


**ID:** 497240
**Sample Name:** tcpmdmaus.exe
**Cookbook:** default.jbs
**Time:** 15:30:09
**Date:** 05/10/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

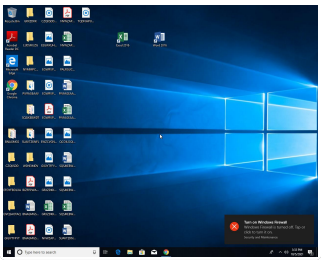
# Windows Analysis Report tcpmdmaus.exe

## Overview

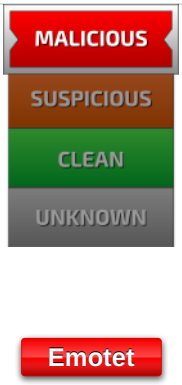
### General Information

| | |
|---|---|
| Sample Name: | tcpmdmaus.exe |
| Analysis ID: | 497240 |
| MD5: | abe13ddc14525c.. |
| SHA1: | 01b8022edd4ef8e. |
| SHA256: | 8524e558dded96.. |
| Infos: | |

Most interesting Screenshot:



### Detection

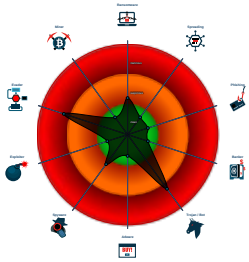



| | |
|---|---|
| Score: | 84 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- Machine Learning detection for samp…
- Hides that the sample has been dow…
- Drops executables to the windows d…
- Uses 32bit PE files
- Queries the volume information (nam…
- Yara signature match
- Deletes files inside the Windows fold…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…

### Classification



## Process Tree

- **System is w10x64**
- tcpmdmaus.exe (PID: 400 cmdline: 'C:\Users\user\Desktop\tcpmdmaus.exe' MD5: ABE13DDC14525C4C35A85224689BFB27)
  - tcpmdmaus.exe (PID: 6768 cmdline: C:\Users\user\Desktop\tcpmdmaus.exe MD5: ABE13DDC14525C4C35A85224689BFB27)
- sharedsls.exe (PID: 4752 cmdline: C:\Windows\SysWOW64\sharedsls.exe MD5: ABE13DDC14525C4C35A85224689BFB27)
  - sharedsls.exe (PID: 5404 cmdline: C:\Windows\SysWOW64\sharedsls.exe MD5: ABE13DDC14525C4C35A85224689BFB27)
- svchost.exe (PID: 6696 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4140 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7056 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6868 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000001.00000002.322257965.0000000001251000.00000020.00000001.sdmp | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 00000001.00000002.322257965.0000000001251000.00000020.00000001.sdmp | Emotet | Emotet Payload | kevoreilly | • 0x5990:$snippet4: 33 C0 C7 05 80 A8 25 01 00 A0 25 01 C7 05 84 A8 25 01 00 A0 25 01 A3 88 A8 25 01 A3 8C A8 25 01 A3 90 A8 25 01 39 05 00 A0 25 01 74 1D 8D 49 00 40 A3 88 A8 25 01 83 3C C5 00 A0 25 01 00 75 F0 ... |
| 00000002.00000002.321224638.0000000001461000.00000020.00000001.sdmp | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 00000002.00000002.321224638.0000000001461000.00000020.00000001.sdmp | Emotet | Emotet Payload | kevoreilly | • 0x5990:$snippet4: 33 C0 C7 05 80 A8 46 01 00 A0 46 01 C7 05 84 A8 46 01 00 A0 46 01 A3 88 A8 46 01 A3 8C A8 46 01 A3 90 A8 46 01 39 05 00 A0 46 01 74 1D 8D 49 00 40 A3 88 A8 46 01 83 3C C5 00 A0 46 01 00 75 F0 ... |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.295437100.0000000000B71000.00000020.00000001.sdmp | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| Click to see the 3 entries | | | | |

### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 1.2.tcpmdmaus.exe.1250000.2.unpack | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 1.2.tcpmdmaus.exe.1250000.2.unpack | Emotet | Emotet Payload | kevoreilly | • 0x5d90:$snippet4: 33 C0 C7 05 80 A8 25 01 00 A0 25 01 C7 05 84 A8 25 01 00 A0 25 01 A3 88 A8 25 01 A3 8C A8 25 01 A3 90 A8 25 01 39 05 00 A0 25 01 74 1D 8D 49 00 40 A3 88 A8 25 01 83 3C C5 00 A0 25 01 00 75 F0 ... |
| 7.2.sharedsls.exe.1450000.3.unpack | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 7.2.sharedsls.exe.1450000.3.unpack | Emotet | Emotet Payload | kevoreilly | • 0x5d90:$snippet4: 33 C0 C7 05 80 A8 45 01 00 A0 45 01 C7 05 84 A8 45 01 00 A0 45 01 A3 88 A8 45 01 A3 8C A8 45 01 A3 90 A8 45 01 39 05 00 A0 45 01 74 1D 8D 49 00 40 A3 88 A8 45 01 83 3C C5 00 A0 45 01 00 75 F0 ... |
| 0.2.tcpmdmaus.exe.b70000.2.unpack | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| Click to see the 3 entries | | | | |

