 4d 38 20 34 76 31 31 68 33 56 34 7a 6d 34 2d 33 76 31 34 68 33 56 31 7a 4d 34 20 37 76 38 68 33 56 37 7a 6d 2d 34 20 33 76 35 68 33 76 2d 35 7a 22 20 73 74 79 6c 65 3d 22 6c 69 6e 65 2d 68 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69 61 6e 74 2d 6c 69 67 61 74 75 72 65 73 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69 61 6e 74 2d 70 6f 73 69 74 69 6f 6e 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69 61 6e 74 2d 63 61 70 73 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69 61 6e 74 2d 6e 75 6d 65 72 69 63 3a 6e 6f	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M8 4v11h3V4zm4-3v14h3V1zM4 7v8h3V7zm-4 3v5h3v-5z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:no	success or wait	1	405A2D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\nsExec.dll	0	6656	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 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 64 fd fd 37 fd fd 37 fd fd 37 fd fd 37 fd fd 37 2c fd fd 37 fd fd 37 fd ef 37 fd fd 37 10 1b 37 fd fd 37 52 69 63 68 fd fd 37 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 72 63 fd 57 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 0c 00 00 00 0e 00 00 00 00 00 00 fd 10 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$d77777,777777Rich7PELrcW!	success or wait	1	405A2D	WriteFile
C:\Users\user\AppData\Local\Temp\nsgFEE3.tmp\System.dll	0	11264	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 29 fd fd fd 6d fd 6d fd 6d fd fd bd 6b fd 6d fd 7e b3 6e fd fd 6a fd 39 4c fd 69 fd 0e 16 fd 6c b3 52 b8 fd 6c fd 52 69 63 68 6d fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 74 63 fd 57 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 1e 00	MZ@!L!This program cannot be run in DOS mode.$)mmmkm~j9illRichmPELtcW!	success or wait	1	405A2D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	unknown	512	success or wait	800	4059FE	ReadFile
C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	unknown	4	success or wait	2	4059FE	ReadFile
C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	unknown	4	success or wait	25	4059FE	ReadFile
C:\Users\user\Pacifisterne\Automatcafeer\Nedrustningspolitikken\Dilemmaers146\Glasgaibleanir\Nodebilledet\Reinspired.Aut	unknown	1	success or wait	1023	4059FE	ReadFile
C:\Users\user\Desktop\Pilne zamowienie nr5363582 UTECH Maszyny i Urzadzenia Techniczne Jaroslaw Koenig sp. k..exe	unknown	4	success or wait	4	4059FE	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Territorialkravets	success or wait	1	4023A8	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Territorialkravets	Tantaliferous	unicode	Sagittary	success or wait	1	402401	RegSetValueExA

Analysis Process: cmd.exe PID: **6104**, Parent PID: **6056**

General

Target ID:	1
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x0E^75"
Imagebase:	
File size:	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: **6112**, Parent PID: **6104**

General

Target ID:	2
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	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: **1116**, Parent PID: **6056**

General

Target ID:	3
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x19^75"
Imagebase:	
File size:	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: **5176**, Parent PID: **1116**

General	
Target ID:	4
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	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: **5136**, Parent PID: **6056**

General	
Target ID:	5
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x05^75"
Imagebase:	
File size:	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: **5152**, Parent PID: **5136**

General	
Target ID:	6
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	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: **5352**, Parent PID: **6056**

General	
Target ID:	7

Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x0E^75"
Imagebase:	
File size:	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: **5328**, Parent PID: **5352**

General	
Target ID:	8
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	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: **5348**, Parent PID: **6056**

General	
Target ID:	9
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x07^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5436**, Parent PID: **5348**

General	
Target ID:	10
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	

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

Analysis Process: cmd.exe PID: **5408**, Parent PID: **6056**

General	
Target ID:	11
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x78^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5380**, Parent PID: **5408**

General	
Target ID:	12
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5516**, Parent PID: **6056**

General	
Target ID:	13
Start time:	09:53:44
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x79^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5500**, Parent PID: **5516**

General	
Target ID:	14
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4696**, Parent PID: **6056**

General	
Target ID:	15
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x71^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3424**, Parent PID: **4696**

General	
Target ID:	16
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	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: **6056**

