ID: 679174
Sample Name: Original Shipment_Document.PDF.exe
Cookbook: default.jbs
Time: 11:23:09
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

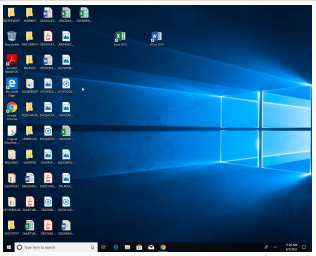
Windows Analysis Report

Original Shipment_Document.PDF.exe

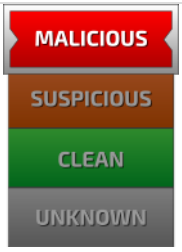
Overview

General Information

Sample Name:	Original Shipment_Document.PDF.exe
Analysis ID:	679174
MD5:	626cdeaa4696c8..
SHA1:	b094f5e4c3792a..
SHA256:	d8519cee2bbf5c...
Tags:	exe guloader
Infos:	



Detection



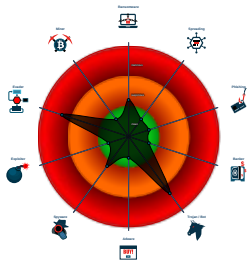
GuLoader

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Yara detected GuLoader
- Initial sample is a PE file and has a...
- Mass process execution to delay an...
- Obfuscated command line found
- Tries to detect virtualization through...
- Executable has a suspicious name ...
- C2 URLs / IPs found in malware con...
- Uses an obfuscated file name to hid...
- Uses 32bit PE files
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /...

Classification



Process Tree

- **System is w10x64**
- Original Shipment_Document.PDF.exe (PID: 3516 cmdline: "C:\Users\user\Desktop\Original Shipment_Document.PDF.exe" MD5: 626CDEAA4696C819FD07921073F6C740)
  - cmd.eXe (PID: 5672 cmdline: cmd.eXe /c SeT /a "0x721C070B^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5656 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 4668 cmdline: cmd.eXe /c SeT /a "0x7C156677^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 4552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Conhost.exe (PID: 5640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Conhost.exe (PID: 5076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 2980 cmdline: cmd.eXe /c SeT /a "0x03631637^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 2952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Conhost.exe (PID: 5636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Conhost.exe (PID: 1428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Conhost.exe (PID: 5884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Conhost.exe (PID: 3720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 5736 cmdline: cmd.eXe /c SeT /a "0x5C382120^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 5628 cmdline: cmd.eXe /c SeT /a "0x7F303920^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 3204 cmdline: cmd.eXe /c SeT /a "0x78713865^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 5920 cmdline: cmd.eXe /c SeT /a "0x4B6D7569^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 6008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 6024 cmdline: cmd.eXe /c SeT /a "0x19307575^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 6112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 2996 cmdline: cmd.eXe /c SeT /a "0x41616575^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 6004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 6080 cmdline: cmd.eXe /c SeT /a "0x09696575^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 4668 cmdline: cmd.eXe /c SeT /a "0x0975752C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - cmd.eXe (PID: 2980 cmdline: cmd.eXe /c SeT /a "0x19697965^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - cmd.eXe (PID: 5696 cmdline: cmd.eXe /c SeT /a "0x49796569^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 3652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.eXe (PID: 1104 cmdline: cmd.eXe /c SeT /a "0x19307571^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - Conhost.exe (PID: 5752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- cmd.eXe (PID: 5772 cmdline: cmd.eXe /c SeT /a "0x15793C65^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 6012 cmdline: cmd.eXe /c SeT /a "0x09216D75^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 6124 cmdline: cmd.eXe /c SeT /a "0x15793C65^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 5892 cmdline: cmd.eXe /c SeT /a "0x09703C6B^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 5640 cmdline: cmd.eXe /c SeT /a "0x4B6C7578^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
- cmd.eXe (PID: 2216 cmdline: cmd.eXe /c SeT /a "0x721C070B^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 5464 cmdline: cmd.eXe /c SeT /a "0x7C156677^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Conhost.exe (PID: 344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 1220 cmdline: cmd.eXe /c SeT /a "0x0363032C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 6040 cmdline: cmd.eXe /c SeT /a "0x4B2D2024^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 5144 cmdline: cmd.eXe /c SeT /a "0x55183929^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 2196 cmdline: cmd.eXe /c SeT /a "0x563A7D2C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5524 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 6088 cmdline: cmd.eXe /c SeT /a "0x09753C65^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Conhost.exe (PID: 5144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 1428 cmdline: cmd.eXe /c SeT /a "0x09216475^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Conhost.exe (PID: 5920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 4700 cmdline: cmd.eXe /c SeT /a "0x09696575^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 5128 cmdline: cmd.eXe /c SeT /a "0x15793C65^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 6088 cmdline: cmd.eXe /c SeT /a "0x09216675^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
- cmd.eXe (PID: 1428 cmdline: cmd.eXe /c SeT /a "0x09697965^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
- cmd.eXe (PID: 4588 cmdline: cmd.eXe /c SeT /a "0x5079653D^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 1892 cmdline: cmd.eXe /c SeT /a "0x0D697C35^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 5828 cmdline: cmd.eXe /c SeT /a "0x172B6478^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 5784 cmdline: cmd.eXe /c SeT /a "0x721C070B^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 2536 cmdline: cmd.eXe /c SeT /a "0x7C156677^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 6108 cmdline: cmd.eXe /c SeT /a "0x03630620^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 6136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Conhost.exe (PID: 4412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 2952 cmdline: cmd.eXe /c SeT /a "0x4D1F3C29^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
- cmd.eXe (PID: 5312 cmdline: cmd.eXe /c SeT /a "0x5C093A2C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 5888 cmdline: cmd.eXe /c SeT /a "0x572D3037^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 2644 cmdline: cmd.eXe /c SeT /a "0x11307537^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 1296 cmdline: cmd.eXe /c SeT /a "0x0C75752C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 4596 cmdline: cmd.eXe /c SeT /a "0x19686375^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 4812 cmdline: cmd.eXe /c SeT /a "0x09697569^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 2660 cmdline: cmd.eXe /c SeT /a "0x19307575^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 3280 cmdline: cmd.eXe /c SeT /a "0x15307575^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 6108 cmdline: cmd.eXe /c SeT /a "0x10307B37^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
- cmd.eXe (PID: 5184 cmdline: cmd.eXe /c SeT /a "0x0A64721C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 6028 cmdline: cmd.eXe /c SeT /a "0x721C070B^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 2952 cmdline: cmd.eXe /c SeT /a "0x7C156677^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
- cmd.eXe (PID: 3400 cmdline: cmd.eXe /c SeT /a "0x03630720^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 5928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 6116 cmdline: cmd.eXe /c SeT /a "0x583D132C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 1524 cmdline: cmd.eXe /c SeT /a "0x553C7D2C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 4532 cmdline: cmd.eXe /c SeT /a "0x4B6C7965^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)

