JoeSandbox Cloud BASIC

**ID:** 797228
**Sample Name:**
MASTER_Malware_Lab1.exe
**Cookbook:** default.jbs
**Time:** 18:01:12
**Date:** 02/02/2023
**Version:** 36.0.0 Rainbow Opal

# Table of Contents


Table of Contents 2
Windows Analysis Report MASTER_Malware_Lab1.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 6
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Persistence and Installation Behavior 6
Malware Analysis System Evasion 6
Lowering of HIPS / PFW / Operating System Security Settings 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 11
General Information 11
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\ProgramData\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml (copy) 12
C:\ProgramData\USOPrivate\UpdateStore\updatestoretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml 12
C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.001.etl (copy) 13
C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration_Temp.1.etl 13
C:\Users\Public\Public\Screens\screenshot.bmp 13
C:\Users\Public\Public\Screens\screenshot000.bmp 14
C:\Users\Public\Public\Screens\screenshot001.bmp 14
C:\Users\Public\Public\Screens\screenshot002.bmp 14
C:\Users\Public\Public\Screens\screenshot003.bmp 15
C:\Users\Public\Public\Screens\screenshot004.bmp 15
C:\Users\Public\Public\Screens\screenshot005.bmp 15
C:\Users\Public\Public\Screens\screenshot006.bmp 15
C:\Users\Public\Public\Screens\screenshot007.bmp 16
C:\Users\Public\Public\Screens\screenshot008.bmp 16
C:\Users\Public\Public\Screens\screenshot009.bmp 16
C:\Users\Public\Public\Screens\screenshot010.bmp 17
C:\Users\Public\Public\Screens\screenshot011.bmp 17
C:\Users\Public\Public\Screens\screenshot012.bmp 17
C:\Users\Public\Public\Screens\screenshot013.bmp 18
C:\Users\Public\Public\Screens\screenshot014.bmp 18
C:\Users\Public\Public\Screens\screenshot015.bmp 18
C:\Users\Public\Public\Screens\screenshot016.bmp 18
C:\Users\Public\Public\Screens\screenshot017.bmp 19
C:\Users\Public\Public\Screens\screenshot018.bmp 19
C:\Users\Public\Public\Screens\screenshot019.bmp 19
C:\Users\Public\Public\Screens\screenshot020.bmp 20
C:\Users\Public\Public\Screens\screenshot021.bmp 20
C:\Users\Public\Public\Screens\screenshot022.bmp 20

C:\Users\Public\Public\Screens\screenshot023.bmp 21
C:\Users\Public\Public\Screens\screenshot024.bmp 21
C:\Users\Public\Public\Screens\screenshot025.bmp 21
C:\Users\Public\Public\Screens\screenshot026.bmp 21
C:\Users\Public\Public\Screens\screenshot027.bmp 22
C:\Users\Public\Public\Screens\screenshot028.bmp 22
C:\Users\Public\Public\Screens\screenshot029.bmp 22
C:\Users\Public\Public\Screens\screenshot030.bmp 23
C:\Users\Public\Public\Screens\screenshot031.bmp 23
C:\Users\Public\Public\Screens\screenshot032.bmp 23
C:\Users\Public\Public\Screens\screenshot033.bmp 24
C:\Users\Public\Public\Screens\screenshot034.bmp 24
C:\Users\Public\Public\Screens\screenshot035.bmp 24
C:\Users\Public\Public\Screens\screenshot036.bmp 24
C:\Users\Public\Public\Screens\screenshot037.bmp 25
C:\Users\Public\Public\Screens\screenshot038.bmp 25
C:\Users\Public\Public\Screens\screenshot039.bmp 25
C:\Users\Public\Public\Screens\screenshot040.bmp 26
C:\Users\Public\Public\Screens\screenshot041.bmp 26
C:\Users\Public\Public\Screens\screenshot042.bmp 26
C:\Users\Public\Public\Screens\screenshot043.bmp 27
C:\Users\Public\Public\Screens\screenshot044.bmp 27
C:\Users\Public\Public\Screens\screenshot045.bmp 27
C:\Users\Public\Public\Screens\screenshot046.bmp 28
C:\Users\Public\Public\Screens\screenshot047.bmp 28
C:\Users\Public\Public\Screens\screenshot048.bmp 28
C:\Users\Public\Public\Screens\screenshot049.bmp 28
C:\Users\Public\Public\Screens\screenshot050.bmp 29
C:\Users\Public\Public\Screens\screenshot051.bmp 29
C:\Users\Public\Public\Screens\screenshot052.bmp 29
C:\Users\Public\Public\Screens\screenshot053.bmp 30
C:\Users\Public\Public\Screens\screenshot054.bmp 30
C:\Users\Public\Public\Screens\screenshot055.bmp 30
C:\Users\Public\Public\Screens\screenshot056.bmp 31
C:\Users\Public\Public\Screens\screenshot057.bmp 31
C:\Users\Public\Public\Screens\screenshot058.bmp 31
C:\Users\Public\Public\Screens\screenshot059.bmp 31
C:\Users\Public\Public\Screens\screenshot060.bmp 32
C:\Users\Public\Public\Screens\screenshot061.bmp 32
C:\Users\Public\Public\Screens\screenshot062.bmp 32
C:\Users\Public\Public\Screens\screenshot063.bmp 33
C:\Users\Public\Public\Screens\screenshot064.bmp 33
C:\Users\Public\Public\Screens\screenshot065.bmp 33
C:\Users\Public\Public\Screens\screenshot066.bmp 34
C:\Users\Public\Public\Screens\screenshot067.bmp 34
C:\Users\Public\Public\Screens\screenshot068.bmp 34
C:\Users\Public\Public\keylogs.txt 35
C:\Users\Public\Public\svchost.exe 35
C:\Users\Public\Public\svchost.exe:Zone.Identifier 35
C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl 35
C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl 36
C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl 36
C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001 (copy) 36
C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy) 37
C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001 (copy) 37
C:\Windows\Logs\waasmedic\waasmedic.20230203_020233_050.etl 37
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log 38
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20230203_020225_210.etl 38
\Device\ConDrv 38
Static File Info 39
General 39
File Icon 39
Static PE Info 39
General 39
Entrypoint Preview 39
Rich Headers 41
Data Directories 41
Sections 41
Resources 41
Imports 41
Possible Origin 42
Network Behavior 42
Statistics 43
Behavior 43
System Behavior 43
Analysis Process: MASTER_Malware_Lab1.exePID: 2560, Parent PID: 3452 43
General 43
File Activities 43

Analysis Process: conhost.exePID: 3076, Parent PID: 2560 43
General 43
Analysis Process: cmd.exePID: 5264, Parent PID: 2560 44
General 44
File Activities 44
Analysis Process: reg.exePID: 5256, Parent PID: 5264 44
General 44
File Activities 44
Registry Activities 44
Analysis Process: svchost.exePID: 628, Parent PID: 3452 44
General 44
File Activities 45
File Created 45
File Written 45
Analysis Process: conhost.exePID: 4788, Parent PID: 628 84
General 84
Analysis Process: cmd.exePID: 5500, Parent PID: 628 84
General 84
Analysis Process: reg.exePID: 5964, Parent PID: 5500 85
General 85
File Activities 85
Analysis Process: svchost.exePID: 732, Parent PID: 580 85
General 85
Analysis Process: svchost.exePID: 3512, Parent PID: 580 85
General 85
File Activities 86
Analysis Process: svchost.exePID: 2792, Parent PID: 580 86
General 86
File Activities 86
Analysis Process: svchost.exePID: 6140, Parent PID: 580 86
General 86
Registry Activities 86
Analysis Process: svchost.exePID: 5240, Parent PID: 580 87
General 87
Analysis Process: svchost.exePID: 4684, Parent PID: 3452 87
General 87
File Activities 87
File Created 87
File Written 87
Analysis Process: conhost.exePID: 4340, Parent PID: 4684 125
General 125
Analysis Process: cmd.exePID: 2384, Parent PID: 4684 125
General 125
Analysis Process: reg.exePID: 5444, Parent PID: 2384 125
General 125
File Activities 125
Analysis Process: svchost.exePID: 848, Parent PID: 580 125
General 126
File Activities 126
Registry Activities 126
Analysis Process: svchost.exePID: 6128, Parent PID: 580 126
General 126
Registry Activities 126
Analysis Process: svchost.exePID: 3020, Parent PID: 580 127
General 127
Analysis Process: MpCmdRun.exePID: 4600, Parent PID: 6128 127
General 127
File Activities 127
File Written 127
Analysis Process: conhost.exePID: 3012, Parent PID: 4600 129
General 129
Disassembly 129

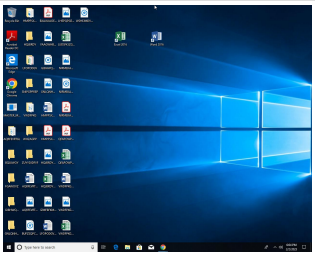
# Windows Analysis Report

## MASTER_Malware_Lab1.exe

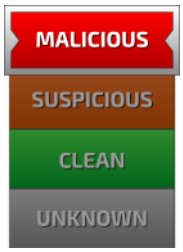
## Overview

### General Information

| | |
|---|---|
| Sample Name: | MASTER_Malware_Lab1.exe |
| Analysis ID: | 797228 |
| MD5: | 07b92f1473b82.. |
| SHA1: | 2d5fa5ca204e2.. |
| SHA256: | ad9427b659a7... |
| Infos: | |



