ID: 800802
Sample Name: file.exe
Cookbook: default.jbs
Time: 20:03:06
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

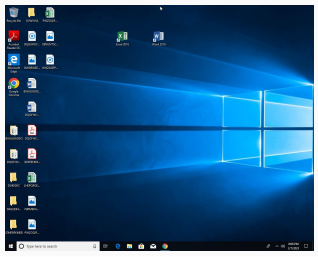
Windows Analysis Report

file.exe

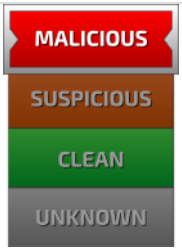
Overview

General Information

Sample Name:	file.exe
Analysis ID:	800802
MD5:	546a040e4479…
SHA1:	69a99c8f2fbfc3..
SHA256:	229d8701db31…
Tags:	exe
Infos:	



Detection



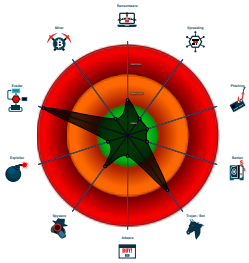
Tofsee

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

Signatures

- Detected unpacking (overwrites its o…
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Yara detected Tofsee
- Uses netsh to modify the Windows …
- Query firmware table information (lik…
- Machine Learning detection for sam…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5128 cmdline: C:\Users\user\Desktop\file.exe MD5: 546A040E4479958F7C6B862DEAD9A269)
  - cmd.exe (PID: 3076 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\htdzdeug\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 2432 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\qbxctmyn.exe" C:\Windows\SysWOW64\htdzdeug\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 1020 cmdline: C:\Windows\System32\sc.exe" create htdzdeug binPath= "C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe /d\"C:\Users\user\Desktop\file.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
    - conhost.exe (PID: 5036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 5828 cmdline: C:\Windows\System32\sc.exe" description htdzdeug "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
    - conhost.exe (PID: 5800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 3108 cmdline: "C:\Windows\System32\sc.exe" start htdzdeug MD5: 24A3E2603E63BCB9695A2935D3B24695)
    - conhost.exe (PID: 4952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - netsh.exe (PID: 5864 cmdline: "C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
    - conhost.exe (PID: 4844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6120 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3592 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5064 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5400 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1764 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1652 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- qbxctmyn.exe (PID: 4532 cmdline: C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe /d"C:\Users\user\Desktop\file.exe" MD5: D83D3102AEE8419201BF810DE2A41992)
  - svchost.exe (PID: 2888 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- svchost.exe (PID: 1328 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2140 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 612 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 1500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 4204 cmdline: c:\windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Tofsee


```
{
  "C2 list": [
    "svartalfheim.top:443",