## Sigma Overview

**No Sigma rule has matched**

## Jbx Signature Overview

Click to jump to signature section

### AV Detection:

**Multi AV Scanner detection for submitted file**

**Antivirus / Scanner detection for submitted sample**

**Machine Learning detection for sample**

### E-Banking Fraud:

**Yara detected Emotet**

### System Summary:

**Malicious sample detected (through community Yara rule)**

### Persistence and Installation Behavior:

**Drops executables to the windows directory (C:\Windows) and starts them**

### Hooking and other Techniques for Hiding and Protection:

**Hides that the sample has been downloaded from the Internet (zone.identifier)**

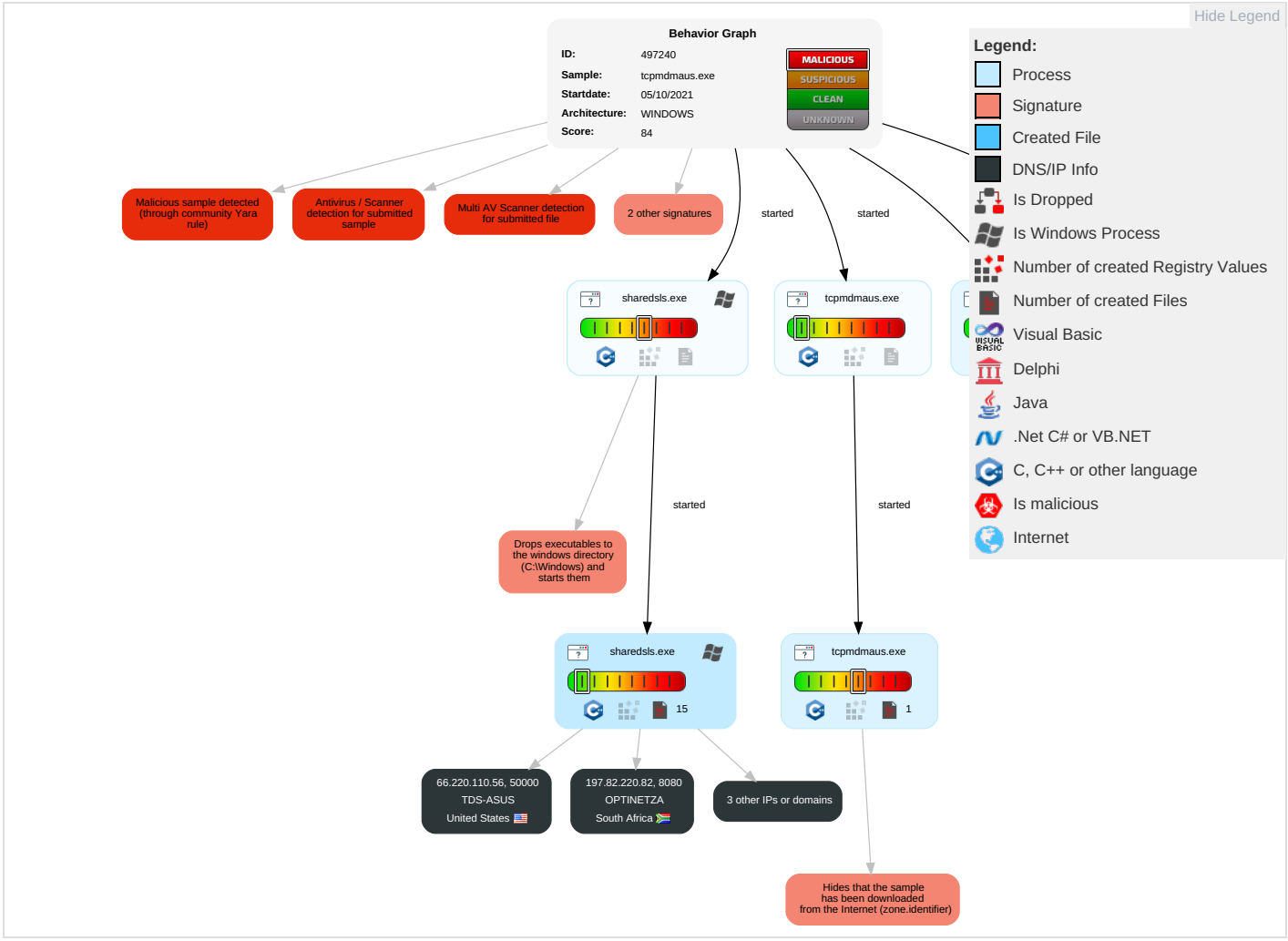
**Stealing of Sensitive Information:**

**Yara detected Emotet**

## 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 1 | Service Execution 1 2 | Valid Accounts 1 | Valid Accounts 1 | Masquerading 1 2 | OS Credential Dumping | Security Software Discovery 1 1 | Remote Services | Archive Collected Data 1 1 | Exfiltration Over Other Network Medium | Encrypted Channel 2 2 | Eavesdr Insecure Network Commur |
| Default Accounts | Scheduled Task/Job | Windows Service 1 2 | Access Token Manipulation 1 | Valid Accounts 1 | LSASS Memory | Virtualization/Sandbox Evasion 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Non-Standard Port 1 | Exploit S Redirect Calls/SM |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Windows Service 1 2 | Virtualization/Sandbox Evasion 1 | Security Account Manager | Process Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Ingress Tool Transfer 1 | Exploit S Track De Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Process Injection 1 | Access Token Manipulation 1 | NTDS | System Service Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Non-Application Layer Protocol 1 | SIM Car Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Process Injection 1 | LSA Secrets | Remote System Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Application Layer Protocol 1 2 | Manipula Device Commur |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Hidden Files and Directories 1 | Cached Domain Credentials | File and Directory Discovery 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming Denial of Service |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Obfuscated Files or Information 1 | DCSync | System Information Discovery 1 4 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue W Access F |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | File Deletion 1 | Proc Filesystem | Network Service Scanning | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgra Insecure Protocols |

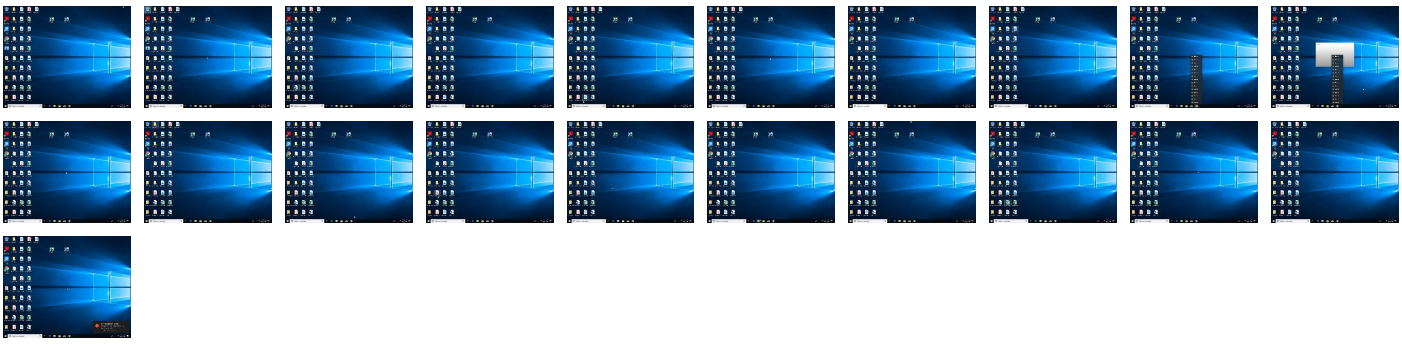
## Behavior Graph




## 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 |
|---|---|---|---|---|
| tcpmdmaus.exe | 85% | Virustotal | | Browse |
| tcpmdmaus.exe | 17% | Metadefender | | Browse |
| tcpmdmaus.exe | 97% | ReversingLabs | Win32.Trojan.Emotet | |
| tcpmdmaus.exe | 100% | Avira | HEUR/AGEN.1116174 | |
| tcpmdmaus.exe | 100% | Joe Sandbox ML | | |