### Detection

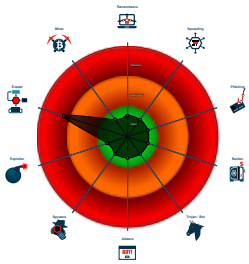



| | |
|---|---|
| Score: | 88 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Antivirus / Scanner detection for sub...
- Multi AV Scanner detection for subm...
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop...
- Query firmware table information (lik...
- Uses cmd line tools excessively to ...
- Changes security center settings (n...
- Drops PE files with benign system n...
- Uses 32bit PE files
- Found a high number of Window / U...
- AV process strings found (often use...
- Drops PE files

### Classification



## Process Tree

- **System is w10x64**
- MASTER_Malware_Lab1.exe (PID: 2560 cmdline: C:\Users\user\Desktop\MASTER_Malware_Lab1.exe MD5: 07B92F1473B82789F71A58EE8999C631)
  - conhost.exe (PID: 3076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5264 cmdline: C:\Windows\system32\cmd.exe /c REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - reg.exe (PID: 5256 cmdline: REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe MD5: CEE2A7E57DF2A159A065A34913A055C2)
- svchost.exe (PID: 628 cmdline: "C:\Users\Public\Public\svchost.exe" MD5: 07B92F1473B82789F71A58EE8999C631)
  - conhost.exe (PID: 4788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5500 cmdline: C:\Windows\system32\cmd.exe /c REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - reg.exe (PID: 5964 cmdline: REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe MD5: CEE2A7E57DF2A159A065A34913A055C2)
- svchost.exe (PID: 732 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3512 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2792 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6140 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5240 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4684 cmdline: "C:\Users\Public\Public\svchost.exe" MD5: 07B92F1473B82789F71A58EE8999C631)
  - conhost.exe (PID: 4340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 2384 cmdline: C:\Windows\system32\cmd.exe /c REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - reg.exe (PID: 5444 cmdline: REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe MD5: CEE2A7E57DF2A159A065A34913A055C2)
- svchost.exe (PID: 848 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6128 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4600 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 3012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 3020 cmdline: c:\windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

## Malware Configuration

No configs have been found

## Yara Signatures

No yara matches

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

### Persistence and Installation Behavior

Uses cmd line tools excessively to alter registry or file data

Drops PE files with benign system names

### Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

### Lowering of HIPS / PFW / Operating System Security Settings

Changes security center settings (notifications, updates, antivirus, firewall)

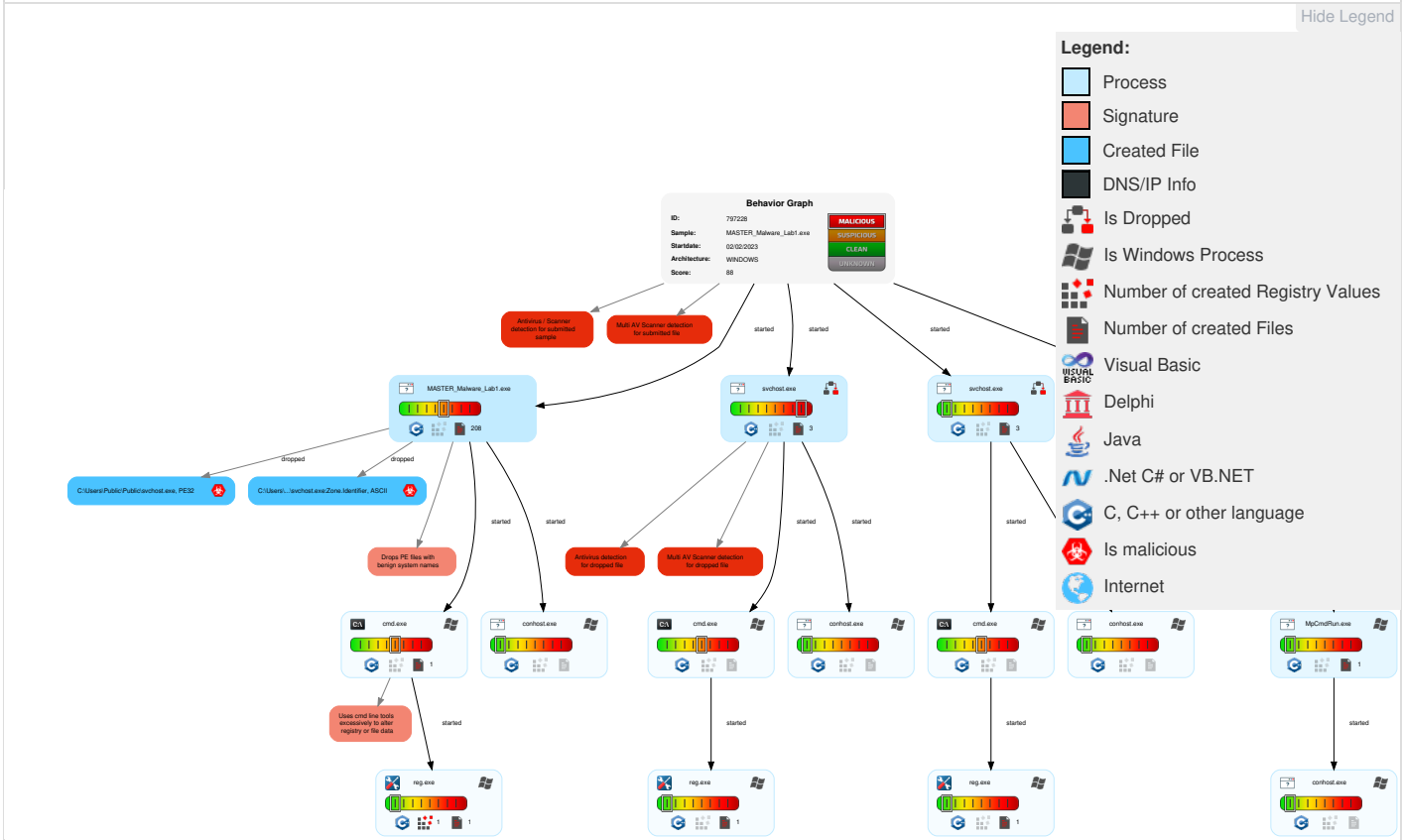
## Mitre Att&ck Matrix

| 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 Windows Management Instrumentation | 1 DLL Side-Loading | 1 1 Process Injection | 1 1 Masquerading | OS Credential Dumping | 2 3 1 Security Software Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Data Obfuscation | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |

Copyright Joe Security LLC 2023

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Default Accounts | 1 Command and Scripting Interpreter | 1 Registry Run Keys / Startup Folder | 1 DLL Side-Loading | 1 Disable or Modify Tools | LSASS Memory | 1 3 1 Virtualization/Sandbox Evasion | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | 1 Registry Run Keys / Startup Folder | 1 Modify Registry | Security Account Manager | 1 Application Window 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 3 1 Virtualization/Sandbox Evasion | NTDS | 1 1 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 1 Process Injection | 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 DLL Side-Loading | 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 |

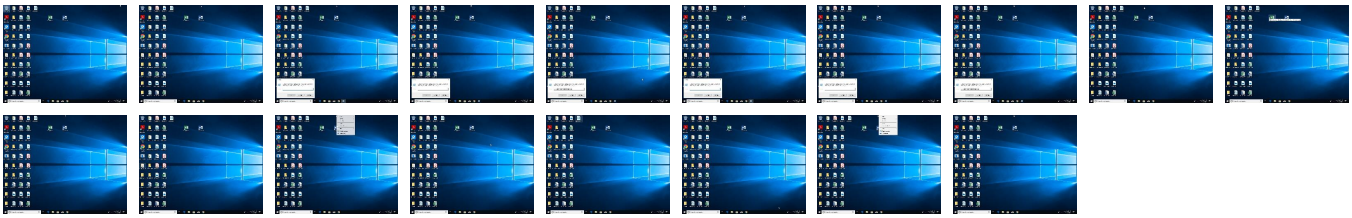
## Behavior Graph




## 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 |
|---|---|---|---|---|
| MASTER_Malware_Lab1.exe | 49% | ReversingLabs | Win32.Trojan.Malex | |
| MASTER_Malware_Lab1.exe | 56% | Virustotal | | Browse |
| MASTER_Malware_Lab1.exe | 100% | Avira | TR/Malex.pfzxh | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\Public\Public\svchost.exe | 100% | Avira | TR/Malex.pfzxh | |
| C:\Users\Public\Public\svchost.exe | 49% | ReversingLabs | Win32.Trojan.Malex | |

Copyright Joe Security LLC 2023

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\Public\Public\svchost.exe | 56% | Virustotal | | Browse |

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://%s.xboxlive.com | 0% | URL Reputation | safe | |
| http://https://dynamic.t | 0% | URL Reputation | safe | |
| http://https://%s.dnet.xboxlive.com | 0% | URL Reputation | safe | |
| http://https://%s.dnet.xboxlive.com | 0% | URL Reputation | safe | |