    "jotunheim.name:443"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.310301101.0000000000400000.00000040.00000001.01000000.00000005.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000011.00000002.310301101.0000000000400000.00000040.00000001.01000000.00000005.sdmp	MALWARE_Win_Tofsee	Detects Tofsee	ditekSHen	• 0x1123e:$s1: n%systemroot%\system32\cmd.exe • 0x10310:$s2: loader_id • 0x10340:$s3: start_srv • 0x10370:$s4: lid_file_upd • 0x10364:$s5: localcfg • 0x10a94:$s6: Incorrect respons • 0x10b74:$s7: mx connect error • 0x10af0:$s8: Error sending command (sent = %d/%d) • 0x10c28:$s9: %s, %u %s %u %.2u:%.2u:%.2u %s%.2u%.2u
00000011.00000002.310301101.0000000000400000.00000040.00000001.01000000.00000005.sdmp	Windows_Trojan_Tofsee_26124fe4	unknown	unknown	• 0x2544:$a: 55 8B EC 8B 45 08 57 8B 7D 10 B1 01 85 FF 74 1D 56 8B 75 0C 2B F0 8A 14 06 32 55 14 88 10 8A D1 02 55 18 F6 D9 00 55 14 40 4F 75 EA 5E 8B 45 08 5F 5D C3 • 0xee95:$b: 8B 44 24 04 53 8A 18 84 DB 74 2D 8B D0 2B 54 24 0C 8B 4C 24 0C 84 DB 74 12 8A 19 84 DB 74 1B 3 8 1C 0A 75 07 41 80 3C 0A 00 75 EE 80 39 00 74 0A 40 8A 18 42 84 DB 75 D9 33 C0 5B C3
00000011.00000002.310875987.0000000000E30000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000011.00000002.310875987.0000000000E30000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.2080e67.1.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
0.2.file.exe.2080e67.1.raw.unpack	MALWARE_Win_Tofsee	Detects Tofsee	ditekSHen	• 0xfc3e:$s1: n%systemroot%\system32\cmd.exe • 0xed10:$s2: loader_id • 0xed40:$s3: start_srv • 0xed70:$s4: lid_file_upd • 0xed64:$s5: localcfg • 0xf494:$s6: Incorrect respons • 0xf574:$s7: mx connect error • 0xf4f0:$s8: Error sending command (sent = %d/%d) • 0xf628:$s9: %s, %u %s %u %.2u:%.2u:%.2u %s%.2u%.2u
0.2.file.exe.2080e67.1.raw.unpack	Windows_Trojan_Tofsee_26124fe4	unknown	unknown	• 0x1944:$a: 55 8B EC 8B 45 08 57 8B 7D 10 B1 01 85 FF 74 1D 56 8B 75 0C 2B F0 8A 14 06 32 55 14 88 10 8A D1 02 55 18 F6 D9 00 55 14 40 4F 75 EA 5E 8B 45 08 5F 5D C3 • 0xe295:$b: 8B 44 24 04 53 8A 18 84 DB 74 2D 8B D0 2B 54 24 0C 8B 4C 24 0C 84 DB 74 12 8A 19 84 DB 74 1B 3 8 1C 0A 75 07 41 80 3C 0A 00 75 EE 80 39 00 74 0A 40 8A 18 42 84 DB 75 D9 33 C0 5B C3
17.2.qbxctmyn.exe.e30e67.1.unpack	MALWARE_Win_Tofsee	Detects Tofsee	ditekSHen	• 0xe110:$s2: loader_id • 0xe140:$s3: start_srv • 0xe170:$s4: lid_file_upd • 0xe164:$s5: localcfg • 0xe894:$s6: Incorrect respons

Source	Rule	Description	Author	Strings
17.2.qbxctmyn.exe.e30e67.1.unpack	Windows_Trojan_Tofsee_26124fe4	unknown	unknown	• 0xd44:$a: 55 8B EC 8B 45 08 57 8B 7D 10 B1 01 85 FF 74 1D 56 8B 75 0C 2B F0 8A 14 06 32 55 14 88 10 8A D1 02 55 18 F6 D9 00 55 14 40 4F 75 EA 5E 8B 45 08 5F 5D C3 • 0xd695:$b: 8B 44 24 04 53 8A 18 84 DB 74 2D 8B D0 2B 54 24 0C 8B 4C 24 0C 84 DB 74 12 8A 19 84 DB 74 1B 38 1C 0A 75 07 41 80 3C 0A 00 75 EE 80 39 00 74 0A 40 8A 18 42 84 DB 75 D9 33 C0 5B C3
Click to see the 39 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.856924532023883 02/07/23-20:05:14.210188
SID:	2023883
Source Port:	56924
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.852387532023883 02/07/23-20:04:33.939091
SID:	2023883
Source Port:	52387
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.860625532023883 02/07/23-20:05:54.726769