- Conhost.exe (PID: 3812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 908 cmdline: cmd.eXe /c SeT /a "0x50792774^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 4708 cmdline: cmd.eXe /c SeT /a "0x15793C65^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 1332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 1128 cmdline: cmd.eXe /c SeT /a "0x09216475^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 4920 cmdline: cmd.eXe /c SeT /a "0x09696575^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 5464 cmdline: cmd.eXe /c SeT /a "0x15733C65^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
- cmd.eXe (PID: 4336 cmdline: cmd.eXe /c SeT /a "0x0975752C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 4412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 4712 cmdline: cmd.eXe /c SeT /a "0x19697C2C^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 4600 cmdline: cmd.eXe /c SeT /a "0x172B6678^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 2644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 4772 cmdline: cmd.eXe /c SeT /a "0x4C2A3037^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - Conhost.exe (PID: 3212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.eXe (PID: 2952 cmdline: cmd.eXe /c SeT /a "0x0A6B6F7F^962155845" MD5: F3BDBE3BB6F734E357235F4D5898582D)

- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1RTjXzM3oLxMQRuQuQg9TR4kX_hPJtp2r"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.520490666.00000000030F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

System Summary

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation

Yara detected GuLoader

Obfuscated command line found

Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion

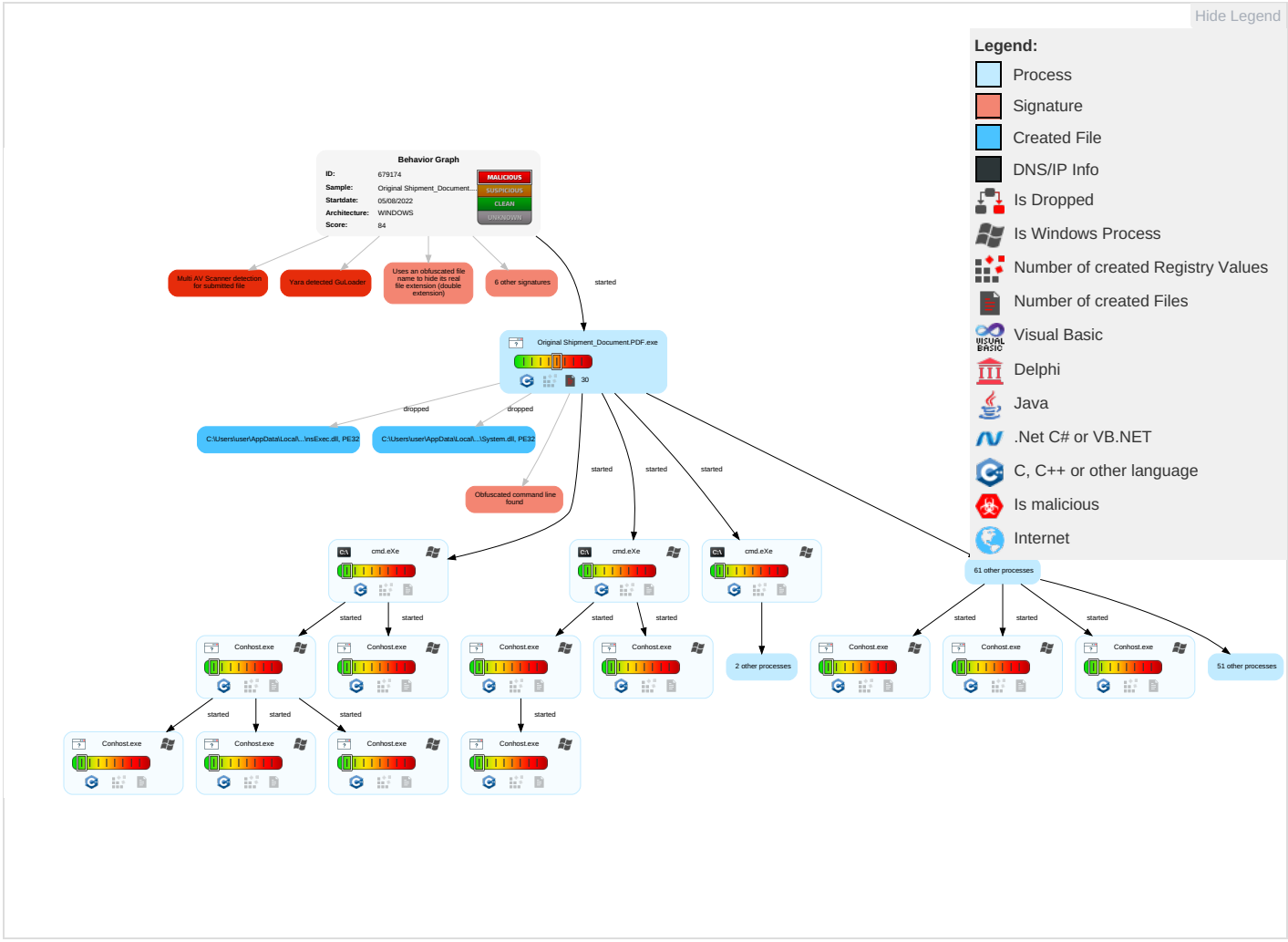
Mass process execution to delay analysis