## Domains and IPs

### Contacted Domains

No contacted domains info

### URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx | svchost.exe, 0000000C.00000003.319329371.000001E0A9061000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r= | svchost.exe, 0000000C.00000003.322748056.000001E0A9056000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.ditu.live.com/REST/v1/Routes/ | svchost.exe, 0000000C.00000002.324142629.000001E0A903D000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.virtualearth.net/REST/v1/Routes/Driving | svchost.exe, 0000000C.00000003.319329371.000001E0A9061000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx | svchost.exe, 0000000C.00000002.324142629.000001E0A903D000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/ | svchost.exe, 0000000C.00000003.322303385.000001E0A905A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.324177574.000001E0A905C000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://t0.tiles.ditu.live.com/tiles/gen | svchost.exe, 0000000C.00000002.324160552.000001E0A904E000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.virtualearth.net/REST/v1/Routes/ | svchost.exe, 0000000C.00000002.324142629.000001E0A903D000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r= | svchost.exe, 0000000C.00000003.322712881.000001E0A9040000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.virtualearth.net/REST/v1/Routes/Walking | svchost.exe, 0000000C.00000003.319329371.000001E0A9061000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log? | svchost.exe, 0000000C.00000003.322303385.000001E0A905A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.322712881.000001E0A9040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.324177574.000001E0A905C000.00000004.00000020.00020000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r= | svchost.exe, 0000000C.00000002.323991243.000001E0A9027000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.324142629.000001E0A903D000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n= | svchost.exe, 0000000C.00000003.322712881.000001E0A9040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.324149332.000001E0A9041000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://%s.xboxlive.com | svchost.exe, 0000000A.00000002.511910088.000001D7B123E000.00000004.00000020.00020000.00000000.sdmp | false | • URL Reputation: safe | low |
| http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v= | svchost.exe, 0000000C.00000002.324160552.000001E0A904E000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.virtualearth.net/REST/v1/Locations | svchost.exe, 0000000C.00000003.319329371.000001E0A9061000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v= | svchost.exe, 0000000C.00000003.293771438.000001E0A9032000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.virtualearth.net/mapcontrol/logging.ashx | svchost.exe, 0000000C.00000003.319329371.000001E0A9061000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.ditu.live.com/mapcontrol/logging.ashx | svchost.exe, 0000000C.00000003.319329371.000001E0A9061000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/ | svchost.exe, 0000000C.00000003.322303385.000001E0A905A000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r= | svchost.exe, 0000000C.00000003.322712881.000001E0A9040000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r= | svchost.exe, 0000000C.00000002.324177574.000001E0A905C000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/ | svchost.exe, 0000000C.00000003.322303385.000001E0A905A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.324177574.000001E0A905C000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/ | svchost.exe, 0000000C.00000003.322712881.000001E0A9040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.324149332.000001E0A9041000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dynamic.t | svchost.exe, 0000000C.00000003.318005078.000001E0A9064000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.324149332.000001E0A9041000.00000004.00000020.00020000.00000000.sdmp | false | • URL Reputation: safe | unknown |
| http://https://dev.virtualearth.net/REST/v1/Routes/Transit | svchost.exe, 0000000C.00000003.319329371.000001E0A9061000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen | svchost.exe, 0000000C.00000003.322712881.000001E0A9040000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r= | svchost.exe, 0000000C.00000003.322303385.000001E0A905A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.324177574.000001E0A905C000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://activity.windows.com | svchost.exe, 0000000A.00000002.511910088.000001D7B123E000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://www.bingmapsportal.com | svchost.exe, 0000000C.00000002.323936739.000001E0A9013000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dev.ditu.live.com/REST/v1/Locations | svchost.exe, 0000000C.00000003.319329371.000001E0A9061000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/ | svchost.exe, 0000000C.00000002.324142629.000001E0A903D000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://%s.dnet.xboxlive.com | svchost.exe, 0000000A.00000002.511910088.000001D7B123E000.00000004.00000020.00020000.00000000.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe | low |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/ | svchost.exe, 0000000C.00000003.322303385.000001E0A905A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.324177574.000001E0A905C000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r= | svchost.exe, 0000000C.00000003.322303385.000001E0A905A000.00000004.00000020.00020000.00000000.sdmp | false | | high |

### World Map of Contacted IPs

No contacted IP infos

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 36.0.0 Rainbow Opal |
| Analysis ID: | 797228 |
| Start date and time: | 2023-02-02 18:01:12 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 8m 3s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 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 |
| Sample file name: | MASTER_Malware_Lab1.exe |
| Detection: | MAL |
| Classification: | mal88.evad.winEXE@29/89@0/0 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .exe |

### Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.

## Simulations

### Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 18:02:06 | API Interceptor | 202x Sleep call for process: MASTER_Malware_Lab1.exe modified |
| 18:02:09 | Autostart | Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Firewall C:\Users\Public\Public\svchost.exe |

| Time | Type | Description |
|---|---|---|
| 18:02:17 | Autostart | Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Firewall C:\Users\Public\Public\svchost.exe |
| 18:02:24 | API Interceptor | 135x Sleep call for process: svchost.exe modified |
| 18:03:35 | API Interceptor | 1x Sleep call for process: MpCmdRun.exe modified |

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

### C:\ProgramData\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml (copy)

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines (2494), with no line terminators |
| Category: | dropped |
| Size (bytes): | 2494 |
| Entropy (8bit): | 5.230229221505206 |
| Encrypted: | false |
| SSDEEP: | 48:cAn/TLtfGgzmQLeUp/B8H6rMSkC9+TykISbs:pTLtf9zmQ7rVkgqSbs |
| MD5: | 6E0F869D3D3BD21E43186115B0CD74DF |
| SHA1: | 9BA7DB68CDAF7F6358A454EB9296E83E9CB9CB6C |
| SHA-256: | 0471ED17C647021B27987587515E43530391228A8F15D17DDED47472F914BF5B |
| SHA-512: | E8F7A2ED0A28DFB9A7B32246A7A4A95D6E438FE5420C0F11C047633EA5E9AEAAAD2C1004D45D731066A54E2680567AF932850D5480654BA8D4BFE85AFB1BDAF9 |
| Malicious: | false |
| Preview: | <?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService dataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataType="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399969272148706</FirstScanAttemptTime><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399969272304939</LastMeteredScanTime><LastScanAttemptTime dataType="21">132399969272148706</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType="21">133051593686244000</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu |

### C:\ProgramData\USOPrivate\UpdateStore\updatestoretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines (2494), with no line terminators |
| Category: | dropped |
| Size (bytes): | 2494 |
| Entropy (8bit): | 5.230229221505206 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 48:cAn/TLtfGgzmQLeUp/B8H6rMSkC9+TyklSbs:pTLtf9zmQ7rVkgqSbs |
| MD5: | 6E0F869D3D3BD21E43186115B0CD74DF |
| SHA1: | 9BA7DB68CDAF7F6358A454EB9296E83E9CB9CB6C |
| SHA-256: | 0471ED17C647021B27987587515E43530391228A8F15D17DDED47472F914BF5B |
| SHA-512: | E8F7A2ED0A28DFB9A7B32246A7A4A95D6E438FE5420C0F11C047633EA5E9AEAAAD2C1004D45D731066A54E2680567AF932850D5480654BA8D4BFE85AFB1BDAF9 |
| Malicious: | false |
| Preview: | <?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService dataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataType="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399969272148706</FirstScanAttemptTime><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399969272304939</LastMeteredScanTime><LastScanAttemptTime dataType="21">132399969272148706</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType="21">133051593686244000</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu |

### C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.001.etl (copy)

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8192 |
| Entropy (8bit): | 3.7553248052032124 |
| Encrypted: | false |
| SSDEEP: | 96:7i8iv/iZxgZNnA8Z6uQZ2Z5k907HUuZbVZ+ZgEZwZeA3HZMTDZLpQ:7i8iv/c8NndOAnTob6d5MBLpQ |
| MD5: | 6A5290D199C60BA00B831AF43CE84139 |
| SHA1: | 89C34056CF9631DB000E108D81C16181E2493C33 |
| SHA-256: | F9BA0E11255941ACB9FDF04CBC0A4AE73F7CB021EAE50275502C11A5F78E6DC7 |
| SHA-512: | 3AB7066BFFA061988BF8712A96B0D2B5827D62DB0DC02EFBBBCCE39A20DCC5741B2978DAD06097629614F7DB9267FE56D698BF7593E6A5356E02BE9EC57ECD82 |
| Malicious: | false |
| Preview: | .....P...p.G.s7.....B.....Zb..K....(.....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....r..... .....p.G.s7.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U.S.O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P.....P...p.G.s7..... |

### C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration_Temp.1.etl

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8192 |
| Entropy (8bit): | 3.7553248052032124 |
| Encrypted: | false |
| SSDEEP: | 96:7i8iv/iZxgZNnA8Z6uQZ2Z5k907HUuZbVZ+ZgEZwZeA3HZMTDZLpQ:7i8iv/c8NndOAnTob6d5MBLpQ |
| MD5: | 6A5290D199C60BA00B831AF43CE84139 |
| SHA1: | 89C34056CF9631DB000E108D81C16181E2493C33 |
| SHA-256: | F9BA0E11255941ACB9FDF04CBC0A4AE73F7CB021EAE50275502C11A5F78E6DC7 |
| SHA-512: | 3AB7066BFFA061988BF8712A96B0D2B5827D62DB0DC02EFBBBCCE39A20DCC5741B2978DAD06097629614F7DB9267FE56D698BF7593E6A5356E02BE9EC57ECD82 |
| Malicious: | false |
| Preview: | .....P...p.G.s7.....B.....Zb..K....(.....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....r..... .....p.G.s7.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U.S.O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P.....P...p.G.s7..... |