SID:	2023883
Source Port:	60625
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

AV Detection

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Spam, unwanted Advertisements and Ransom Demands

Yara detected Tofsee

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

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

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

HIPS / PFW / Operating System Protection Evasion

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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

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

Modifies the windows firewall

Stealing of Sensitive Information

Yara detected Tofsee

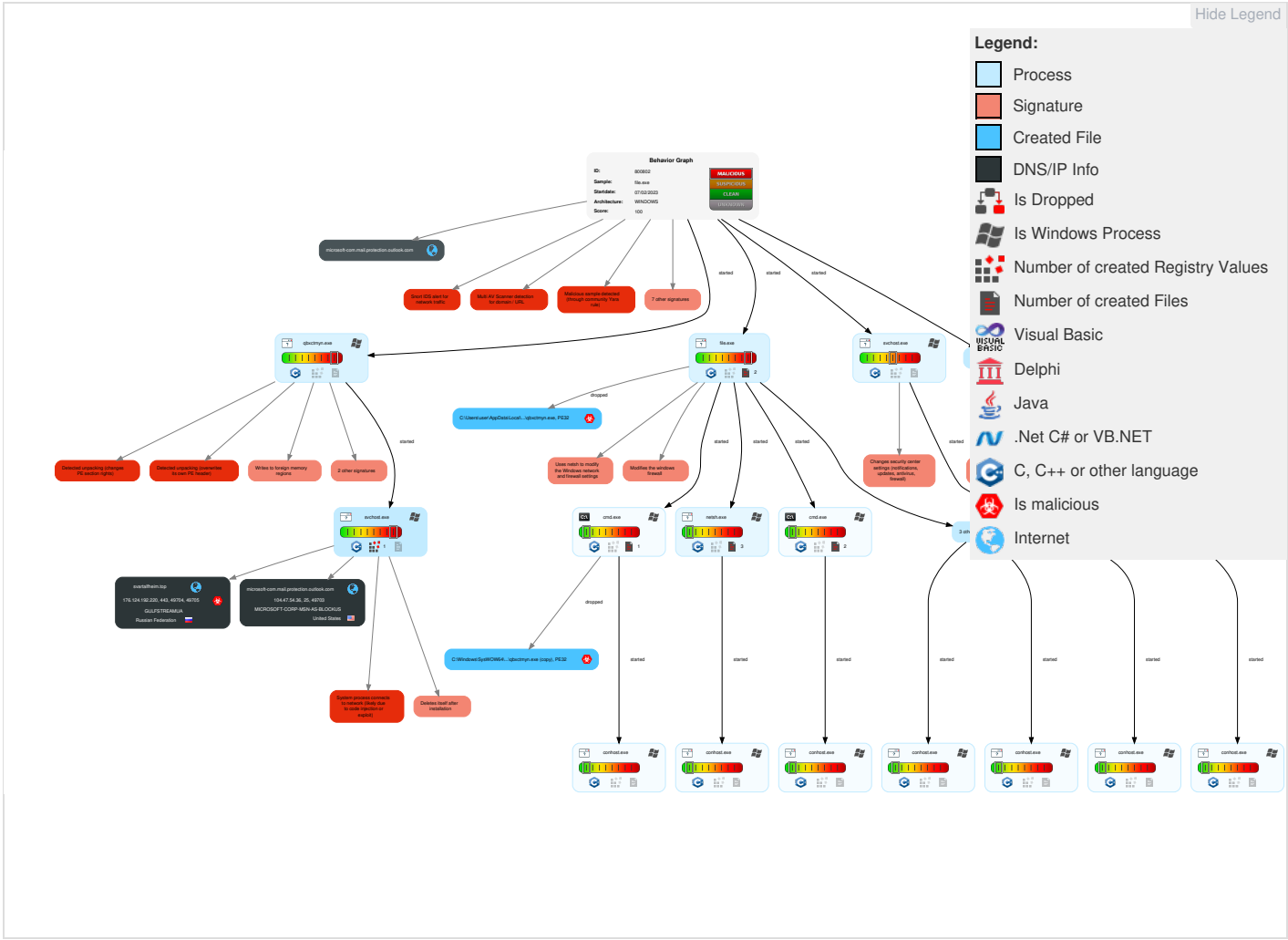
Remote Access Functionality

Yara detected Tofsee

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
1 Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	3 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	4 1 Native API	1 Valid Accounts	1 Valid Accounts	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	1 4 Windows Service	1 Access Token Manipulation	2 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	3 Service Execution	Logon Script (Mac)	1 4 Windows Service	2 1 Software Packing	NTDS	2 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	4 1 2 Process Injection	1 DLL Side-Loading	LSA Secrets	1 4 1 Security Software 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 File Deletion	Cached Domain Credentials	1 2 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 1 Masquerading	DCSync	1 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Valid Accounts	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 2 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Access Token Manipulation	Network Sniffing	1 System Network Configuration Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	4 1 2 Process Injection	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

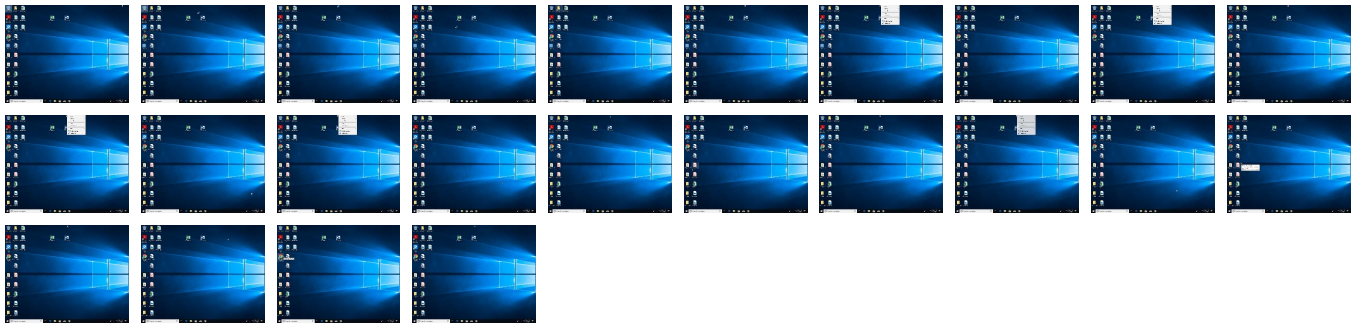
Behavior Graph



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
file.exe	44%	ReversingLabs	Win32.Ransomware.Stop	
file.exe	34%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\qbxctmyn.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\Users\user\AppData\Local\Temp\qbxctmyn.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.qbxctmyn.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
23.2.svchost.exe.120000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.2.qbxctmyn.exe.e90000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.file.exe.2080e67.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
23.3.svchost.exe.649000.1.unpack	100%	Avira	HEUR/AGEN.1253311		Download File
23.3.svchost.exe.649000.2.unpack	100%	Avira	HEUR/AGEN.1253311		Download File
23.3.svchost.exe.649000.4.unpack	100%	Avira	HEUR/AGEN.1253311		Download File
23.3.svchost.exe.649000.3.unpack	100%	Avira	HEUR/AGEN.1253311		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
0.3.file.exe.21c0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.2.qbxctmyn.exe.e30e67.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.3.qbxctmyn.exe.e50000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