General	
Target ID:	17
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	

Commandline:	cmd.exe /c set /A "0x71^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4912**, Parent PID: **1400**

General

Target ID:	18
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4908**, Parent PID: **6056**

General

Target ID:	19
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x08^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1852**, Parent PID: **4908**

General

Target ID:	20
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1556**, Parent PID: **6056**

General	
Target ID:	21
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x39^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **576**, Parent PID: **1556**

General	
Target ID:	22
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2360**, Parent PID: **6056**

General	
Target ID:	23
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x2E^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **240**, Parent PID: **2360**

General	
Target ID:	24
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe

Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3384**, Parent PID: **6056**

General	
Target ID:	25
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x2A^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5672**, Parent PID: **3384**

General	
Target ID:	26
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1176**, Parent PID: **6056**

General	
Target ID:	27
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x3F^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1540**, Parent PID: **1176**

General	
Target ID:	28
Start time:	09:53:45
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **688**, Parent PID: **6056**

General	
Target ID:	29
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x2E^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **676**, Parent PID: **688**

General	
Target ID:	30
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5760**, Parent PID: **6056**

General	
Target ID:	31
Start time:	09:53:46

Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x0D^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5748**, Parent PID: **5760**

General	
Target ID:	32
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5836**, Parent PID: **6056**

General	
Target ID:	33
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5792**, Parent PID: **5836**

General	
Target ID:	34
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	

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

Analysis Process: cmd.exe PID: **5860**, Parent PID: **6056**

General	
Target ID:	35
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x27^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4996**, Parent PID: **5860**

General	
Target ID:	36
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4964**, Parent PID: **6056**

General	
Target ID:	37
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x2E^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4932**, Parent PID: **4964**

General	
Target ID:	38

Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5808**, Parent PID: **6056**

General	
Target ID:	39
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x0A^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5700**, Parent PID: **5808**

General	
Target ID:	40
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5884**, Parent PID: **6056**

General	
Target ID:	41
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x63^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D

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

Analysis Process: Conhost.exe PID: **5892**, Parent PID: **5884**

General	
Target ID:	42
Start time:	09:53:46
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5448**, Parent PID: **6056**

General	
Target ID:	43
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x26^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5452**, Parent PID: **5448**

General	
Target ID:	44
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **6056**

General

Target ID:	45
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5744**, Parent PID: **5736**

General	
Target ID:	46
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5928**, Parent PID: **6056**

General	
Target ID:	47
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x39^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5948**, Parent PID: **5928**

General	
Target ID:	48
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes

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

Analysis Process: cmd.exe PID: **6136**, Parent PID: **6056**

General	
Target ID:	49
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7F^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6132**, Parent PID: **6136**

General	
Target ID:	50
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **684**, Parent PID: **6056**

General	
Target ID:	51
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1672**, Parent PID: **684**

General	
Target ID:	52
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5360**, Parent PID: **6056**

General	
Target ID:	53
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5356**, Parent PID: **5360**

General	
Target ID:	54
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5316**, Parent PID: **6056**

General	
Target ID:	55
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	

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

Analysis Process: Conhost.exe PID: **5312**, Parent PID: **5316**

General	
Target ID:	56
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5412**, Parent PID: **6056**

General	
Target ID:	57
Start time:	09:53:47
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5428**, Parent PID: **5412**

General	
Target ID:	58
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5456**, Parent PID: **6056**

General	
Target ID:	59
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5404**, Parent PID: **5456**

General	
Target ID:	60
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4228**, Parent PID: **6056**

General	
Target ID:	61
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4768**, Parent PID: **4228**

General	
Target ID:	62
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5008**, Parent PID: **6056**

General

Target ID:	63
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x33^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **648**, Parent PID: **5008**

General

Target ID:	64
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	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: **6056**

General

Target ID:	65
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x73^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4224**, Parent PID: **2056**

General	
Target ID:	66
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4556**, Parent PID: **6056**

General	
Target ID:	67
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **816**, Parent PID: **4556**

General	
Target ID:	68
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **496**, Parent PID: **6056**

General	
Target ID:	69
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1500**, Parent PID: **496**

General	
Target ID:	70
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1296**, Parent PID: **6056**

General	
Target ID:	71
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	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: **1296**