### C:\Users\Public\Public\Screens\screenshot.bmp

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.221117558239095 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |

| | |
|---|---|
| MD5: | 86558E92FA584C81D56C2AA48FD775F7 |
| SHA1: | C68E99459D355F0C4EE8BB134BEAFB836D3EFE16 |
| SHA-256: | 35B061B7C71C47B61BD5C1A045D1E53A183054D7EDFD135F5B00F61C3D792AFC |
| SHA-512: | 1C326316542811DEF84254E6DDCAB78F68D1E4C03FDC10379613EABCFDBEB9909872F0DFEB09D4076F34BF6FF829C5C20D3CD3C64C1D4D3FD3C642B0E7210DE |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot000.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot001.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot002.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |

| | |
|---|---|
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot003.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot004.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot005.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot006.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

### C:\Users\Public\Public\Screens\screenshot007.bmp

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

### C:\Users\Public\Public\Screens\screenshot008.bmp

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

### C:\Users\Public\Public\Screens\screenshot009.bmp

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |

| | |
|---|---|
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot010.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot011.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot012.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot013.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217768203369236 |
| Encrypted: | false |
| SSDEEP: | 98304:gLxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:9YG90dhIJ |
| MD5: | A3EA2E73FE3F86F3EA834097A969E78B |
| SHA1: | 9B5F2E01D29615AC1CFCD88935F2E05EBE036FAD |
| SHA-256: | A648A1000DB157793D1AE248DEDE6A307414F7444D93FDB07C142D7AF3F3D687 |
| SHA-512: | AE55955C3DA15E113F17F77ADF7B589A917BC888CDAA77279E86789741EA7DD90BDF0E06C475E9DC09939E7A53434348F07B95F5AD62221F7A91964C4D3822C |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot014.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.228098935069598 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | 4A6487EB853A62BA13ED907E17D6C38C |
| SHA1: | 60DE98B9F3FD0F39A06B6B42C0C11DF45A11080E |
| SHA-256: | 4EFBA6FB63E965F3B7D624DCE2CE61098B2D1CC6B64CFA39EBFE892D5113A1C7 |
| SHA-512: | A1828FE42479608F6FA461157405AEE939FB328C181C2B1603015025D3EA69111D8147C2D65809CF38727F73B7FC4908ED8EBD5B9D2253458C79F4A93316A555 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot015.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot016.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot017.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot018.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot019.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAI6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |

| | |
|---|---|
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot020.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot021.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot022.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot023.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot024.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot025.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | 98304:9LxIeXAl6vKgK4qkVfSIrLfPLxWkh4+HxYNtxYRC++e3nuO2Buvkb5yJN6mi5Jl5:wYG90dhIJ |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot026.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |

| | |
|---|---|
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot027.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot028.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot029.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.221102234090809 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 04C82F2596FBAA18E6A4E0CB6FCCD75D |

| | |
|---|---|
| SHA1: | A9DDCE0215BE5FE391D1DB791ADE9F1B910809F2 |
| SHA-256: | B0209ED881AEF9DD3CD3BA35A425BF30F302FF5ACAE5E754AA02ACC45F944658 |
| SHA-512: | 5D4B71CA610985649D868EFEB466C2EF58C16F0C023EC2E311E60E7C070C7B8A734C4C7C6D9F532B2E89CF18D3658CF7318EED6E1B8741D7F19C1C14E112D8 3 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot030.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE93 7 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot031.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.221447740148902 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | AB7EB8BB77800E29B01132EAB40576C0 |
| SHA1: | FA67BEB4B07073AC9E63022C20B5D7FC83DECFCF |
| SHA-256: | CC4A914453FC65478A05DD4E73A950CD84C335B3BF44441A07ADDE7BEFB19257 |
| SHA-512: | D320E6125B9F57DE14FEBCC31E241E620CCC3BBA8C12670C2C23E592F0607E9119C39F6ED2A4A081410298825345F1E998FCF0B682405F75F8E54007D2C4C82 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot032.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE93 7 |
| Malicious: | false |

| | |
|---|---|
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot033.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot034.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot035.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot036.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot037.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot038.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot039.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot040.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot041.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot042.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |

| | |
|---|---|
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot043.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot044.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot045.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot046.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot047.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot048.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

| C:\Users\Public\Public\Screens\screenshot049.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |

| | |
|---|---|
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot050.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.221408679682695 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | C0C74D0B84CBEA80CFB335CB2CA8C437 |
| SHA1: | E33B7A642FFE55BF10DCA5737328A2A901F4AC14 |
| SHA-256: | 08F9ECDD888E6432AA3BF57E463EFBC4F70C73687B15C1C412973516D6633C19 |
| SHA-512: | 4F0C24D05E0941B409C327EF72C42C7DDEBFF8208E50E9216DF8DB84056B69D3E56BF550B29A734D7D9FE013EA67B8694F279553C03CFA4DF29D1B62CB11554B |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot051.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot052.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |

| | |
|---|---|
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot053.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot054.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot055.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |

| | |
|---|---|
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot056.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot057.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot058.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769400106787 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | DB29ED5D33E174A6A6870FCBCC848520 |
| SHA1: | 20C24733DF8B5BB8CBA28000C71387407830A883 |
| SHA-256: | 877ED0E32D70B227567AB92D89E7580EC7096B45E550DC8E87D85CC2A3C23954 |
| SHA-512: | 6779A6454EC06DAAEF20FD14882BCA34F2770A9AEC4E89C6820549B17421A8D734B88B957CEDA51DAB3E4A9C16775D6C8C798051034AEF89826ADC670DBE937 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot059.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.220773371957926 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | C8B78E8DBD203579F4FE4D9310536F1F |
| SHA1: | 9FF6E96193D25033442E19A45908FE8C9A97597F |
| SHA-256: | D7276DA57FFF0338E1B226B344DE86FEC5F01F109E589B2314663988308558B9 |
| SHA-512: | 31B777C42E4CF8F4EEA03CF6A92A57E0FAA200DDA9B8F7D8CC53E82063FBD9F9E3DFD109320DAA6444161ECB3B8AD7E1B08F28927A7577C9230552C7B6030E 8D |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot060.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.2296226339111485 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | C2BB83CAB978E593AF7480086AE4421B |
| SHA1: | 0585E924CF407AAB0AEBF3430DE273895E16FD87 |
| SHA-256: | 458909BC79473DBD8D5B81701931F0A4556E1E6FFF19E0E9207B0E06A23EFA2D |
| SHA-512: | C44EFA25EB56464A724DE181AC0233D09B8C7BDA90A13ED2769F13904B67826CD116600D499D2E786664A073C7B76D2B57CF34EE9748CE1D5C3F2D2F960E13E 4 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot061.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.225921621697788 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F8172BAAB31572E2B421F7F303386823 |
| SHA1: | 303827B4D73C3D3289AD2EB0FC7031EADD34BE05 |
| SHA-256: | ECE3336CAF6F24135814453A6568E25D7FC58D691F1CDA460961DF60C314B1D7 |
| SHA-512: | 29EAE73D685BB02A0A667D19FDD510B366E46AF28F83102BC357C6B7B0834AC5561DCCA8235BB8181F687ACB274DF00FBBAD03D010571C9F8FC0141F523F6D 7 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot062.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769908125988 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 473EEAD42BB2AC00D0AED2AB8C195797 |
| SHA1: | FD3CA65702498290074B5DEA60EC33181B2B4F12 |
| SHA-256: | BF8A321C1C34BF4E0CE3A14C866C94C63BB60AFECC38D975293F6A544D50FFD8 |
| SHA-512: | 1B14D292CBA3328FF56BAE803203F7343D8E9A197957110A233639DBCC2BBA30D00B716269A81D38DBB9E4355A57DD07A0C8D2498BDA4DF0806D0E9767530D2 8 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot063.bmp**

| | |
|---|---|
| Process: | C:\Users\Public\Public\svchost.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769908125988 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 473EEAD42BB2AC00D0AED2AB8C195797 |
| SHA1: | FD3CA65702498290074B5DEA60EC33181B2B4F12 |
| SHA-256: | BF8A321C1C34BF4E0CE3A14C866C94C63BB60AFECC38D975293F6A544D50FFD8 |
| SHA-512: | 1B14D292CBA3328FF56BAE803203F7343D8E9A197957110A233639DBCC2BBA30D00B716269A81D38DBB9E4355A57DD07A0C8D2498BDA4DF0806D0E9767530D2 8 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot064.bmp**