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

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

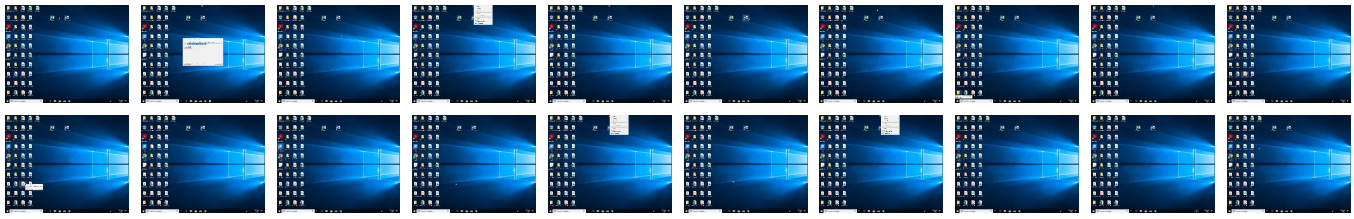
Behavior Graph



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
Original Shipment_Document.PDF.exe	32%	Virustotal		Browse
Original Shipment_Document.PDF.exe	22%	ReversingLabs	Win32.Trojan.Guloader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\nsExec.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\nsExec.dll	4%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\nsExec.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

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://nsis.sf.net/NSIS_ErrorError	Original Shipment_Document.PDF.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679174
Start date and time: 05/08/202211:23:09	2022-08-05 11:23:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Original Shipment_Document.PDF.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	149
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:	mal84.troj.evad.winEXE@185/6@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.9% (good quality ratio 61.7%) • Quality average: 88.6% • Quality standard deviation: 21.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nse53EC.tmp\System.dll

Process:	C:\Users\user\Desktop\Original Shipment_Document.PDF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\nse53EC.tmp\nsExec.dll

Process:	C:\Users\user\Desktop\Original Shipment_Document.PDF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	5.298362543684714
Encrypted:	false
SSDEEP:	96:J9zdzBzMDByZtr/HDQIUIq9m6v6vBckzu9wSBpLEgvElHlernNQaSGYuH2DQ:JykDr/HA5v6G2lElFernNQZGdHW
MD5:	675C4948E1EFC929EDCABFE67148EDDD
SHA1:	F5BDD2C4329ED2732ECFE3423C3CC482606EB28E
SHA-256:	1076CA39C449ED1A968021B76EF31F22A5692DFAFEEA29460E8D970A63C59906
SHA-512:	61737021F86F54279D0A4E35DB0D0808E9A55D89784A31D597F2E4B65B7BBEEC99AA6C79D65258259130EEDA2E5B2820F4F1247777A3010F2DC53E30C612A683
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 4%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,.....Rich.....PE..L.....Oa.....!. ....P.....@.....$..l.... ..P.....@..... .....text..... ..`.rdata..<.... .....@..@.data.....0.....@....reloc.....@.....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\Integrationsprvens.Adg72

Process:	C:\Users\user\Desktop\Original Shipment_Document.PDF.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	56802
Entropy (8bit):	3.999776572782735
Encrypted:	false
SSDEEP:	1536:MiSOEpxqtPV0vXzt3Ov2Kh2+ir/qY3TAK7tgjofP:QpeSPztK2YVK7iE
MD5:	7C22C978F9497BB753456B3AA833F7DE
SHA1:	5566F37ED12035AD659E8E71B09A46FC3A907D27
SHA-256:	8126292C7A2EE04C5D5286BCD0584CF8FF39745F17E28DE70A72CBF1EBCA900B
SHA-512:	C33B835EFC5EB8C19A6429E588D8BD6BBD6C26DA379B7F24A6322CDF09094DF777C7C1DBB0B41E43EE5F24D5A11374E2D95135E70EC4285C0C28A8D3F7644 4B
Malicious:	false
Preview:	751B5626ED1D59DCECA17FC07B6590E02267FE3B2CD7A757A3164D2442E94F22E7417624324FB00CADEF5E125A7A344E60BED74BC30F36CD1FC851B3 AD4732C6EA226EB072F8E714BFA6387A8D207880017E9AC6FEEBE6A73C2845B2010C4322E8DC529575F955085F49CFD5389BA20DB5FE9CCA8B739E13 6A7672B5D2F4472D326B8961AC7A1D2BE941B3207256738921359864F7DCD7AEC49C3C1E7CC69AF9A2AF9CB338F2002503BA46ECAC9CB7044F3290D9 0BAC2852B3BB0083DC03E4D5EBA5CEA9D0A787F3862CCD2C6EC3325DEACC5CB5818C829C68E98E4C9833F007B86693B4C6776056B342C33E34C5201C 378F536C73A444DA46B37933404F6CDE80F0FF3BEE724769B921E9A924F35714874EB7DC63C16604B0487C1A2F1D201C1C8B5CD77378607E2DF70370 56A2043753275C1A55BA8CD1CFEC4571E57D5A2331ED816A72AD23FF030A715BC4CDEF157B56B25E576F4F59EB903849D9446368C20AC6283FDD2627 141ED25B1A794C55D1FDD15E1F6F5B78A58957BA7871754426D16868771513FAD305AEA8DD85058FC14F2437A34BBC4DEBA70E52D1ACE512EA32218D FED4211F0B5EA40ECD74C2062AA179E6DD0BBE910ADAA8CC1974916BD62BE762ED036F9C2A8BDF043DBB4411C94797F2B82DE9BA0A257AC9E7458DE8 3CC1AAF0A8D0249200F483B276BFE5D91DFE0787

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\format-text-bold-symbolic.svg

Process:	C:\Users\user\Desktop\Original Shipment_Document.PDF.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1330
Entropy (8bit):	4.276818433927216
Encrypted:	false
SSDEEP:	24:2dPnnxu3tlACrmYbJ1BtxhUuLos3CrmYbJ1qtxhUuLosN:cfnz6XXNUuLos36XcNUuLosN
MD5:	B0BE3814C6303C5B8C080D654FDF2EA7
SHA1:	8231CACDA98442D068D80EC063CE75DC05AE7A2E
SHA-256:	4A71E8903E3673A98AB8D8BAC7579F7EA2D8C016ADC7ABC6EA23F5565D8643DA
SHA-512:	62F55F19DFE1A8D9B12CD4968401CA19ED332298FBA3ED9DCF714F5E41BA41ED1F8DE07F9F55C90E6B461B73A5F34C2E9C4F505B736960BE814ACB3779F693 A
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <g fill="#2e3436">. <path d="m 5 3 v 2 h 6 c 0.429688 0 1 0.613281 1 1 v 1 h -5 c -0.917969 0 -1.734375 0.378906 -2.25 0.964844 c -0.515625 0.585937 -0.742188 1.324218 -0.738281 2.046875 c 0.007812 0.71875 0.246093 1.445312 0.757812 2.027343 c 0.515625 0.578126 1.320313 0.960938 2.230469 0.960938 h 7 v -7 c 0 -1.632812 -1.320312 -3 -3 -3 z m 2 6 h 5 v 2 h -5 c -0.398438 0 -0.578125 -0.117188 -0.730469 -0.289062 c -0.152343 -0.167969 -0.253906 -0.441407 -0.257812 -0.722657 c 0 -0.277343 0.09375 -0.539062 0.238281 -0.703125 c 0.148438 -0.164062 0.328125 -0.285156 0.75 -0.285156 z m 0 0"/>. <path d="m 4 3 v 2 h 5 c 0.429688 0 1 0.613281 1 1 v 1 h -5 c -0.917969 0 -1.734375 0.378906 -2.25 0.964844 c -0.515625 0.585937 -0.742188 1.324218 -0.738281 2.046875 c 0.007812 0.71875 0.246093 1.445312 0.757812 2.027343 c 0.515625 0.578126 1.320313 0.960938