## Dropped Files

No Antivirus matches

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 2.2.sharedsls.exe.12e3d44.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 2.2.sharedsls.exe.1460000.3.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 1.2.tcpmdmaus.exe.1310000.3.unpack | 100% | Avira | HEUR/AGEN.1116174 | | Download File |
| 7.2.sharedsls.exe.1433d44.2.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 0.0.tcpmdmaus.exe.1310000.0.unpack | 100% | Avira | HEUR/AGEN.1116174 | | Download File |
| 0.2.tcpmdmaus.exe.ab3d44.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 1.2.tcpmdmaus.exe.1240000.1.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 1.0.tcpmdmaus.exe.1310000.0.unpack | 100% | Avira | HEUR/AGEN.1116174 | | Download File |

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 7.0.sharedsls.exe.1310000.0.unpack | 100% | Avira | HEUR/AGEN.1116174 | | Download File |
| 0.2.tcpmdmaus.exe.1310000.3.unpack | 100% | Avira | HEUR/AGEN.1116174 | | Download File |
| 1.2.tcpmdmaus.exe.1250000.2.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 0.2.tcpmdmaus.exe.b70000.2.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 0.2.tcpmdmaus.exe.b60000.1.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 2.2.sharedsls.exe.1300000.1.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 7.2.sharedsls.exe.c30000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 2.0.sharedsls.exe.1310000.0.unpack | 100% | Avira | HEUR/AGEN.1116174 | | Download File |
| 2.2.sharedsls.exe.1310000.2.unpack | 100% | Avira | HEUR/AGEN.1116174 | | Download File |
| 7.2.sharedsls.exe.1450000.3.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 1.2.tcpmdmaus.exe.de3d44.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 7.2.sharedsls.exe.1310000.1.unpack | 100% | Avira | HEUR/AGEN.1116174 | | Download File |

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| windowsupdate.s.llnwi.net | 0% | Virustotal | | Browse |

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://www.disneyplus.com/legal/your-california-privacy-rights | 1% | Virustotal | | Browse |
| http://https://www.disneyplus.com/legal/your-california-privacy-rights | 0% | Avira URL Cloud | safe | |
| http://77.157.40.119:443/?6 | 0% | Avira URL Cloud | safe | |
| http://77.157.40.119:443/ | 2% | Virustotal | | Browse |
| http://77.157.40.119:443/ | 0% | Avira URL Cloud | safe | |
| http://77.157.40.119:443/1 | 0% | Avira URL Cloud | safe | |
| http://77.157.40.119:443/. | 0% | Avira URL Cloud | safe | |
| http://66.220.110.56:50000/f | 0% | Avira URL Cloud | safe | |
| http://77.157.40.119:443// | 0% | Avira URL Cloud | safe | |
| http://77.157.40.119:443/& | 0% | Avira URL Cloud | safe | |
| http://crl.ver) | 0% | Avira URL Cloud | safe | |
| http://https://www.tiktok.com/legal/report/feedback | 0% | URL Reputation | safe | |
| http://66.220.110.56:50000/1 | 0% | Avira URL Cloud | safe | |
| http://197.82.220.82:8080/ | 0% | Avira URL Cloud | safe | |
| http://77.157.40.119:443/V | 0% | Avira URL Cloud | safe | |
| http://https://www.disneyplus.com/legal/privacy-policy | 0% | Avira URL Cloud | safe | |
| http://https://77.157.40.119:443/ | 0% | Avira URL Cloud | safe | |
| http://184.186.78.177/:$ | 0% | Avira URL Cloud | safe | |
| http://77.157.40.119:443/#6 | 0% | Avira URL Cloud | safe | |
| http://110.143.116.201/&$ | 0% | Avira URL Cloud | safe | |
| http://110.143.116.201/ | 0% | Avira URL Cloud | safe | |
| http://184.186.78.177/ | 0% | Avira URL Cloud | safe | |
| http://66.220.110.56:50000/ | 0% | Avira URL Cloud | safe | |
| http://https://disneyplus.com/legal. | 0% | Avira URL Cloud | safe | |
| http://110.143.116.201/g$ | 0% | Avira URL Cloud | safe | |
| http://197.82.220.82:8080/v | 0% | Avira URL Cloud | safe | |
| http://197.82.220.82:8080/1 | 0% | Avira URL Cloud | safe | |
| http://110.143.116.201/-$ | 0% | Avira URL Cloud | safe | |
| http://help.disneyplus.com. | 0% | Avira URL Cloud | safe | |