| | |
|---|---|
| Process: | C:\Users\Public\Public\svchost.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.221408568096128 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 414D0843A86BFFF5D40378380F20D565 |
| SHA1: | DF2A46BA550AEA2A7F78657BD095DFD8E64CA37D |
| SHA-256: | 0512233C8018FB1189CEBFD7A5FE4CA6761105565E69F33DCF4D8DDEA2EDBC11 |
| SHA-512: | C07711666A49921317E51E01809CA0C983DBBC7630CE344B53EEA19B5051C2F23F27C8EF74A38372040FB2575E56E5E929F3442B3C90F6EDFB089EBC053D9D9 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot065.bmp**

| | |
|---|---|
| Process: | C:\Users\Public\Public\svchost.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | modified |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769908125988 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 473EEAD42BB2AC00D0AED2AB8C195797 |
| SHA1: | FD3CA65702498290074B5DEA60EC33181B2B4F12 |
| SHA-256: | BF8A321C1C34BF4E0CE3A14C866C94C63BB60AFECC38D975293F6A544D50FFD8 |

| | |
|---|---|
| SHA-512: | 1B14D292CBA3328FF56BAE803203F7343D8E9A197957110A233639DBCC2BBA30D00B716269A81D38DBB9E4355A57DD07A0C8D2498BDA4DF0806D0E9767530D2 8 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot066.bmp**

| | |
|---|---|
| Process: | C:\Users\Public\Public\svchost.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769908125988 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 473EEAD42BB2AC00D0AED2AB8C195797 |
| SHA1: | FD3CA65702498290074B5DEA60EC33181B2B4F12 |
| SHA-256: | BF8A321C1C34BF4E0CE3A14C866C94C63BB60AFECC38D975293F6A544D50FFD8 |
| SHA-512: | 1B14D292CBA3328FF56BAE803203F7343D8E9A197957110A233639DBCC2BBA30D00B716269A81D38DBB9E4355A57DD07A0C8D2498BDA4DF0806D0E9767530D2 8 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot067.bmp**

| | |
|---|---|
| Process: | C:\Users\Public\Public\svchost.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | dropped |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.221408568096128 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 414D0843A86BFFF5D40378380F20D565 |
| SHA1: | DF2A46BA550AEA2A7F78657BD095DFD8E64CA37D |
| SHA-256: | 0512233C8018FB1189CEBFD7A5FE4CA6761105565E69F33DCF4D8DDEA2EDBC11 |
| SHA-512: | C07711666A49921317E51E01809CA0C983DBBC7630CE344B53EEA19B5051C2F23F27C8EF74A38372040FB2575E56E5E929F3442B3C90F6EDFB089EBC053D9D9 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

**C:\Users\Public\Public\Screens\screenshot068.bmp**

| | |
|---|---|
| Process: | C:\Users\Public\Public\svchost.exe |
| File Type: | PC bitmap, Windows 3.x format, 1920 x 1080 x 32, 3 compression, image size 8294400, cbSize 8294466, bits offset 66 |
| Category: | modified |
| Size (bytes): | 8294466 |
| Entropy (8bit): | 4.217769908125988 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 473EEAD42BB2AC00D0AED2AB8C195797 |
| SHA1: | FD3CA65702498290074B5DEA60EC33181B2B4F12 |
| SHA-256: | BF8A321C1C34BF4E0CE3A14C866C94C63BB60AFECC38D975293F6A544D50FFD8 |
| SHA-512: | 1B14D292CBA3328FF56BAE803203F7343D8E9A197957110A233639DBCC2BBA30D00B716269A81D38DBB9E4355A57DD07A0C8D2498BDA4DF0806D0E9767530D2 8 |
| Malicious: | false |
| Preview: | BMB.~.....B...(.....8..... .....~..... |

### C:\Users\Public\Public\keylogs.txt

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | ASCII text, with very long lines (637), with no line terminators |
| Category: | dropped |
| Size (bytes): | 637 |
| Entropy (8bit): | 3.330762844151229 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 4A6B302891B1908800E8863321BE7320 |
| SHA1: | C3C8D3C4106B085D3E24BB9F877A9DFBCE80F6BA |
| SHA-256: | 7CF2E8ED183917B02CBACA1C5987E9B33ADFF0FFE7FE5E355C6E67BB171122B8 |
| SHA-512: | 0554A37992E3697CBABC3B408814E0CCE42EFAFDC8CBF7C68A73B12162F589E9DFE61BC467156C8C4A2B1A74C454F909870D13D2B84F82090D4F8D60F1F2526 D |
| Malicious: | false |
| Preview: | **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** **RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** * *RIGHT_CLICK** **LEFT_CLICK** **LEFT_CLICK** |

### C:\Users\Public\Public\svchost.exe

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | PE32 executable (console) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 40960 |
| Entropy (8bit): | 6.220836733793725 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 07B92F1473B82789F71A58EE8999C631 |
| SHA1: | 2D5FA5CA204E2D31E6AAA5BCAE12CEC921F6DA62 |
| SHA-256: | AD9427B659A7B77E08566627B82C21AF23F35FA3047356113CFEE764A890AD92 |
| SHA-512: | 44D3CE9218778DC375FAEEEB240A1B611978AB6083B041C0D6CD0F62D9BB901BE5F155B1907F0D3C7C44A18A671C7CE915ADBA6499D0111F8F5A381645EB3C D |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Avira, Detection: 100%<br>• Antivirus: ReversingLabs, Detection: 49%<br>• Antivirus: Virustotal, Detection: 56%, Browse |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5=.2q\.aq\.aq\.ax$pa}\.a.,.`}\.a.,.`p\.a.,.`j\.a.,.`u\.a*4.`v\.aq\.a.\.a.-.`s\.a.-.ap\.a.-.`p\.aRichq\.a.....PE..L....h._.....d...:.....b.....@.....@.....p.....X...@.....0.....text...Db.....d..... ..`.rdata..n(.....*...h.....@..@.data.....@....rsrc.....@..@.reloc.....@..B..... |

### C:\Users\Public\Public\svchost.exe:Zone.Identifier

| | |
|---|---|
| Process: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 26 |
| Entropy (8bit): | 3.95006375643621 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 187F488E27DB4AF347237FE461A079AD |
| SHA1: | 6693BA299EC1881249D59262276A0D2CB21F8E64 |
| SHA-256: | 255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309 |
| SHA-512: | 89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E |
| Malicious: | **true** |
| Preview: | [ZoneTransfer]....ZoneId=0 |

### C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 65536 |
| Entropy (8bit): | 0.11013620174689967 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 0588F1296F7F1FDDE141D2FDABB7FAD5 |
| SHA1: | F82614257DFBFC1102827C0065D02E640BC5C2D2 |
| SHA-256: | 67AFFCF77687D7B552EE535F010B93DA6E4E39CCE3D5237241785E25EE810640 |
| SHA-512: | 9D310670835B1C3D119799FF219FF456C3329D2D154ABDC8BEC84946FA190C0DE3BF58C99224675BAB0D3D724B85F29D6B5BCB10C77B7A5367759924FCDBAD 1 |
| Malicious: | false |
| Preview: | .....q.Og.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....r..... .....s7.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c. k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....Pg..... ..... ..... |

**C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl**

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 65536 |
| Entropy (8bit): | 0.11262325110440781 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F2B61D630EEAE6EE4A8A6AA2A3AA9AE4 |
| SHA1: | CE5BE05CED5C296CB1BC8C170E3423A21FDD3FDF |
| SHA-256: | 316573276F52A5E6474CBD5252DD8F5259FE6447F7116516777364408630C6E5 |
| SHA-512: | 06E7523579C15B1B44813520458A5F3AE170189DE87F85CA8FC396C72AA904E561010BDD22418FF40F833BDBAE909509FE000C2208F195F7DA6751BAE1CF11DC |
| Malicious: | false |
| Preview: | .....*DLg.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....r..... .....W..s7.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....gXLg..... ..... ..... |

**C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl**

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 65536 |
| Entropy (8bit): | 0.11238869034146516 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | B7D4ED2C1879CCFD7BE7638A456C10BD |
| SHA1: | A1666AF4F9C327009DB7D1A469FEFA9096718728 |
| SHA-256: | 492153307D679C36C56836CAC97571DC76FDC0545C76F53E5F0B9BE89F937149 |
| SHA-512: | 0D3DF0158F91E63ABF4D1A0682F4A28C45D50E7338587E69683F0CC468AA483D8C39422E49175BC9C88760E081CF0BC2EF32BF1F253DE0D28EEFFD74C9F357C 8 |
| Malicious: | false |
| Preview: | .....IDg.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....r..... .....s2.s7.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a. l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....AtDg..... ..... ..... |

**C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001 (copy)**

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 65536 |
| Entropy (8bit): | 0.11013620174689967 |
| Encrypted: | false |

| | |
|---|---|
| SSDEEP: | |
| MD5: | 0588F1296F7F1FDDE141D2FDABB7FAD5 |
| SHA1: | F82614257DFBFC1102827C0065D02E640BC5C2D2 |
| SHA-256: | 67AFFCF77687D7B552EE535F010B93DA6E4E39CCE3D5237241785E25EE810640 |
| SHA-512: | 9D310670835B1C3D119799FF219FF456C3329D2D154ABDC8BEC84946FA190C0DE3BF58C99224675BAB0D3D724B85F29D6B5BCB10C77B7A5367759924FCDBAD 1 |
| Malicious: | false |
| Preview: | .....q.Og.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....r..... .....s7.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c. k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....Pg..... ..... ..... |