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\location-services-disabled-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\Original Shipment_Document.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	285
Entropy (8bit):	7.002882763277556
Encrypted:	false
SSDEEP:	6:6v/lhPysuci+aOXTk585U+UliBie7cQkF2HTtWAJdp:6v/7Oci+aOogUVli9AZWBz
MD5:	91B30844C5145188A9DCE697271B8BCF
SHA1:	69C3F0AFA91A3E725A26017EC282499152500DC9
SHA-256:	3B79DEE63724F1BAFFB1E51D55CB96CEB2849C0536000BE3A6C848CE36230049
SHA-512:	6AAF7F986B121484A96B3C85CA382A471DC2B6CFC87C7D7C1838714217C17199649A98825AFF70E62CD0DC2E9C6A3DDF41E4CC743CD44977A452F494340BD77
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...1J.A.....Q..!.I....V.B:.Li.5.F0'.Hi'X.....h.op\t...S..vwh...t..a...^1B/C..2....:Y..W.E.Kl`.W.....@.....w..s&..x..V*.Y3..c.|e.....%.....y..).y8P#c..3.xL..`..c..{.....S...R.1.~.....di....W-z._.....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\uforfrdetheden.Rid

Process:	C:\Users\user\Desktop\Original Shipment_Document.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	99762
Entropy (8bit):	7.345890691572136
Encrypted:	false
SSDEEP:	1536:C42UhrrhyVKSRG5jbu3E4ClJB8SkPoVcrlCDh4AusPrji0Dz:GG0KSRCnu3E9qdbos94AuuPP/
MD5:	251EE827C992B4E481634030C2E681F3
SHA1:	88065FA2EDAE7B94B6891675DF8A9028DC5F28E6
SHA-256:	E9DD8E6A46B89E22E83743D0578339458E7C2CE719BFF5FDD9FDC66652DB161A
SHA-512:	6042BAD2119F19C0355DC43C7CC0F03A5943C524252DC7F0DA0FF4ED254D9486EC3C485BBF0D8010CF5CBF2A22B5F2BFFA8247D87EEFFEF91A72B891FCFAD9D
Malicious:	false
Preview:	Y.!&.Z....o.....-....D....8.)8E^.+.....a..7..[?cH.Y...d..[....2R.&..f.....,t.y.OO..q.>..@.%..r...h,.N.~xh.....&..{.....6.pR2cM...tM8X.1....q.....;)../0.u...f}...j}.3.....+[._.`VS..U+!yo Y.....?R...Z..X.i...o....O.}...9.`F.e>~.%...E..Z...(?.....j..^zC.>...\.n.3."f....V;.....,....&...-.#...,c....\3Z.....}^!..[A....Y.U./Rz....a.....|.....:5p...._.[...g....B&.-....T.WF..dY..^.Z..W/.....M.V. ....*..:I...A.....{.5.....2f5A.....W*.p.T..9K..n3.Js..N<.L.W...=Hv.8Q.d.(.H!`k.aO....Y....s....l.1.A`H.P<u.Z4..).0.n.....M/GL..JjD.;.P.... .;.H..h.7D.|..e..(._WTD.....:<J^..a....Eq]}.f....t...J&.:d+t.....5.)]'.ww..`.A...q....!.....Y..7...X.p.y.D...].y...P.=pc..V&T. `W}B.....%..D."...P....#.,,..:.&."4$1..e.9Z.....F2."mTM....~...g.....c..%".T...q..$_I...#j...:t...."...t=.e.....@.U.i.U..Bj.....E#...~.r.<....,.UP5t..@e....G....H.....7Ye..i.....^.....9..4C.o.3..F'..A..e..=.u..Bw.6S..^..]..v..&.....<)$On.UxV5.+:..vh....a.q..R...e

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.715600015491742
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:	Original Shipment_Document.PDF.exe
File size:	341696
MD5:	626cdeaa4696c819fd07921073f6c740
SHA1:	b094f5e4c3792a05b7f307ad78d2e52cfcbf87b4
SHA256:	d8519cee2bbf5c257375b339d530b33f275db40c06de0f96911eb5b4f207f2c5
SHA512:	2cbfa1d322bd8b6bd861c97f43ef4778a6ef2fb86b718f2571b54f1ce5874afbdf3a9e1728986c7593eb7f48b2defcff624ac467a5ff2677d9036093edaf88f0
SSDEEP:	6144:JNeZc5FBkXpIwbmr2KEROaPdEY8mff3PgRsmq:JNRTr2KEROoT8mfH+q
TLSH:	9F741AC1E199FCD5C428007659B9E521251BAB6EF0B8493B396A7519B0FF383607BE0F

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	ccc0d4ccccdc6cb4

Static PE Info

General

Entrypoint:	0x4034f7
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:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 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:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="Slnggrebets Buginese Itemizer ", OU="Louped Estes ", E=Kodeskrifter@Blakkers.For, O=Kedging, L=Bury, 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	• 9/30/2021 7:49:03 AM 9/29/2024 7:49:03 AM
Subject Chain	• CN="Slnggrebets Buginese Itemizer ", OU="Louped Estes ", E=Kodeskrifter@Blakkers.For, O=Kedging, L=Bury, S=England, C=GB
Version:	3
Thumbprint MD5:	9531A5E4D76383B4586733B6369AA05A
Thumbprint SHA-1:	EB1025208E0319CC8EEFE675D7F0134D108F989B
Thumbprint SHA-256:	1860FBBE1C07E5046864295E0AE0BA476642D85716E6DDB0C4D6E2BF3405DB86
Serial:	2A16DD32E2795EBB