## Domains and IPs

### Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| windowsupdate.s.llnwi.net | 178.79.242.128 | true | false | • 0%, Virustotal, Browse | unknown |

### Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://77.157.40.119:443/ | false | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 184.186.78.177 | unknown | United States | | 22773 | ASN-CXA-ALL-CCI-22773-RDCUS | false |
| 77.157.40.119 | unknown | France | | 15557 | LDCOMNETFR | false |
| 110.143.116.201 | unknown | Australia | | 1221 | ASN-TELSTRATelstraCorporation LtdAU | false |
| 66.220.110.56 | unknown | United States | | 4181 | TDS-ASUS | false |
| 197.82.220.82 | unknown | South Africa | | 10474 | OPTINETZA | false |

### Private

| IP |
|---|
| 192.168.2.1 |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 497240 |
| Start date: | 05.10.2021 |
| Start time: | 15:30:09 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 33s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | tcpmdmaus.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: | 23 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal84.troj.evad.winEXE@10/0@0/6 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 37.9% (good quality ratio 32.1%)<br>• Quality average: 68.6%<br>• Quality standard deviation: 36.2% |
| HCA Information: | • Successful, ratio: 77%<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 |
|---|---|---|
| 15:31:46 | API Interceptor | 10x Sleep call for process: svchost.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 184.186.78.177 | Emotet.doc | Get hash | malicious | Browse | |
| | Emotet.doc | Get hash | malicious | Browse | |
| 110.143.116.201 | EMOTET.EXE | Get hash | malicious | Browse | • 110.143.116.201/ |
| 66.220.110.56 | Daily Payroll for Jun 9 [dv46011].doc | Get hash | malicious | Browse | |
| | Daily Payroll for Jun 9 [dv46011].doc | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| windowsupdate.s.llnwi.net | SOA_SEPT.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | PAYMENT REMITTANCE.jar | Get hash | malicious | Browse | • 178.79.242.0 |
| | P-O9478384.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | PAYMENT REMITTANCE.jar | Get hash | malicious | Browse | • 178.79.242.0 |
| | pgwgFkZRpD.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | theaction.jpg.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | BAF599ABAB1D6969E1BA455F83375CBC9643BBE504918.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | Dbz4oHObUI.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | RQF 100028153.jar | Get hash | malicious | Browse | • 178.79.242.128 |
| | INVOICE PAYMENT PDF.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | RFQ-847393.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | UaZ4NIOJgGSE1F3.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | LOI-20210510473689004882.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | OFFER.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | MxrLKe23Kh.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | Duc2Vs7SsB.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | ERP - US Stock Selection - 202109.xls | Get hash | malicious | Browse | • 95.140.230.192 |
| | ERP - US Stock Selection - 202109.xls | Get hash | malicious | Browse | • 95.140.230.128 |
| | UCH Hospital Tender Inquiry.exe | Get hash | malicious | Browse | • 178.79.242.128 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| ASN-CXA-ALL-CCI-22773-RDCUS | arm7-20211004-1530 | Get hash | malicious | Browse | • 209.34.217.143 |
| | yir8ieZzXL | Get hash | malicious | Browse | • 70.163.133.117 |
| | Zot0D0dD8J | Get hash | malicious | Browse | • 70.181.229.157 |
| | cu8KB5if2T | Get hash | malicious | Browse | • 68.96.149.188 |
| | 8qv45JJrGQ | Get hash | malicious | Browse | • 68.111.25.31 |
| | lessie.arm7 | Get hash | malicious | Browse | • 184.178.190.23 |
| | lessie.x86 | Get hash | malicious | Browse | • 68.102.97.252 |
| | 834V8Sq5HQ | Get hash | malicious | Browse | • 72.200.138.26 |
| | CdGi0KyPWX | Get hash | malicious | Browse | • 204.62.73.120 |
| | dLM8lB4AQ7 | Get hash | malicious | Browse | • 24.120.45.59 |
| | SN3tZLChOJ | Get hash | malicious | Browse | • 98.171.80.191 |
| | CDcUegnLSd | Get hash | malicious | Browse | • 68.101.118.225 |
| | sora.arm7 | Get hash | malicious | Browse | • 68.13.191.193 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | sora.x86 | Get hash | malicious | Browse | • 68.6.255.103 |
| | index_2021-09-30-12_54 | Get hash | malicious | Browse | • 68.7.243.91 |
| | Wns7odRLbP | Get hash | malicious | Browse | • 70.175.218.163 |
| | te2GttY5SP | Get hash | malicious | Browse | • 70.167.152.11 |
| | 6IT73F9Sr1 | Get hash | malicious | Browse | • 68.109.156.159 |
| | X3m77l2V5l | Get hash | malicious | Browse | • 184.181.23 6.242 |
| | arm | Get hash | malicious | Browse | • 68.101.117.79 |
| LDCOMNETFR | x86-20211004-1530 | Get hash | malicious | Browse | • 92.88.49.227 |
| | FX8w3rl5cw | Get hash | malicious | Browse | • 93.13.141.130 |
| | UpsxN0u4wi | Get hash | malicious | Browse | • 109.26.56.191 |
| | 5V5oGkJhwW | Get hash | malicious | Browse | • 109.2.184.120 |
| | Zot0D0dD8J | Get hash | malicious | Browse | • 92.91.122.200 |
| | nMftbNUfgt | Get hash | malicious | Browse | • 92.90.213.96 |
| | 8qv45JJrGQ | Get hash | malicious | Browse | • 93.10.100.217 |
| | 8kYSWVCyyy | Get hash | malicious | Browse | • 109.24.53.65 |
| | 0AQOcdTkg3 | Get hash | malicious | Browse | • 79.80.68.176 |
| | JE91d4cv34 | Get hash | malicious | Browse | • 62.39.174.188 |
| | e18hGJfKoy | Get hash | malicious | Browse | • 37.67.167.219 |
| | R3Y21HxKFx | Get hash | malicious | Browse | • 109.25.68.178 |
| | 02uKvQqAqD | Get hash | malicious | Browse | • 79.85.233.144 |
| | 834V8Sq5HQ | Get hash | malicious | Browse | • 37.65.116.217 |
| | 4uSa8tiph0 | Get hash | malicious | Browse | • 77.146.106.160 |
| | CdGi0KyPWX | Get hash | malicious | Browse | • 93.27.166.11 |
| | DcgPw20VOI.exe | Get hash | malicious | Browse | • 143.198.15.243 |
| | KkCBUSjS0h | Get hash | malicious | Browse | • 92.88.104.224 |
| | sora.arm | Get hash | malicious | Browse | • 79.81.225.29 |
| | Wns7odRLbP | Get hash | malicious | Browse | • 77.145.59.28 |