svartalfheim.top	18%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
jotunheim.name:443	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
svartalfheim.top:443	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
svartalfheim.top	176.124.192.220	true	true	• 18%, Virustotal, Browse	unknown
microsoft-com.mail.protection.outlook.com	104.47.54.36	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
jotunheim.name:443	true	• URL Reputation: safe	unknown
svartalfheim.top:443	true	• URL Reputation: safe	unknown

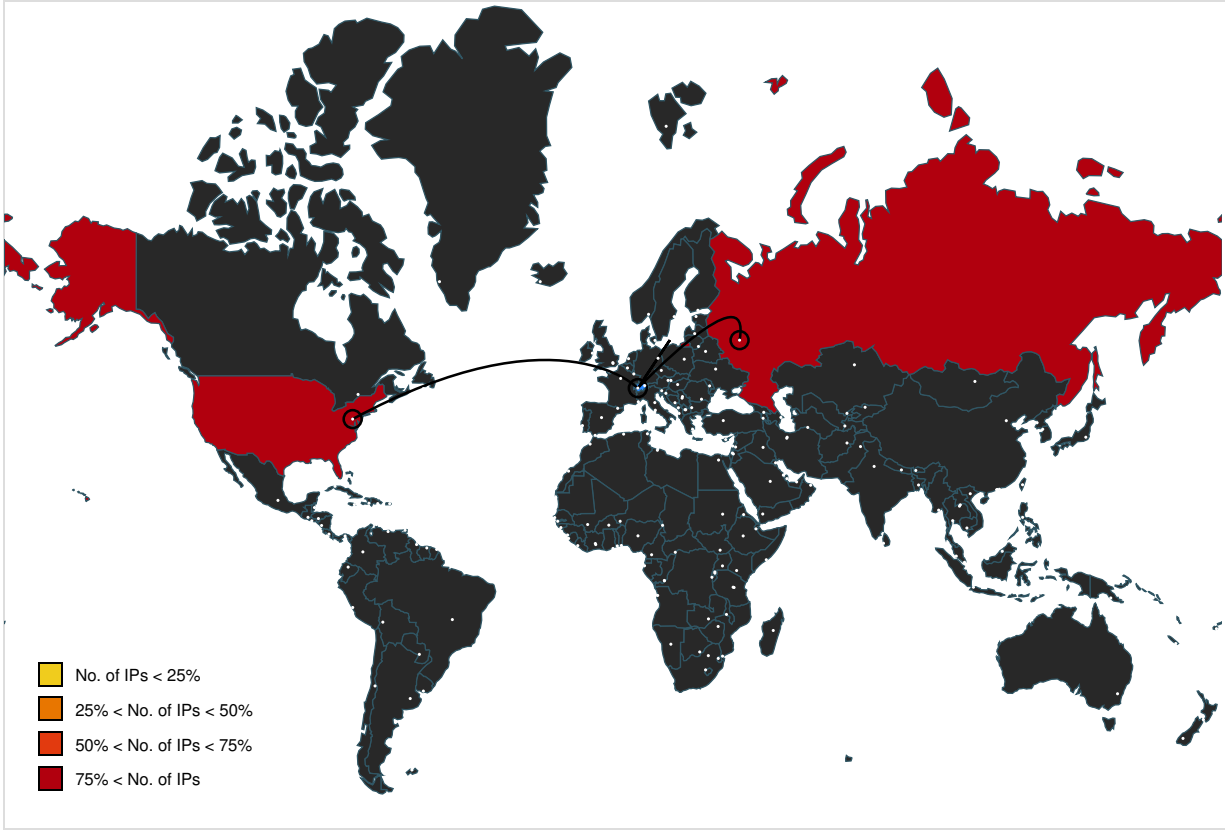
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000B.00000003.308983350.00000189DAC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000003.309037099.00000189DAC45000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309018203.00000189DAC40000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000B.00000002.309374208.00000189DAC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000B.00000003.308983350.00000189DAC60000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000B.00000002.309374208.00000189DAC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000B.00000002.309387517.00000189DAC4B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309001871.00000189DAC49000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000B.00000003.309061387.00000189DAC50000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.309440269.00000189DAC56000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.308990855.00000189DAC4E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000B.00000002.309374208.00000189DAC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000B.00000003.286983822.00000189DAC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000003.286983822.00000189DAC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000B.00000003.308983350.00000189DAC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000B.00000003.309018203.00000189DAC40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.309387517.00000189DAC4B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309001871.00000189DAC49000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000002.309310506.00000189DAC13000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.309374208.00000189DAC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000B.00000003.309018203.00000189DAC40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.309380373.00000189DAC42000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309042425.00000189DAC41000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000005.00000002.531375972.0000028763243000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000003.309061387.00000189DAC50000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.309440269.00000189DAC56000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.308990855.00000189DAC4E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000B.00000003.308983350.00000189DAC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000003.286983822.00000189DAC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.308983350.00000189DAC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.308983350.00000189DAC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000003.309001871.00000189DAC49000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 