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]

Instruction
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FC308AD500Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FC308AD4FDAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

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	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x52000	0x2eec8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x52fb0	0x710	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x6515	0x6600	False	0.6615349264705882	data	6.439707948554623	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.145774564074664	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.4993489583333333	data	4.013698650446401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x27000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x52000	0x2eec8	0x2f000	False	0.3425500748005319	data	5.305541691795029	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x52340	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x62b68	0x94a8	data	English	United States
RT_ICON	0x6c010	0x6cb4	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x72cc8	0x5488	data	English	United States
RT_ICON	0x78150	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 1056964608	English	United States
RT_ICON	0x7c378	0x25a8	data	English	United States
RT_ICON	0x7e920	0x10a8	data	English	United States
RT_ICON	0x7f9c8	0x988	data	English	United States
RT_ICON	0x80350	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x807b8	0x100	data	English	United States
RT_DIALOG	0x808b8	0x11c	data	English	United States
RT_DIALOG	0x809d8	0xc4	data	English	United States
RT_DIALOG	0x80aa0	0x60	data	English	United States
RT_GROUP_ICON	0x80b00	0x84	data	English	United States
RT_MANIFEST	0x80b88	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject

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

Possible Origin

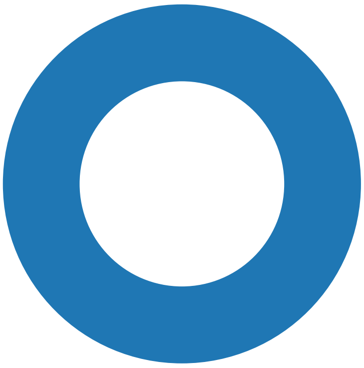
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- Original Shipment_Document.PDF....
- 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: Original Shipment_Document.PDF.exe PID: 3516, Parent PID: 472

General

Target ID:	0
Start time:	11:24:13
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\Original Shipment_Document.PDF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Original Shipment_Document.PDF.exe"
Imagebase:	0x400000
File size:	341696 bytes
MD5 hash:	626CDEAA4696C819FD07921073F6C740
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.520490666.00000000030F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsf495B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405AC1	CreateDirectoryW
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	2	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405AC1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\uforfrdetheden.Rid	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\format-text-bold-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\Integrationsprvens.Adg72	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\location-services-disabled-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\nso52F1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nse53EC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
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	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse53EC.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	405A81	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\nsExec.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\nsExec.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	73	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	406023	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf495B.tmp	success or wait	1	40383F	DeleteFileW
C:\Users\user\AppData\Local\Temp\nse53EC.tmp	success or wait	1	405C42	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\uforfrdetheden.Rid	0	16407	59 fd 21 26 fd 5a fd fd 0f 0a 6f fd 19 fd fd fd 2d fd fd fd fd 44 1d 1b fd fd 38 fd 29 38 45 5e fd 2b 7f fd fd d1 15 61 fd fd 37 1a 2e 5b 3f 63 48 1a 59 fd fd fd 64 1d 13 5b fd fd 09 fd 32 52 05 26 fd fd 66 2e fd fd fd fd 2c 74 fd 79 fd 4f 4f fd fd 71 fd 3e fd fd 40 fd 25 fd fd 72 fd fd 17 68 2c fd 4e 0c 7e 78 68 fd fd fd fd 1c fd 26 fd fd 7b 00 fd 79 1b fd 36 db 70 52 32 63 4d fd 10 fd 74 4d 38 58 e3 31 18 fd 12 fd 71 03 fd 06 fd 0b fd fd 3b 29 fd fd fd 2f 30 fd 75 fd fd fd 66 7d fd fd fd 6a 7d fd 33 fd fd 06 13 02 07 2b 5b fd 5f c5 60 56 53 fd fd 55 2b 21 79 6f 59 fd fd 16 fd fd fd fd fd 3f 52 fd 0f fd 5a fd fd 58 fd 69 0b fd fd 6f 09 fd fd 03 4f 0c 7d fd 14 fd 39 fd 60 46 01 65 3e 7e fd 25 07 11 fd 45 fd 06 5a fd fd fd 28	Y!&Zo-D8)8E^+a7.[?cHYd[2R&f.,tyOOq>@%rh,N~xh&{6pR2cMtM8X1q;)/0uf}j}3+[_`VSU+!yoY?RZXioO}9`Fe>~%EZ(	success or wait	5	4060C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\format-text-bold-symbolic.svg	0	1330	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 36 70 78 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 22 20 77 69 64 74 68 3d 22 31 36 70 78 22 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 3e 0a 20 20 20 20 3c 67 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36 22 3e 0a 20 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 35 20 33 20 76 20 32 20 68 20 36 20 63 20 30 2e 34 32 39 36 38 38 20 30 20 31 20 30 2e 36 31 33 32 38 31 20 31 20 31 20 76 20 31 20 68 20 2d 35 20 63 20 2d 30 2e 39 31 37 39 36 39 20 30 20 2d 31 2e 37 33 34 33 37 35 20 30 2e 33 37 38 39 30 36 20 2d 32 2e 32	751B5626ED1D59DCECA17FC07B6590E02267FE3B2CD7A757A3164D2442E94F22E7417624324FB00CADEF5E125A7A344E60BED74BC30F36CD1FC851B3AD4732C6EA226EB072F8E714BFA6387A8D207880017E9AC6FEEBE6A73C2845B2010C4322E8DC529575F955085F49CFD5389BA20DB5FE9CCA8B739E136A7672B5D2F4472	success or wait	1	4060C3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\Integrationsprvens.Adg72	0	31423	37 35 31 42 35 36 32 36 45 44 31 44 35 39 44 43 45 43 41 31 37 46 43 30 37 42 36 35 39 30 45 30 32 32 36 37 46 45 33 42 32 43 44 37 41 37 35 37 41 33 31 36 34 44 32 34 34 32 45 39 34 46 32 32 45 37 34 31 37 36 32 34 33 32 34 46 42 30 30 43 41 44 45 46 35 45 31 32 35 41 37 41 33 34 34 45 36 30 42 45 44 37 34 42 43 33 30 46 33 36 43 44 31 46 43 38 35 31 42 33 41 44 34 37 33 32 43 36 45 41 32 32 36 45 42 30 37 32 46 38 45 37 31 34 42 46 41 36 33 38 37 41 38 44 32 30 37 38 38 30 30 31 37 45 39 41 43 36 46 45 45 42 45 36 41 37 33 43 32 38 34 35 42 32 30 31 30 43 34 33 32 32 45 38 44 43 35 32 39 35 37 35 46 39 35 35 30 38 35 46 34 39 43 46 44 35 33 38 39 42 41 32 30 44 42 35 46 45 39 43 43 41 38 42 37 33 39 45 31 33 36 41 37 36 37 32 42 35 44 32 46 34 34 37 32	751B5626ED1D59DCECA17FC07B6590E02267FE3B2CD7A757A3164D2442E94F22E7417624324FB00CADEF5E125A7A344E60BED74BC30F36CD1FC851B3AD4732C6EA226EB072F8E714BFA6387A8D207880017E9AC6FEEBE6A73C2845B2010C4322E8DC529575F955085F49CFD5389BA20DB5FE9CCA8B739E136A7672B5D2F4472	success or wait	2	4060C3	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\location-services-disabled-symbolic.symbolic.png</td><td>0</td><td>285</td><td>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 fd 49 44 41 54 38 fd fd 31 4a fd 41 10 06 fd 17 fd fd fd 51 1b 11 fd 21 16 49 fd fd fd 56 02 42 3a fd 4c 69 fd 35 fd 46 30 27 fd 48 69 27 58 0a fd fd fd 68 fd 6f 70 5c 74 fd fd 07 53 fd fd 76 77 68 fd fd fd 74 fd fd 61 7b fd 13 5e 31 42 2f 43 fd 02 32 fd fd fd 3a 59 04 fd 57 fd 45 fd 4b 6c 60 13 57 fd 7f fd 01 fd 01 fd 40 fd fd fd 02 fd 01 77 fd fd 73 26 fd 0a 78 fd 07 56 2a fd 59 33 fd fd 63 fd 7c 65 fd fd fd 05 fd 87 fd 25 fd fd 19 fd fd fd 04 79 fd fd 29 fd 79 38 50 23 63 c3 fd 33 fd 78 4c fd fd 60 fd fd 63 12 fd 7b fd 2e fd 1c fd fd 53 1c fd fd 52 fd 31 fd 7e</td><td>PNGIHDRasBIT|dIDAT81JAQ!IVB:Li5F0'Hi'Xhop\tSvwhta^1B/C2:YWEKl`W@ws&xV*Y3c|e%y)y8P#c3xL`c{.SR1~</td><td>success or wait</td><td>1</td><td>4060C3</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nse53EC.tmp\nsExec.dll</td><td>0</td><td>7168</td><td>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 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2c fd fd fd fd fd fb ef fd fd fd fd 10 1b fd fd fd fd 52 69 63 68 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 06 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 0e 00 00 00 0e 00 00 00 00 00 00 fd 10 00 00 00 10 00</td><td>MZ@!L!This program cannot be run in DOS mode.$,RichPELOa.!</td><td>success or wait</td><td>1</td><td>4060C3</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse53EC.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060C3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Original Shipment_Document.PDF.exe	unknown	512	success or wait	448	406094	ReadFile
C:\Users\user\Desktop\Original Shipment_Document.PDF.exe	unknown	4	success or wait	2	406094	ReadFile
C:\Users\user\Desktop\Original Shipment_Document.PDF.exe	unknown	4	success or wait	13	406094	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\timelrer\Tdlen\Integrationsprvens.Adg72	unknown	2	success or wait	1023	40275E	ReadFile
C:\Users\user\Desktop\Original Shipment_Document.PDF.exe	unknown	4	success or wait	4	406094	ReadFile