### JA3 Fingerprints

**No context**

### Dropped Files

**No context**

## Created / dropped Files

**No created / dropped files found**

## Static File Info

### General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 4.458919584976166 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | tcpmdmaus.exe |
| File size: | 280576 |
| MD5: | abe13ddc14525c4c35a85224689bfb27 |
| SHA1: | 01b8022edd4ef8e9ab20807c032b7ce2849b3df3 |
| SHA256: | 8524e558dded9665e69541b332d556e43c007d0d4001fe5355ac4816c22e7a21 |
| SHA512: | 1592bd7a07aff9f04f44ecbdc049daef083e943cd2e930a9bd40ab1f7fbab71ae23c8229a3857b8917c7fc93427827fc0b9a02db2cb5a4a0351fc914eecee834 |

## General

| | |
|---|---|
| SSDEEP: | 1536:y1dwtM1uD1drq12rh0PC4nRh87bEOYPyGy5oBu7WiKT:Y7uDDq8qHnRsbEjP/u7I |
| File Content Preview: | MZ.....@.....st.!.am.nL.7r....dern32.u....!..i...g!. .e!..$MZ.. mu.bThrL. un ....This pro W.....PE..L...`d.[.....@.....@..... |

## File Icon

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

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40100f |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE |
| DLL Characteristics: | TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x5B1E6460 [Mon Jun 11 12:00:32 2018 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 5 |
| OS Version Minor: | 0 |
| File Version Major: | 5 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 5 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 0b7b2a1ae1bd9f4631da141abed1aa7d |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x17898 | 0x17a00 | False | 0.0648044808201 | data | 0.983565645054 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x19000 | 0x46c | 0x600 | False | 0.238932291667 | data | 1.7374447372 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .bT | 0x1a000 | 0x16eb | 0x400 | False | 0.576171875 | data | 4.5070923188 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .idata | 0x1c000 | 0x59a | 0x600 | False | 0.257161458333 | data | 2.47810388592 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_READ |
| D | 0x1d000 | 0x127ec | 0x12800 | False | 0.308290223818 | data | 5.2061094126 | IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .crt0 | 0x30000 | 0xccbc | 0xce00 | False | 0.561343294903 | data | 5.66222181743 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| cji8 | 0x3d000 | 0x5dd3 | 0x5e00 | False | 0.00835272606383 | data | 4.06889527583 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x43000 | 0x5e4c | 0x6000 | False | 0.133138020833 | data | 3.29366479111 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .reloc | 0x49000 | 0x472 | 0x600 | False | 0.209635416667 | data | 1.61290752237 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