0000000B.00000003.286983822.00000189DAC30000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000B.00000003.286983822.00000189DAC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000002.309387517.00000189DAC4B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309001871.00000189DAC49000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000002.309387517.00000189DAC4B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309001871.00000189DAC49000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000B.00000003.309018203.00000189DAC40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.309380373.00000189DAC42000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309042425.00000189DAC41000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000B.00000003.308990855.00000189DAC4E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309042425.00000189DAC41000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000B.00000003.308983350.00000189DAC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000B.00000002.309364718.00000189DAC39000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.286983822.00000189DAC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000002.309387517.00000189DAC4B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309001871.00000189DAC49000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000005.00000002.531375972.0000028763243000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000B.00000002.309310506.00000189DAC13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000B.00000003.308983350.00000189DAC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000002.309374208.00000189DAC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000005.00000002.531375972.0000028763243000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000002.309387517.00000189DAC4B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.309001871.00000189DAC49000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000003.309001871.00000189DAC49000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.124.192.220	svartalfheim.top	Russian Federation		59652	GULFSTREAMUA	true
104.47.54.36	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800802
Start date and time:	2023-02-07 20:03:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 12s
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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	file.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@34/16@5/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 49.5% (good quality ratio 47.1%) • Quality average: 86.9% • Quality standard deviation: 25.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Excluded IPs from analysis (whitelisted): 20.112.52.29, 20.81.111.85, 20.84.181.62, 20.103.85.33, 20.53.203.50
- Excluded domains from analysis (whitelisted): fs.microsoft.com, microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:05:14	API Interceptor	2x Sleep call for process: svchost.exe modified