Analysis Process: cmd.eXe PID: **5672**, Parent PID: **3516**

General

Target ID:	1
Start time:	11:24:16
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x721C070B^962155845"
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: **5656**, Parent PID: **5672**

General

Target ID:	2
Start time:	11:24:17
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	

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

Analysis Process: cmd.eXe PID: **4668**, Parent PID: **3516**

General

Target ID:	3
Start time:	11:24:17
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x7C156677^962155845"
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: **4552**, Parent PID: **4668**

General

Target ID:	4
Start time:	11:24:18
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.eXe PID: **2980**, Parent PID: **3516**

General

Target ID:	6
Start time:	11:24:18
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x03631637^962155845"
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: **2952**, Parent PID: **2980**

General	
Target ID:	7
Start time:	11:24:18
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.eXe PID: **5736**, Parent PID: **3516**

General	
Target ID:	8
Start time:	11:24:19
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x5C382120^962155845"
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: **5764**, Parent PID: **5736**

General	
Target ID:	10
Start time:	11:24:19
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5628**, Parent PID: **3516**

General	
Target ID:	11
Start time:	11:24:20
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x7F303920^962155845"
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: **5692**, Parent PID: **5628**

General	
Target ID:	12
Start time:	11:24:20
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **3204**, Parent PID: **3516**

General	
Target ID:	13
Start time:	11:24:20
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x78713865^962155845"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5660**, Parent PID: **3204**

General	
Target ID:	14
Start time:	11:24:20
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	

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

Analysis Process: cmd.eXe PID: **5920**, Parent PID: **3516**

General

Target ID:	15
Start time:	11:24:21
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x4B6D7569^962155845"
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: **6008**, Parent PID: **5920**

General

Target ID:	17
Start time:	11:24:21
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **6024**, Parent PID: **3516**

General

Target ID:	18
Start time:	11:24:21
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x19307575^962155845"
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: **6112**, Parent PID: **6024**

General	
Target ID:	19
Start time:	11:24:22
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **2996**, Parent PID: **3516**

General	
Target ID:	20
Start time:	11:24:22
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x41616575^962155845"
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: **6004**, Parent PID: **2996**

General	
Target ID:	21
Start time:	11:24:22
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **6080**, Parent PID: **3516**

General	
Target ID:	22
Start time:	11:24:22
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe

Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09696575^962155845"
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: **5096**, Parent PID: **6080**

General	
Target ID:	23
Start time:	11:24:23
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4668**, Parent PID: **3516**