General	
Target ID:	72
Start time:	09:53:48
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3092**, Parent PID: **6056**

General	
Target ID:	73
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4648**, Parent PID: **3092**

General	
Target ID:	74
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3236**, Parent PID: **6056**

General	
Target ID:	75
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	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: **3236**

General	
Target ID:	76
Start time:	09:53:49

Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	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: **6056**

General	
Target ID:	77
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5864**, Parent PID: **5872**

General	
Target ID:	78
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4988**, Parent PID: **6056**

General	
Target ID:	79
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	

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

Analysis Process: Conhost.exe PID: **4972**, Parent PID: **4988**

General	
Target ID:	80
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4920**, Parent PID: **6056**

General	
Target ID:	81
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5956**, Parent PID: **4920**

General	
Target ID:	82
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	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: **6056**

General	
Target ID:	83

Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5476**, Parent PID: **5484**

General	
Target ID:	84
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5908**, Parent PID: **6056**

General	
Target ID:	85
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5472**, Parent PID: **5908**

General	
Target ID:	86
Start time:	09:53:49
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: cmd.exe PID: **5732**, Parent PID: **6056**

General	
Target ID:	87
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	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: **5732**

General	
Target ID:	88
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5768**, Parent PID: **6056**

General	
Target ID:	89
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5776**, Parent PID: **5768**

General

Target ID:	90
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2576**, Parent PID: **6056**

General	
Target ID:	91
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6040**, Parent PID: **2576**

General	
Target ID:	92
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6112**, Parent PID: **6056**

General	
Target ID:	93
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes

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

Analysis Process: Conhost.exe PID: **5156**, Parent PID: **6112**

General	
Target ID:	94
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5164**, Parent PID: **6056**

General	
Target ID:	95
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x3B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5176**, Parent PID: **5164**

General	
Target ID:	96
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	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: **6056**

General	
Target ID:	97
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5320**, Parent PID: **5152**

General	
Target ID:	98
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5344**, Parent PID: **6056**

General	
Target ID:	99
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5332**, Parent PID: **5344**

General	
Target ID:	100
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	

File size:	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: **6056**

General	
Target ID:	101
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5440**, Parent PID: **5436**

General	
Target ID:	102
Start time:	09:53:50
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5380**, Parent PID: **6056**

General	
Target ID:	103
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5396**, Parent PID: **5380**

General	
Target ID:	104
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1768**, Parent PID: **6056**

General	
Target ID:	105
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3408**, Parent PID: **1768**

General	
Target ID:	106
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4252**, Parent PID: **6056**

General	
Target ID:	107
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	

Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **648**, Parent PID: **4252**

General

Target ID:	108
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **576**, Parent PID: **6056**

General

Target ID:	109
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7F^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **3780**, Parent PID: **576**

General

Target ID:	110
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1412**, Parent PID: **6056**

General	
Target ID:	111
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **416**, Parent PID: **1412**

General	
Target ID:	112
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3988**, Parent PID: **6056**

General	
Target ID:	113
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **2300**, Parent PID: **3988**

General	
Target ID:	114
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe

Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5752**, Parent PID: **6056**

General	
Target ID:	115
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x22^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **1216**, Parent PID: **5752**

General	
Target ID:	116
Start time:	09:53:51
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4852**, Parent PID: **6056**

General	
Target ID:	117
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x6B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5788**, Parent PID: **4852**

General	
Target ID:	118
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5760**, Parent PID: **6056**

General	
Target ID:	119
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	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: **5760**

General	
Target ID:	120
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4984**, Parent PID: **6056**

General	
Target ID:	121
Start time:	09:53:52

Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x33^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4976**, Parent PID: **4984**

General	
Target ID:	122
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5860**, Parent PID: **6056**

General	
Target ID:	123
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x73^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **4928**, Parent PID: **5860**

General	
Target ID:	124
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	

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

Analysis Process: cmd.exe PID: **4956**, Parent PID: **6056**

General	
Target ID:	125
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x7B^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5784**, Parent PID: **4956**

General	
Target ID:	126
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5808**, Parent PID: **6056**

General	
Target ID:	127
Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd.exe /c set /A "0x67^75"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5896**, Parent PID: **5808**

General	
Target ID:	128

Start time:	09:53:52
Start date:	25/01/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Disassembly

No disassembly