20:05:29	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):	5.2403296958449355
Encrypted:	false

SSDEEP:	24:2dS48pX4y/DvKWDkQpyH2YX8ICDKbNRTrxKTBM2JT52YwFPYzKEqXpUfKFkeRupB:cAn/TLtfGgzmQLeUp/B8HoSkC9+TIYAs
MD5:	BDC008D0C34A85E8B2CF0502871A8D73
SHA1:	0DBF1368F6D3C401D410BFA69B1A0E1BCBCE2558
SHA-256:	514AD1AC5994134A6314AD8A504B79EB558775C1E0269F811B1C11F2CF26AD12
SHA-512:	0D495FCB897BFF1A3530F9F6684770082BC330131B26E263C9E55B04288B6E36F8DFEE9A6B61566809F55DB353C8B35FCF0A8E5D7352307F5DBEBC5A7C9FF8FC
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):	5.2403296958449355
Encrypted:	false
SSDEEP:	24:2dS48pX4y/DvKWDkQpyH2YX8ICDKbNRTrxKTBM2JT52YwFPYzKEqXpUfKFkeRupB:cAn/TLtfGgzmQLeUp/B8HoSkC9+TIYAs
MD5:	BDC008D0C34A85E8B2CF0502871A8D73
SHA1:	0DBF1368F6D3C401D410BFA69B1A0E1BCBCE2558
SHA-256:	514AD1AC5994134A6314AD8A504B79EB558775C1E0269F811B1C11F2CF26AD12
SHA-512:	0D495FCB897BFF1A3530F9F6684770082BC330131B26E263C9E55B04288B6E36F8DFEE9A6B61566809F55DB353C8B35FCF0A8E5D7352307F5DBEBC5A7C9FF8FC
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):	3.7601426671271163
Encrypted:	false
SSDEEP:	96:uoi8itl/ZndZNnAp9Z61zZs4Z5k907HUffZ3AZOX6Z6NZeA3CbZTQZMTkInZLpQ:Zi8ite3NneWpmaXid0eMYiLpQ
MD5:	4D6F0CCB342CAC8385F7158440CBB800
SHA1:	7B2187390048610B2C82A361A2E8EEEF0868C21B
SHA-256:	7C33E7A878DA01E5E1825603194C2C9E0FB8F260B8AB331613C2EB0B327A3864
SHA-512:	4462E8CCF3268C46377E67F9799A7B01EBA24717B84F8E14C84FCA92F42609D573B1C1D4AE5CDB502C2FA4D1B662C81D8F4BC01EA9F4338D4DF128A3350A328
Malicious:	false
Preview:	.....0.....`mr;.....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.....%.?..... .....`mr;.....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.,...0....8gmr;.....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.7601426671271163
Encrypted:	false
SSDEEP:	96:uoi8itl/ZndZNnAp9Z61zZs4Z5k907HUffZ3AZOX6Z6NZeA3CbZTQZMTkInZLpQ:Zi8ite3NneWpmaXid0eMYiLpQ

MD5:	4D6F0CCB342CAC8385F7158440CBB800
SHA1:	7B2187390048610B2C82A361A2E8EEEF0868C21B
SHA-256:	7C33E7A878DA01E5E1825603194C2C9E0FB8F260B8AB331613C2EB0B327A3864
SHA-512:	4462E8CCF3268C46377E67F9799A7B01EBA24717B84F8E14C84FCA92F42609D573B1C1D4AE5CDB502C2FA4D1B662C81D8F4BC01EA9F4338D4DF128A3350A32 8
Malicious:	false
Preview:	.....,...0.....`mr;.....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.....%.?..... .....`mr;.....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.,...0....8gmr;..... ....

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):	0.11004012961626064
Encrypted:	false
SSDEEP:	12:26Y3xgXm/Ey6q99950anNq3qQ10nMCldimE8eawHjcogn:26QLl68SagLyMCldzE9BHjcp
MD5:	5398B5971E6A8C924757AD8450DDDCEA
SHA1:	2B0B99C436D023DDB496F8549CDA84AF76EEE48A
SHA-256:	F69C7AEF9BE67BA09D2D8A9673475CEA648ED784A96579B02C0883CA73EB6732
SHA-512:	F2DD0A29A0C8EBC01C124E0EF7B5B6DC99435C09B631ED0784650C89759E8F71048D4436ED02715A3F2FE3904C00C2132B8468F18D670FD33220FC6D14D9348
Malicious:	false
Preview:	.....j.q.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....%.?..... .....jr;.....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.....I.q..... ....