General	
Target ID:	24
Start time:	11:24:23
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x0975752C^962155845"
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: **5640**, Parent PID: **4668**

General	
Target ID:	25
Start time:	11:24:23
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **2980**, Parent PID: **3516**

General	
Target ID:	26
Start time:	11:24:24
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x19697965^962155845"
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: **3720**, Parent PID: **2980**

General	
Target ID:	27
Start time:	11:24:24
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5696**, Parent PID: **3516**

General	
Target ID:	28
Start time:	11:24:24
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x49796569^962155845"
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: **3652**, Parent PID: **5696**

General	
Target ID:	29
Start time:	11:24:25

Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **1104**, Parent PID: **3516**

General	
Target ID:	30
Start time:	11:24:25
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x19307571^962155845"
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: **5752**, Parent PID: **1104**

General	
Target ID:	31
Start time:	11:24:25
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff73c930000
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: **5772**, Parent PID: **3516**

General	
Target ID:	32
Start time:	11:24:26
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x15793C65^962155845"
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: **5780**, Parent PID: **5772**

General	
Target ID:	33
Start time:	11:24:26
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **6012**, Parent PID: **3516**

General	
Target ID:	34
Start time:	11:24:27
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09216D75^962155845"
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: **6044**, Parent PID: **6012**

General	
Target ID:	35
Start time:	11:24:28
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **6124**, Parent PID: **3516**

General	
Target ID:	36

Start time:	11:24:30
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x15793C65^962155845"
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: **6112**, Parent PID: **6124**

General	
Target ID:	37
Start time:	11:24:32
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5892**, Parent PID: **3516**

General	
Target ID:	39
Start time:	11:24:32
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09703C6B^962155845"
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: **2344**, Parent PID: **5892**

General	
Target ID:	40
Start time:	11:24:33
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: cmd.eXe PID: **5640**, Parent PID: **3516**

General	
Target ID:	42
Start time:	11:24:33
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x4B6C7578^962155845"
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: **5076**, Parent PID: **5640**

General	
Target ID:	43
Start time:	11:24:34
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **2216**, Parent PID: **3516**

General	
Target ID:	45
Start time:	11:24:35
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x721C070B^962155845"
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: **2236**, Parent PID: **2216**

General

Target ID:	47
Start time:	11:24:35
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5464**, Parent PID: **3516**

General

Target ID:	48
Start time:	11:24:35
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x7C156677^962155845"
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: **1464**, Parent PID: **5464**

General

Target ID:	49
Start time:	11:24:36
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **1220**, Parent PID: **3516**

General

Target ID:	50
Start time:	11:24:36
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x0363032C^962155845"
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: **4264**, Parent PID: **1220**

General	
Target ID:	52
Start time:	11:24:36
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **6040**, Parent PID: **3516**

General	
Target ID:	54
Start time:	11:24:37
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x4B2D2024^962155845"
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: **6044**, Parent PID: **6040**

General	
Target ID:	55
Start time:	11:24:37
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5144**, Parent PID: **3516**

General	
Target ID:	57
Start time:	11:24:38
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x55183929^962155845"
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: **6056**, Parent PID: **5144**

General	
Target ID:	58
Start time:	11:24:38
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **2196**, Parent PID: **3516**

General	
Target ID:	61
Start time:	11:24:38
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x563A7D2C^962155845"
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: **5524**, Parent PID: **2196**

General	
Target ID:	62
Start time:	11:24:39
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	

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

Analysis Process: cmd.eXe PID: **6088**, Parent PID: **3516**

General	
Target ID:	63
Start time:	11:24:39
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09753C65^962155845"
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: **6048**, Parent PID: **6088**

General	
Target ID:	64
Start time:	11:24:39
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **1428**, Parent PID: **3516**

General	
Target ID:	65
Start time:	11:24:40
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09216475^962155845"
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: **3920**, Parent PID: **1428**

General	
Target ID:	66
Start time:	11:24:40
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4700**, Parent PID: **3516**

General	
Target ID:	67
Start time:	11:24:40
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09696575^962155845"
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: **2244**, Parent PID: **4700**

General	
Target ID:	68
Start time:	11:24:41
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5128**, Parent PID: **3516**

General	
Target ID:	69
Start time:	11:24:41
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	

Commandline:	cmd.eXe /c SeT /a "0x15793C65^962155845"
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: **6044**, Parent PID: **5128**

General

Target ID:	70
Start time:	11:24:41
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **6088**, Parent PID: **3516**

General

Target ID:	71
Start time:	11:24:42
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09216675^962155845"
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: **5144**, Parent PID: **6088**

General

Target ID:	72
Start time:	11:24:42
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **1428**, Parent PID: **3516**

General	
Target ID:	73
Start time:	11:24:42
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09697965^962155845"
Imagebase:	
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **5920**, Parent PID: **1428**

General	
Target ID:	74
Start time:	11:24:42
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4588**, Parent PID: **3516**

General	
Target ID:	75
Start time:	11:24:43
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x5079653D^962155845"
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: **6048**, Parent PID: **4588**

General	
Target ID:	76
Start time:	11:24:43
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe

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

Analysis Process: cmd.eXe PID: **1892**, Parent PID: **3516**

General	
Target ID:	77
Start time:	11:24:43
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x0D697C35^962155845"
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: **3920**, Parent PID: **1892**

General	
Target ID:	78
Start time:	11:24:44
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5828**, Parent PID: **3516**

General	
Target ID:	79
Start time:	11:24:44
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x172B6478^962155845"
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: **5828**

General	
Target ID:	80
Start time:	11:24:44
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5784**, Parent PID: **3516**

General	
Target ID:	81
Start time:	11:24:45
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x721C070B^962155845"
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: **6044**, Parent PID: **5784**

General	
Target ID:	82
Start time:	11:24:45
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **2536**, Parent PID: **3516**

General	
Target ID:	83
Start time:	11:24:45

Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x7C156677^962155845"
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: **4588**, Parent PID: **2536**

General	
Target ID:	84
Start time:	11:24:45
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **6108**, Parent PID: **3516**

General	
Target ID:	85
Start time:	11:24:46
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x03630620^962155845"
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: **6136**, Parent PID: **6108**

General	
Target ID:	86
Start time:	11:24:46
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	

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

Analysis Process: cmd.eXe PID: **2952**, Parent PID: **3516**

General	
Target ID:	87
Start time:	11:24:46
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x4D1F3C29^962155845"
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: **5636**, Parent PID: **2952**