## Resources

## Imports

## Version Infos

## Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| Bulgarian | Bulgaria |  |
| Chinese | Taiwan |  |
| Czech | Czech Republic |  |
| Danish | Denmark |  |
| Greek | Greece |  |
| English | United States |  |
| Finnish | Finland |  |
| Hebrew | Israel |  |
| Hungarian | Hungary |  |
| Japanese | Japan |  |

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| Korean | North Korea |  |
| Korean | South Korea |  |
| Polish | Poland |  |
| Romanian | Romania |  |
| Russian | Russia |  |
| Croatian | Croatia |  |
| Slovak | Slovakia |  |
| Thai | Thailand |  |
| Turkish | Turkey |  |
| Slovenian | Slovenia |  |
| Vietnamese | Vietnam |  |
| Chinese | China |  |

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| Portuguese | Portugal |  |

# Network Behavior

## Network Port Distribution

## TCP Packets

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Oct 5, 2021 15:31:52.911623955 CEST | 8.8.8.8 | 192.168.2.3 | 0x11af | No error (0) | windowsupdate.s.llnwi.net | | 178.79.242.128 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- 77.157.40.119:443

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.3 | 49859 | 77.157.40.119 | 443 | C:\Windows\SysWOW64\sharedsls.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Oct 5, 2021 15:33:09.416189909 CEST | 8921 | OUT | POST / HTTP/1.1<br>User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)<br>Host: 77.157.40.119:443<br>Content-Length: 404<br>Connection: Keep-Alive<br>Cache-Control: no-cache<br>Data Raw: 94 2c 73 df ad 1a aa a2 e9 ad 40 ba 8d bb ba 87 51 2f 9b f3 3c c0 5d de 3e 13 14 42 f0 17 65 da c6 64 9a 9d e5 ae 62 71 10 d4 51 aa cd 34 1e 14 85 0d 2f 8c 64 a7 30 4e 71 11 54 3b 10 ee 2c 57 cb b4 d3 91 23 19 20 04 42 65 eb d3 ac ec 20 8f 34 d4 a4 e5 f4 60 b7 8c c8 e6 c2 c1 23 c5 4c 26 76 4c 09 d7 c7 0a 7a 8b 85 02 df a5 0b 05 2e a2 a5 48 64 e1 70 41 89 9f 86 2d d3 55 79 8f ae 2d 2a e5 24 b5 21 5e 57 46 f4 69 26 5c c5 10 28 bb 90 77 92 d0 dd ae 57 a1 49 a0 84 4b 9d 76 34 43 9c 0f 4c 9a 51 a4 fe 3a 4e 54 b0 3c 20 3f 2d 75 a9 e9 40 2d 59 87 16 e7 75 b3 c8 a4 60 9f 95 3f 70 09 6e cd fc e8 7b d6 47 88 70 19 b2 d6 55 22 30 cf 6b e6 7a a7 f3 b5 72 3e 3b 49 4f 3f 9b a1 77 5c aa ab 7e fb 0b c6 ca d1 39 f1 9d fa 93 80 2b 63 3a 28 a8 d6 7a 9f 7d 7d ea 64 68 2c db 4c 1e cb 5c f7 63 aa 16 c0 a5 1a 90 4a 7f c0 6b 6e a8 c8 92 5a 3c 7b ff 87 66 f8 e5 ae 05 6a 09 dc 4f 26 a3 17 67 57 c7 5f 16 b9 9d f6 21 9d 4c 1c 13 00 bc 2e f2 84 4d 0b 25 3d df 13 63 38 b0 3e 33 2c 88 db af 9f f2 e8 c3 de bc 59 37 38 d6 9f 57 ea b6 b5 04 fd 2e 8b 7d dd 1b c3 3f 26 27 a8 b5 77 e0 f6 d2 1f bf 03 ce 67 55 11 aa a7 a4 7c da ea df 9f fa 60 54 61 a8 e6 01 d5 49 6c 29 b3 d0 62 64 f4 b0 0d f3 5d 7d f5 10 34 bb 22 e6 db dd d8 35 15<br>Data Ascii: ,s@Q/<]>BedbqQ4/d0NqT;,W# Be 4`#L&vLz.HdpA-Uy-*$!^WFi&\(wWIKv4CLQ:NT< ?-u@-Yu`?pn{GpU"0k zr>;lO?w\~9+c:(z}}dh,L\cJknZ<{fjO&gW_!L.M%=c8>3,Y78W.}?&'wgU\|`TaIl)bd]}4"5 |