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):	0.11249012819257488
Encrypted:	false
SSDEEP:	12:MxdlDXm/Ey6q99950aOg1miM3qQ10nMCldimE8eawHza1miIrSd:MvIl68SaX1tMLyMCldzE9BHza1tIC
MD5:	D1338C24B474F80B9D7A721DDDA3E149
SHA1:	C726DCA04341646E0453B24CF482077ADCE7DB74
SHA-256:	6DA48AD356AA520E0FDBE965FD998041401F0C46758DF1ED849DFEB62CC55A15
SHA-512:	132F97E55880EDBCC5807C5CC41613A64F9BB0D7FBC3B1DE400B6438A8BEC3078D999F319CE27C605879023ADBF5DCDB0C2622E4DCF8C4865643FF61CF1AD 49
Malicious:	false
Preview:	.....*_o.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....%.?..... .....d.jr;.....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.....go..... ....

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):	0.1125005015962772
Encrypted:	false
SSDEEP:	12:MxCnXm/Ey6q99950ap11mK2P3qQ10nMCldimE8eawHza1mK2P:MUWl68SaT1iPLyMCldzE9BHza1l
MD5:	F7FF3F878EA4E230282D26BD877E2689
SHA1:	4BC8A22487FA18BFA85E083ADA2C8BAEC128E764
SHA-256:	E34E59D46F9316AA83FE293A0F1E3A7BE34C3A908DA952B470D97503DF85E9B1

SHA-512:	41E21EBA179704BCE1BC8B5686B5D372DA9122960BF76919F9ACE30DB677D5C21E00E11599C5C3207ED09FB979BFC29BC4819657FC1C1D28E626B3A333A7C51
Malicious:	false
Preview:	.....n.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....%.?..... .....<.jr;.....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.....N(n..... ....

C:\Users\user\AppData\Local\Temp\qbxctmyn.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12343296
Entropy (8bit):	3.4208454596549234
Encrypted:	false
SSDEEP:	6144:4JMjbyLY3DuTsP8d2nQO0o7MFGU15Ts+XAW:4JMjbyM3DW8qQa5TsV
MD5:	D83D3102AEE8419201BF810DE2A41992
SHA1:	30EC9FD8B35C5FEC5366FE52C7BF77E57A0C67A2
SHA-256:	4F8B000276DE586232FC912CDB72B497C305E8E13A8DEF72D3A2B0BA2FB7E0C9
SHA-512:	F3E9CEF20B8751716F1426DCACDA675F2672F60FF55218CB4A9BEC141A736D2B12E8761BCFC7115CD5F46DF3E5A83F3D399BD110EF37000F31EAEABDAE3BDCA2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w...a.....q.....t...Rich.....PE.. L.....a.....>.....or.....@.....I...P.....@.....p9..@.....text... ....`.data...0.....8.....@....rsrc..... .....@..@.reloc..n'.....x.....@..B..... ....

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):	0.11004012961626064
Encrypted:	false
SSDEEP:	12:26Y3xgXm/Ey6q99950anNq3qQ10nMCldimE8eawHjcogn:26QLl68SagLyMCldzE9BHjcp
MD5:	5398B5971E6A8C924757AD8450DDDCEA
SHA1:	2B0B99C436D023DDB496F8549CDA84AF76EEE48A
SHA-256:	F69C7AEF9BE67BA09D2D8A9673475CEA648ED784A96579B02C0883CA73EB6732
SHA-512:	F2DD0A29A0C8EBC01C124E0EF7B5B6DC99435C09B631ED0784650C89759E8F71048D4436ED02715A3F2FE3904C00C2132B8468F18D670FD33220FC6D14D9348
Malicious:	false
Preview:	.....j.q.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....%.?..... .....jr;.....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.....I.q..... ....