### C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 65536 |
| Entropy (8bit): | 0.11262325110440781 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F2B61D630EEAE6EE4A8A6AA2A3AA9AE4 |
| SHA1: | CE5BE05CED5C296CB1BC8C170E3423A21FDD3FDF |
| SHA-256: | 316573276F52A5E6474CBD5252DD8F5259FE6447F711651677736440863 0C6E5 |
| SHA-512: | 06E7523579C15B1B44813520458A5F3AE170189DE87F85CA8FC396C72AA904E561010BDD22418FF40F833BDBAE909509FE000C2208F195F7DA6751BAE1CF11DC |
| Malicious: | false |
| Preview: | .....*DLg.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....r..... .....W..s7.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....gXLg..... ..... ..... |

### C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001 (copy)

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 65536 |
| Entropy (8bit): | 0.11238869034146516 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | B7D4ED2C1879CCFD7BE7638A456C10BD |
| SHA1: | A1666AF4F9C327009DB7D1A469FEFA9096718728 |
| SHA-256: | 492153307D679C36C56836CAC97571DC76FDC0545C76F53E5F0B9BE89F937149 |
| SHA-512: | 0D3DF0158F91E63ABF4D1A0682F4A28C45D50E7338587E69683F0CC468AA483D8C39422E49175BC9C88760E081CF0BC2EF32BF1F253DE0D28EEFFD74C9F357C 8 |
| Malicious: | false |
| Preview: | .....IDg.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....r..... .....s2.s7.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a. l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....AtDg..... ..... ..... |

### C:\Windows\Logs\waasmedic\waasmedic.20230203_020233_050.etl

| | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8192 |
| Entropy (8bit): | 2.73479418886721 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | E15085C22E05811AD31FD41834C8E6AE |
| SHA1: | BEFBAC6963AA8510FF7F3AEC844B7EE284FFBFE4 |
| SHA-256: | 0A56893BBF725D0802C759DDD5BB7F87CDFEBF9A08D9AC9C304DCD467233ADD5 |

| | |
|---|---|
| SHA-512: | 5861906B0EB11D94D5CB726417B8A9470261DB0A2700EE82FF6812147D2EF945F9A5B9D56A5F387A8F6E6F9EA0A191BCE8E67E9A73E4248969B01D5ACCBD6AA 2 |
| Malicious: | false |
| Preview: | .....!.....,..... .E.....B.....s7..Zb..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....WW..... .....J.*.s7.....E.C.C.B.1.7.5.F.-.1.E.B.2.-.4.3.D.A.-.B.F.B.5.-.A.8.D.5.8.A.4.0.A.4.D.7...C. :.\.W.i.n.d.o.w.s.\.l.o.g.s.\.w.a.a.s.m.e.d.i.c.\.w.a.a.s.m.e.d.i.c...2.0.2.3.0.2.0.3._.0.2.0.2.3.3._.0.5.0...e.t.l.....P.P.,..... .E.....9.B. .E.....17134.1.amd64fre.rs4_release.180410-1804.....5.@. .E.....OYo."(.s..O.....WaaSMedicSvc.pdb..... ..... |

### C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

| | |
|---|---|
| Process: | C:\Program Files\Windows Defender\MpCmdRun.exe |
| File Type: | Unicode text, UTF-16, little-endian text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 10874 |
| Entropy (8bit): | 3.1652533662848836 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 54F1BF0991F70FED43D36387452A38F7 |
| SHA1: | 91899AAD877A8895200CF8FAB5D832D9ECE994C5 |
| SHA-256: | 3A34AE9B6B493B7D4E07A0E0F9EED9B17776F1FC7F9C8E2E7702930A15844985 |
| SHA-512: | 5AA34C051A5864E1F3AEC29CE76F021A30AA0679E8B6799679547A4FA0D64D1377C1D7133D223434127531B2136186ABF10D5DA6389C383ADAC973A57E2D6BF |
| Malicious: | false |
| Preview: | .....-.-.-.

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (console) Intel 80386, for MS Windows |
| Entropy (8bit): | 6.220836733793725 |
| 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: | MASTER_Malware_Lab1.exe |
| File size: | 40960 |
| MD5: | 07b92f1473b82789f71a58ee8999c631 |
| SHA1: | 2d5fa5ca204e2d31e6aaa5bcae12cec921f6da62 |
| SHA256: | ad9427b659a7b77e08566627b82c21af23f35fa3047356113cfee764a890ad92 |
| SHA512: | 44d3ce9218778dc375faeeeb240a1b611978ab6083b041c0d6cd0f62d9bb901be5f155b1907f0d3c7c44a18a671c7ce915adba6499d0111f8f5a381645eb3c0d |
| SSDEEP: | 768:fZiXwifvv5il3eIIOeb7cIKo0FnQVu7Cx96+:fgk3eIIOebBAnqs+ |
| TLSH: | 5703F533BA0BC7B3EA1503F105756BA687EBB4240F5002C737845E7E25252DAAD77876 |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5=.2q\.aq\.aq\.ax$pa}\.a.,.`}\.a.,.`p\.a.,.`j\.a.,.`u\.a*4.`v\.aq\.a.\.a.-.`s\.a.-.ap\.a.-.`p\.aRichq\.a.....PE..L.. |

## File Icon

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

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4062e4 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows cui |
| Image File Characteristics: | EXECUTABLE_IMAGE, 32BIT_MACHINE |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x5F8C68C1 [Sun Oct 18 16:09:37 2020 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 6 |
| OS Version Minor: | 0 |
| File Version Major: | 6 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 6 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 962e2dbbc5bb67a0f87fcd14de36453f |

### Entrypoint Preview

| Instruction |
|---|
| call 00007F2628C19EB6h |
| jmp 00007F2628C19929h |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| push esi |
| mov ecx, dword ptr [eax+3Ch] |
| add ecx, eax |
| movzx eax, word ptr [ecx+14h] |
| lea edx, dword ptr [ecx+18h] |

| Instruction |
| --- |
| add edx, eax |
| movzx eax, word ptr [ecx+06h] |
| imul esi, eax, 28h |
| add esi, edx |
| cmp edx, esi |
| je 00007F2628C19ACBh |
| mov ecx, dword ptr [ebp+0Ch] |
| cmp ecx, dword ptr [edx+0Ch] |
| jc 00007F2628C19ABCh |
| mov eax, dword ptr [edx+08h] |
| add eax, dword ptr [edx+0Ch] |
| cmp ecx, eax |
| jc 00007F2628C19ABEh |
| add edx, 28h |
| cmp edx, esi |
| jne 00007F2628C19A9Ch |
| xor eax, eax |
| pop esi |
| pop ebp |
| ret |
| mov eax, edx |
| jmp 00007F2628C19AABh |
| push esi |
| call 00007F2628C1A3B4h |
| test eax, eax |
| je 00007F2628C19AD2h |
| mov eax, dword ptr fs:[00000018h] |
| mov esi, 0040B21Ch |
| mov edx, dword ptr [eax+04h] |
| jmp 00007F2628C19AB6h |
| cmp edx, eax |
| je 00007F2628C19AC2h |
| xor eax, eax |
| mov ecx, edx |
| lock cmpxchg dword ptr [esi], ecx |
| test eax, eax |
| jne 00007F2628C19AA2h |
| xor al, al |
| pop esi |
| ret |
| mov al, 01h |
| pop esi |
| ret |
| push ebp |
| mov ebp, esp |
| cmp dword ptr [ebp+08h], 00000000h |
| jne 00007F2628C19AB9h |
| mov byte ptr [0040B220h], 00000001h |
| call 00007F2628C1A1A3h |
| call 00007F2628C19E85h |
| test al, al |
| jne 00007F2628C19AB6h |
| xor al, al |
| pop ebp |
| ret |
| call 00007F2628C19E78h |
| test al, al |
| jne 00007F2628C19ABCh |
| push 00000000h |

| Instruction |
| --- |
| call 00007F2628C19E6Dh |
| pop ecx |
| jmp 00007F2628C19A9Bh |
| mov al, 01h |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| cmp byte ptr [0040B221h], 00000000h |
| je 00007F2628C19AB6h |
| mov al, 01h |

## Rich Headers

| | |
| --- | --- |
| Programming Language: | • [IMP] VS2008 SP1 build 30729 |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
| --- | --- | --- | --- |
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x95ac | 0xf0 | .rdata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0xc000 | 0x1e0 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0xd000 | 0x7f0 | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x87e4 | 0x70 | .rdata |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x8858 | 0x40 | .rdata |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x8000 | 0x230 | .rdata |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_RESERVED | 0x0 | 0x0 | |

## Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| .text | 0x1000 | 0x6244 | 0x6400 | False | 0.488125 | data | 6.297825159654746 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| .rdata | 0x8000 | 0x286e | 0x2a00 | False | 0.36551339285714285 | data | 4.981255823703229 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0xb000 | 0x59c | 0x400 | False | 0.19140625 | data | 2.8760248433349993 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .rsrc | 0xc000 | 0x1e0 | 0x200 | False | 0.529296875 | data | 4.701503258251789 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0xd000 | 0x7f0 | 0x800 | False | 0.86865234375 | data | 6.593452583866235 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