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: tcpmdmaus.exe PID: 400 Parent PID: 3640

### General

| | |
|---|---|
| Start time: | 15:31:06 |
| Start date: | 05/10/2021 |
| Path: | C:\Users\user\Desktop\tcpmdmaus.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\tcpmdmaus.exe' |
| Imagebase: | 0x1310000 |
| File size: | 280576 bytes |
| MD5 hash: | ABE13DDC14525C4C35A85224689BFB27 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.295437100.0000000000B71000.00000020.00000001.sdmp, Author: Joe Security<br>• Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.295437100.0000000000B71000.00000020.00000001.sdmp, Author: kevoreilly |
| Reputation: | low |

## Analysis Process: tcpmdmaus.exe PID: 6768 Parent PID: 400

### General

| | |
|---|---|
| Start time: | 15:31:07 |
| Start date: | 05/10/2021 |
| Path: | C:\Users\user\Desktop\tcpmdmaus.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\tcpmdmaus.exe |
| Imagebase: | 0x1310000 |
| File size: | 280576 bytes |
| MD5 hash: | ABE13DDC14525C4C35A85224689BFB27 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.322257965.0000000001251000.00000020.00000001.sdmp, Author: Joe Security<br>• Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.322257965.0000000001251000.00000020.00000001.sdmp, Author: kevoreilly |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Deleted

## Analysis Process: sharedsls.exe PID: 4752 Parent PID: 572

### General

| | |
|---|---|
| Start time: | 15:31:09 |
| Start date: | 05/10/2021 |
| Path: | C:\Windows\SysWOW64\sharedsls.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\sharedsls.exe |
| Imagebase: | 0x1310000 |
| File size: | 280576 bytes |
| MD5 hash: | ABE13DDC14525C4C35A85224689BFB27 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.321224638.0000000001461000.00000020.00000001.sdmp, Author: Joe Security<br>• Rule: Emotet, Description: Emotet Payload, Source: 00000002.00000002.321224638.0000000001461000.00000020.00000001.sdmp, Author: kevoreilly |
| Reputation: | low |

## Analysis Process: svchost.exe PID: 6696 Parent PID: 572

### General

| | |
|---|---|
| Start time: | 15:31:17 |
| Start date: | 05/10/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff70d6e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: sharedsls.exe PID: 5404 Parent PID: 4752

### General

| | |
|---|---|
| Start time: | 15:31:19 |
| Start date: | 05/10/2021 |
| Path: | C:\Windows\SysWOW64\sharedsls.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\sharedsls.exe |
| Imagebase: | 0x1310000 |
| File size: | 280576 bytes |
| MD5 hash: | ABE13DDC14525C4C35A85224689BFB27 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.557763672.0000000001451000.00000020.00000001.sdmp, Author: Joe Security<br>• Rule: Emotet, Description: Emotet Payload, Source: 00000007.00000002.557763672.0000000001451000.00000020.00000001.sdmp, Author: kevoreilly |
| Reputation: | low |

File Activities | Show Windows behavior

File Created

## Analysis Process: svchost.exe PID: 4140 Parent PID: 572

### General

| | |
|---|---|
| Start time: | 15:31:25 |
| Start date: | 05/10/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff70d6e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

File Activities | Show Windows behavior

## Analysis Process: svchost.exe PID: 7056 Parent PID: 572

### General

| | |
|---|---|
| Start time: | 15:31:33 |
| Start date: | 05/10/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff70d6e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

File Activities | Show Windows behavior

## Analysis Process: svchost.exe PID: 6868 Parent PID: 572

### General

| | |
|---|---|
| Start time: | 15:31:44 |
| Start date: | 05/10/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff70d6e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |

| | |
|---|---|
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

# Disassembly

## Code Analysis