General	
Target ID:	88
Start time:	11:24:46
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5312**, Parent PID: **3516**

General	
Target ID:	89
Start time:	11:24:47
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x5C093A2C^962155845"
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: **5828**, Parent PID: **5312**

General	
Target ID:	91

Start time:	11:24:47
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5888**, Parent PID: **3516**

General	
Target ID:	92
Start time:	11:24:48
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x572D3037^962155845"
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: **5124**, Parent PID: **5888**

General	
Target ID:	93
Start time:	11:24:49
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **2644**, Parent PID: **3516**

General	
Target ID:	94
Start time:	11:24:51
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x11307537^962155845"
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: **2944**, Parent PID: **2644**

General	
Target ID:	95
Start time:	11:24:51
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **1296**, Parent PID: **3516**

General	
Target ID:	96
Start time:	11:24:51
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x0C75752C^962155845"
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: **1428**, Parent PID: **1296**

General	
Target ID:	97
Start time:	11:24:51
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4596**, Parent PID: **3516**

General

Target ID:	98
Start time:	11:24:52
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x19686375^962155845"
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: **5856**, Parent PID: **4596**

General	
Target ID:	99
Start time:	11:24:52
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4812**, Parent PID: **3516**

General	
Target ID:	100
Start time:	11:24:52
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09697569^962155845"
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: **3416**, Parent PID: **4812**

General	
Target ID:	101
Start time:	11:24:53
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes

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

Analysis Process: cmd.eXe PID: **2660**, Parent PID: **3516**

General	
Target ID:	102
Start time:	11:24:53
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x19307575^962155845"
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: **2660**

General	
Target ID:	103
Start time:	11:24:53
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **3280**, Parent PID: **3516**

General	
Target ID:	104
Start time:	11:24:54
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x15307575^962155845"
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: **5144**, Parent PID: **3280**

General	
Target ID:	105
Start time:	11:24:54
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **6108**, Parent PID: **3516**

General	
Target ID:	106
Start time:	11:24:54
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x10307B37^962155845"
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: **4412**, Parent PID: **6108**

General	
Target ID:	107
Start time:	11:24:54
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5184**, Parent PID: **3516**

General	
Target ID:	108
Start time:	11:24:55
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x0A64721C^962155845"
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: **4400**, Parent PID: **5184**

General	
Target ID:	109
Start time:	11:24:55
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **6028**, Parent PID: **3516**

General	
Target ID:	110
Start time:	11:24:55
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x721C070B^962155845"
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: **2944**, Parent PID: **6028**

General	
Target ID:	111
Start time:	11:24:56
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **2952**, Parent PID: **3516**

General	
Target ID:	112
Start time:	11:24:56
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x7C156677^962155845"
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: **1428**, Parent PID: **2952**

General	
Target ID:	113
Start time:	11:24:56
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **3400**, Parent PID: **3516**

General	
Target ID:	114
Start time:	11:24:56
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x03630720^962155845"
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: **5928**, Parent PID: **3400**

General	
Target ID:	115
Start time:	11:24:57
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	

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

Analysis Process: cmd.eXe PID: **6116**, Parent PID: **3516**

General

Target ID:	116
Start time:	11:24:57
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x583D132C^962155845"
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: **2788**, Parent PID: **6116**

General

Target ID:	117
Start time:	11:24:57
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **1524**, Parent PID: **3516**

General

Target ID:	118
Start time:	11:24:58
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x553C7D2C^962155845"
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: **4504**, Parent PID: **1524**

General	
Target ID:	119
Start time:	11:24:58
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4532**, Parent PID: **3516**

General	
Target ID:	120
Start time:	11:24:59
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x4B6C7965^962155845"
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: **3812**, Parent PID: **4532**

General	
Target ID:	121
Start time:	11:24:59
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **908**, Parent PID: **3516**

General	
Target ID:	122
Start time:	11:24:59
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe

Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x50792774^962155845"
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: **748**, Parent PID: **908**

General	
Target ID:	123
Start time:	11:24:59
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4708**, Parent PID: **3516**

General	
Target ID:	124
Start time:	11:25:00
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x15793C65^962155845"
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: **1332**, Parent PID: **4708**

General	
Target ID:	125
Start time:	11:25:00
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **1128**, Parent PID: **3516**

General	
Target ID:	126
Start time:	11:25:00
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09216475^962155845"
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: **3876**, Parent PID: **1128**

General	
Target ID:	127
Start time:	11:25:00
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4920**, Parent PID: **3516**

General	
Target ID:	128
Start time:	11:25:01
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x09696575^962155845"
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: **4916**, Parent PID: **4920**

General	
Target ID:	129
Start time:	11:25:01

Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **5464**, Parent PID: **3516**

General	
Target ID:	130
Start time:	11:25:02
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x15733C65^962155845"
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: **344**, Parent PID: **5464**

General	
Target ID:	131
Start time:	11:25:02
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4336**, Parent PID: **3516**

General	
Target ID:	132
Start time:	11:25:02
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x0975752C^962155845"
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: **4412**, Parent PID: **4336**

General	
Target ID:	133
Start time:	11:25:03
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4712**, Parent PID: **3516**

General	
Target ID:	134
Start time:	11:25:03
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x19697C2C^962155845"
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: **2988**, Parent PID: **4712**

General	
Target ID:	135
Start time:	11:25:03
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4600**, Parent PID: **3516**

General	
Target ID:	136

Start time:	11:25:04
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x172B6678^962155845"
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: **2644**, Parent PID: **4600**

General	
Target ID:	137
Start time:	11:25:04
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: cmd.eXe PID: **4772**, Parent PID: **3516**

General	
Target ID:	138
Start time:	11:25:04
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x4C2A3037^962155845"
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: **3212**, Parent PID: **4772**

General	
Target ID:	139
Start time:	11:25:04
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: cmd.eXe PID: **2952**, Parent PID: **3516**

General	
Target ID:	140
Start time:	11:25:05
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.eXe
Wow64 process (32bit):	
Commandline:	cmd.eXe /c SeT /a "0x0A6B6F7F^962155845"
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: **5884**, Parent PID: **2952**

General	
Target ID:	141
Start time:	11:25:05
Start date:	05/08/2022
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Disassembly

No disassembly