## Resources

| Name | RVA | Size | Type | Language | Country |
| --- | --- | --- | --- | --- | --- |
| RT_MANIFEST | 0xc060 | 0x17d | XML 1.0 document, ASCII text, with CRLF line terminators | English | United States |

## Imports

| DLL | Import |
|---|---|
| KERNEL32.dll | AllocConsole, SetUnhandledExceptionFilter, GetModuleHandleW, InitializeSListHead, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCurrentProcessId, CloseHandle, CreateFileA, SetFilePointer, GetModuleFileNameW, WriteFile, CopyFileW, IsDebuggerPresent, Sleep, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, UnhandledExceptionFilter |
| USER32.dll | GetDC, ShowWindow, FindWindowA, ReleaseDC, GetSystemMetrics, GetAsyncKeyState |
| GDI32.dll | CreateCompatibleBitmap, SelectObject, CreateCompatibleDC, GetDIBits, DeleteDC, DeleteObject, BitBlt |
| MSVCP140.dll | ?id@?$codecvt@DDU_Mbstatet@@@std@@2V0locale@2@A, ?_Fiopen@std@@YAPAU_iobuf@@PBDHH@Z, ?_Xlength_error@std@@YAXPBD@Z, _Cnd_do_broadcast_at_thread_exit, _Thrd_id, _Thrd_join, ?_Osfx@?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEXXZ, ?_Getcat@?$codecvt@DDU_Mbstatet@@@std@@SAIPAPBVfacet@locale@2@PBV42@@Z, ?sputn@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QAE_JPBD_J@Z, ?put@?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV12@D@Z, ?flush@?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV12@XZ, ?_Getgloballocale@locale@std@@CAPAV_Locimp@12@XZ, ?widen@?$basic_ios@DU?$char_traits@D@std@@@std@@QBEDD@Z, ?unshift@?$codecvt@DDU_Mbstatet@@@std@@QBEHAAU_Mbstatet@@PAD1AAPAD@Z, ??0?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAE@XZ, ?getloc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QBE?AVlocale@2@XZ, ?_Init@?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAEXXZ, ?in@?$codecvt@DDU_Mbstatet@@@std@@QBEHAAU_Mbstatet@@PBD1AAPBDPAD3AAPAD@Z, ?out@?$codecvt@DDU_Mbstatet@@@std@@QBEHAAU_Mbstatet@@PBD1AAPBDPAD3AAPAD@Z, ?_Pninc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAEPADXZ, ?clear@?$basic_ios@DU?$char_traits@D@std@@@std@@QAEXH_N@Z, ?setstate@?$basic_ios@DU?$char_traits@D@std@@@std@@QAEXH_N@Z, ??0?$basic_ios@DU?$char_traits@D@std@@@std@@IAE@XZ, ??0?$basic_ostream@DU?$char_traits@D@std@@@std@@QAE@PAV?$basic_streambuf@DU?$char_traits@D@std@@@1@_N@Z, ??1?$basic_streambuf@DU?$char_traits@D@std@@@std@@UAE@XZ, ?showmanyc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAE_JXZ, ?xsgetn@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAE_JPAD_J@Z, ?xsputn@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAE_JPBD_J@Z, ??1?$basic_ios@DU?$char_traits@D@std@@@std@@UAE@XZ, ??1?$basic_ostream@DU?$char_traits@D@std@@@std@@UAE@XZ, ??6?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV01@P6AAAV01@AAV01@@Z@Z, ?always_noconv@codecvt_base@std@@QBE_NXZ, ??Bid@locale@std@@QAEIXZ, ?cout@std@@3V?$basic_ostream@DU?$char_traits@D@std@@@1@A, ?_Throw_Cpp_error@std@@YAXH@Z, ??0_Lockit@std@@QAE@H@Z, ??1_Lockit@std@@QAE@XZ, ?uncaught_exception@std@@YA_NXZ, ?sputc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QAEHD@Z |
| VCRUNTIME140.dll | memset, __current_exception_context, __current_exception, _except_handler4_common, memcpy, __CxxFrameHandler3, __std_exception_destroy, __std_exception_copy, __std_terminate, _CxxThrowException, memmove |
| api-ms-win-crt-stdio-l1-1-0.dll | ungetc, setvbuf, fgetpos, fwrite, fread, __p__commode, fsetpos, _get_stream_buffer_pointers, fgetc, _fseeki64, fclose, fflush, fputc, _set_fmode |
| api-ms-win-crt-runtime-l1-1-0.dll | _initterm_e, exit, _exit, terminate, __p___argc, _initterm, _cexit, _c_exit, _register_thread_local_exe_atexit_callback, _get_initial_narrow_environment, _initialize_narrow_environment, _configure_narrow_argv, _initialize_onexit_table, _register_onexit_function, _crt_atexit, _set_app_type, _controlfp_s, _seh_filter_exe, system, _invalid_parameter_noinfo_noreturn, _beginthreadex, __p___argv |
| api-ms-win-crt-filesystem-l1-1-0.dll | _mkdir, _unlock_file, _access, _lock_file |
| api-ms-win-crt-heap-l1-1-0.dll | malloc, _callnewh, _set_new_mode, free |
| api-ms-win-crt-math-l1-1-0.dll | __setusermatherr |
| api-ms-win-crt-locale-l1-1-0.dll | _configthreadlocale |

### Possible Origin

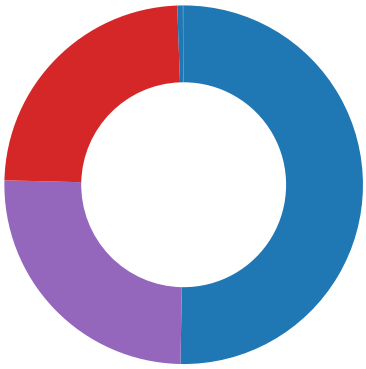
| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States | |

## Network Behavior

**Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.**

# Statistics

## Behavior



- MASTER_Malware_Lab1.exe
- conhost.exe
- cmd.exe
- reg.exe
- svchost.exe
- conhost.exe
- cmd.exe
- reg.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- conhost.exe
- cmd.exe
- reg.exe
- svchost.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe

Click to jump to process

# System Behavior

## Analysis Process: MASTER_Malware_Lab1.exe PID: **2560**, Parent PID: **3452**

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 18:02:04 |
| Start date: | 02/02/2023 |
| Path: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\MASTER_Malware_Lab1.exe |
| Imagebase: | 0x190000 |
| File size: | 40960 bytes |
| MD5 hash: | 07B92F1473B82789F71A58EE8999C631 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### File Activities

## Analysis Process: conhost.exe PID: **3076**, Parent PID: **2560**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 18:02:04 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff745070000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |

| | |
|---|---|
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: cmd.exe PID: **5264**, Parent PID: **2560**

### General

| | |
|---|---|
| Target ID: | 2 |
| Start time: | 18:02:04 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\cmd.exe /c REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe |
| Imagebase: | 0xb0000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: reg.exe PID: **5256**, Parent PID: **5264**

### General

| | |
|---|---|
| Target ID: | 3 |
| Start time: | 18:02:04 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\SysWOW64\reg.exe |
| Wow64 process (32bit): | true |
| Commandline: | REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe |
| Imagebase: | 0x310000 |
| File size: | 59392 bytes |
| MD5 hash: | CEE2A7E57DF2A159A065A34913A055C2 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

### Registry Activities

## Analysis Process: svchost.exe PID: **628**, Parent PID: **3452**

### General

| | |
|---|---|
| Target ID: | 4 |
| Start time: | 18:02:17 |

| | |
|---|---|
| Start date: | 02/02/2023 |
| Path: | C:\Users\Public\Public\svchost.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\Public\Public\svchost.exe" |
| Imagebase: | 0x1a0000 |
| File size: | 40960 bytes |
| MD5 hash: | 07B92F1473B82789F71A58EE8999C631 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Antivirus matches: | • Detection: 100%, Avira<br>• Detection: 49%, ReversingLabs<br>• Detection: 56%, Virustotal, Browse |
| Reputation: | low |

## File Activities

### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\svchost.exe | read data or list directory \| read attributes \| delete \| write dac \| synchronize \| generic read \| generic write | device \| sparse file | sequential only \| non directory file | object name collision | 1 | 1A3240 | CopyFileW |
| C:\Users\Public\Public\svchost.exe | read data or list directory \| read attributes \| delete \| write dac \| synchronize \| generic write | device \| sparse file | sequential only \| non directory file | object name collision | 1 | 1A3240 | CopyFileW |

### File Written

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot000.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot000.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot000.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot000.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot001.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot003.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot003.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot005.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot005.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot005.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot007.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot007.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot007.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot007.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot008.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot009.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot009.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot009.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot009.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot010.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot012.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot012.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot014.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot014.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot014.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot016.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot016.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot016.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot016.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot017.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot018.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot018.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot018.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot018.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot019.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot021.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot021.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot023.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot023.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot023.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot025.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot025.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot025.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot025.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot026.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot027.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot027.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot027.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot027.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot028.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot030.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot030.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot032.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot032.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot032.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot034.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot034.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot034.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot034.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot035.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot036.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot036.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot036.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot036.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot037.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot039.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot039.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot041.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot041.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot041.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot043.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot043.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot043.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot043.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot044.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot045.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot045.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot045.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot045.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot046.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot048.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot048.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot050.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot050.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot050.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot052.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot052.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot052.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot052.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot053.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot054.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot054.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot054.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot054.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot055.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot057.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot057.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot059.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot059.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot059.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot061.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot061.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot061.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot061.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot062.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot063.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot063.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot063.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot063.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot064.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot066.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot066.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot068.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot068.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot068.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| | |
|---|---|
| Imagebase: | 0xb0000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: reg.exe PID: **5964**, Parent PID: **5500**

### General

| | |
|---|---|
| Target ID: | 7 |
| Start time: | 18:02:19 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\SysWOW64\reg.exe |
| Wow64 process (32bit): | true |
| Commandline: | REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe |
| Imagebase: | 0x310000 |
| File size: | 59392 bytes |
| MD5 hash: | CEE2A7E57DF2A159A065A34913A055C2 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: svchost.exe PID: **732**, Parent PID: **580**

### General

| | |
|---|---|
| Target ID: | 8 |
| Start time: | 18:02:21 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService |
| Imagebase: | 0x7ff651c80000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: svchost.exe PID: **3512**, Parent PID: **580**

### General

| | |
|---|---|
| Target ID: | 9 |
| Start time: | 18:02:22 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k unistacksvcgroup |
| Imagebase: | 0x7ff651c80000 |

| | |
|---|---|
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: svchost.exe PID: **2792**, Parent PID: **580**

### General

| | |
|---|---|
| Target ID: | 10 |
| Start time: | 18:02:23 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc |
| Imagebase: | 0x7ff651c80000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: svchost.exe PID: **6140**, Parent PID: **580**

### General

| | |
|---|---|
| Target ID: | 11 |
| Start time: | 18:02:24 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc |
| Imagebase: | 0x7ff651c80000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: svchost.exe PID: **5240**, Parent PID: **580**

### General

| | |
|---|---|
| Target ID: | 12 |
| Start time: | 18:02:25 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k NetworkService -p |
| Imagebase: | 0x7ff651c80000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

## Analysis Process: svchost.exe PID: **4684**, Parent PID: **3452**

### General

| | |
|---|---|
| Target ID: | 13 |
| Start time: | 18:02:25 |
| Start date: | 02/02/2023 |
| Path: | C:\Users\Public\Public\svchost.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\Public\Public\svchost.exe" |
| Imagebase: | 0x1a0000 |
| File size: | 40960 bytes |
| MD5 hash: | 07B92F1473B82789F71A58EE8999C631 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

#### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\svchost.exe | read data or list directory \| read attributes \| delete \| write dac \| synchronize \| generic read \| generic write | device \| sparse file | sequential only \| non directory file | object name collision | 1 | 1A3240 | CopyFileW |
| C:\Users\Public\Public\svchost.exe | read data or list directory \| read attributes \| delete \| write dac \| synchronize \| generic write | device \| sparse file | sequential only \| non directory file | object name collision | 1 | 1A3240 | CopyFileW |

#### File Written

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot001.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot001.bmp | 66 | 8294400 | 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot003.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot003.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot003.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot005.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot005.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot005.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot005.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot006.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot007.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot007.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot007.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot007.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot008.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot010.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot010.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot012.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot012.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot012.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot014.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot014.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot014.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot014.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot015.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot016.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot016.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot016.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot016.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot017.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot019.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot019.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot021.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot021.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot021.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot023.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot023.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot023.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot023.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot024.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot025.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot025.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot025.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot025.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot026.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot028.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot028.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot030.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot030.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot030.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot032.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot032.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot032.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot032.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot033.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot034.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot034.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot034.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot034.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot035.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot037.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot037.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot039.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot039.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot039.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot041.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot041.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot041.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot041.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot042.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot043.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot043.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot043.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot043.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot044.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot046.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot046.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot048.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot048.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot048.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot050.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot050.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot050.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot050.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot051.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot052.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot052.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot052.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot052.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot053.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot055.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot055.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot057.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot057.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot057.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot059.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot059.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot059.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot059.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot060.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A5A70 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot061.bmp | 0 | 14 | 42 4d 42 fd 7e 00 00 00 00 00 42 00 00 00 | BMB~B | success or wait | 1 | 1A597F | WriteFile |
| C:\Users\Public\Public\Screens\screenshot061.bmp | 14 | 40 | 28 00 00 00 fd 07 00 00 38 04 00 00 01 00 20 00 03 00 00 00 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | (8 ~ | success or wait | 1 | 1A59A1 | WriteFile |
| C:\Users\Public\Public\Screens\screenshot061.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot061.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot062.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\Public\Public\Screens\screenshot064.bmp | 54 | 12 | 00 00 fd 00 00 fd 00 00 fd 00 00 00 | | success or wait | 1 | 1A59FD | WriteFile |
| C:\Users\Public\Public\Screens\screenshot064.bmp | 66 | 8294400 | 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>

## Analysis Process: conhost.exe PID: **4340**, Parent PID: **4684**

### General

| | |
|---|---|
| Target ID: | 14 |
| Start time: | 18:02:26 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff745070000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

## Analysis Process: cmd.exe PID: **2384**, Parent PID: **4684**

### General

| | |
|---|---|
| Target ID: | 15 |
| Start time: | 18:02:26 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\cmd.exe /c REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe |
| Imagebase: | 0xb0000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

## Analysis Process: reg.exe PID: **5444**, Parent PID: **2384**

### General

| | |
|---|---|
| Target ID: | 16 |
| Start time: | 18:02:26 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\SysWOW64\reg.exe |
| Wow64 process (32bit): | true |
| Commandline: | REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V Firewall /t REG_SZ /F /D C:\Users\Public\Public\svchost.exe |
| Imagebase: | 0x310000 |
| File size: | 59392 bytes |
| MD5 hash: | CEE2A7E57DF2A159A065A34913A055C2 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: svchost.exe PID: **848**, Parent PID: **580**

### General

| | |
|---|---|
| Target ID: | 18 |
| Start time: | 18:02:29 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff651c80000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

### Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: svchost.exe PID: **6128**, Parent PID: **580**

### General

| | |
|---|---|
| Target ID: | 19 |
| Start time: | 18:02:32 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc |
| Imagebase: | 0x7ff651c80000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: svchost.exe PID: **3020**, Parent PID: **580**

### General

| | |
|---|---|
| Target ID: | 20 |
| Start time: | 18:02:32 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc |
| Imagebase: | 0x7ff651c80000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: MpCmdRun.exe PID: **4600**, Parent PID: **6128**

### General

| | |
|---|---|
| Target ID: | 21 |
| Start time: | 18:03:34 |
| Start date: | 02/02/2023 |
| Path: | C:\Program Files\Windows Defender\MpCmdRun.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable |
| Imagebase: | 0x7ff76d380000 |
| File size: | 455656 bytes |
| MD5 hash: | A267555174BFA53844371226F482B86B |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

### File Written

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log | 9968 | 182 | 0d 00 0a 00 0d 00 0a 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 0d 00 0a 00 | ----------<br>----------<br>---------- | success or wait | 1 | 7FF76D3ABC96 | WriteFile |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log | 10150 | 258 | 4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 68 00 75 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 30 00 32 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 31 00 38 00 3a 00 30 00 33 00 3a 00 33 00 35 00 0d 00 0a 00 0d | MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Thu Feb 02 2023 18:03:35 | success or wait | 1 | 7FF76D3ABC96 | WriteFile |
| C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log | 10408 | 86 | 4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00 | MpEnsureProcessMitigationPolicy: hr = 0x1 | success or wait | 1 | 7FF76D3ABC96 | WriteFile |
| C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log | 10494 | 20 | 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 | WDEnable | success or wait | 1 | 7FF76D3ABC96 | WriteFile |
| C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log | 10514 | 86 | 45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00 | ERROR: MpWDEnable(TRUE) failed (800704EC) | success or wait | 1 | 7FF76D3ABC96 | WriteFile |
| C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log | 10600 | 100 | 4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 68 00 75 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 30 00 32 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 31 00 38 00 3a 00 30 00 33 00 3a 00 33 00 35 00 0d 00 0a 00 | MpCmdRun: End Time: Thu Feb 02 2023 18:03:35 | success or wait | 1 | 7FF76D3ABC96 | WriteFile |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log | 10700 | 174 | 2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 2d 00 2d 00 2d 00<br>2d 00 0d 00 0a 00 | ----------<br>----------<br>---------- | success or wait | 1 | 7FF76D3ABC96 | WriteFile |

## Analysis Process: conhost.exe PID: **3012**, Parent PID: **4600**

### General

| | |
|---|---|
| Target ID: | 22 |
| Start time: | 18:03:34 |
| Start date: | 02/02/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff745070000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

## Disassembly

**No disassembly**