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):	0.11249012819257488
Encrypted:	false
SSDEEP:	12:MxdlDXm/Ey6q99950aOg1miM3qQ10nMCldimE8eawHza1miIrSd:MvII68SaX1tMLyMCldzE9BHza1tIC
MD5:	D1338C24B474F80B9D7A721DDDA3E149
SHA1:	C726DCA04341646E0453B24CF482077ADCE7DB74
SHA-256:	6DA48AD356AA520E0FDBE965FD998041401F0C46758DF1ED849DFEB62CC55A15
SHA-512:	132F97E55880EDBCC5807C5CC41613A64F9BB0D7FBC3B1DE400B6438A8BEC3078D999F319CE27C605879023ADBF5DCDB0C2622E4DCF8C4865643FF61CF1AD49
Malicious:	false

Preview:	....*_o......................B.............Zb...@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..%.?...... ......d.jr;..........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..........go.. ....

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):	0.1125005015962772
Encrypted:	false
SSDEEP:	12:MxCnXm/Ey6q99950ap11mK2P3qQ10nMCldimE8eawHza1mK2P:MUWl68SaT1iPLyMCldzE9BHza1I
MD5:	F7FF3F878EA4E230282D26BD877E2689
SHA1:	4BC8A22487FA18BFA85E083ADA2C8BAEC128E764
SHA-256:	E34E59D46F9316AA83FE293A0F1E3A7BE34C3A908DA952B470D97503DF85E9B1
SHA-512:	41E21EBA179704BCE1BC8B5686B5D372DA9122960BF76919F9ACE30DB677D5C21E00E11599C5C3207ED09FB979BFC29BC4819657FC1C1D28E626B3A333A7C5 1
Malicious:	false
Preview:	....n......................B.............Zb...@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..%.?...... ......<.jr;..........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.........N(n.. ....

C:\Windows\Logs\waasmedic\waasmedic.20230208_040427_786.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.7367341524723185
Encrypted:	false
SSDEEP:	48:31lr52QWsb7kUub7kE7b7klXb7kib7kbIl9lnb7k0tplKb7k0b7k6b7kwQb7k9O:62k0Uu0g010i0U910ClK00060P09O
MD5:	ECA63CBE24540409B8D7D26006AFC7E9
SHA1:	E68668D56F8DE0B218AB8CE1CAEDAB67738758F5
SHA-256:	C335F94E1135F05A7C9C43DE5836BDBE27F2E434F787D9FC0009F5FAEA226B57
SHA-512:	C0181EA0EE254E387F50B9526BAF3241AF700955588AC99FBE12105B9D40EFB857CD981C8BF533C6CF777AFF0DFFD62873601A3D2EA9FA96804758436E12F50F
Malicious:	false
Preview:	....!..........................4...l...........................B.......)..r;..Zb....... ....@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..WW...... ....'pr;..........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...2.0.2.3.0.2.0.8._.0.4.0.4.2.7._.7.8.6...e.t.l.............P.P.4...l..9. B.........17134.1.amd64fre.rs4_release.180410-1804............5.@.........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):	3.1639573047664586
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z5+6I3+zJf+k:j+s+v+b+P+m+0+Q+q+q+73+zB+k
MD5:	0B770DFFF3F665694BF6BF00027A9FBD
SHA1:	6012FF2CF0F996B044312A974D75656DCBED702D
SHA-256:	3B7BA89B0A8AD80E3BEF0616DFF905DA9A50608933FAFC2B76DA22A4B610B6B6
SHA-512:	A151849ADB59ED84FA413787466E05EA042C7269383B4E24AEB0F4E74E43F4EC33324F90459ACD1BED6ACD30A3F9036D886360480697C24F1EB5A616D1012D08
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20230208_040419_207.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.3870081431882535
Encrypted:	false
SSDEEP:	96:oC/2o+oa5Q+97/YzWC9/l2lfikm/441T2ljFzdNMCn6JROY5Y:7uRjuu2g9CC4q
MD5:	703B2EA8C4DAFDC027C9C239FD4E6F41
SHA1:	5F826A311D1DA602C058515822326D2DC4B19540
SHA-256:	13529537165F17E8C7916312AAE8444F013F69CA50F9C5FCBF04539B7085417E
SHA-512:	31941279367ED33D22B2A84F1E906D263E2DEA3C03C0961962A428957CBD7516AEAFF16EC6A90C35D5600C13B80A98A3355E619BA6AFB2284F888FAA1507709A
Malicious:	false
Preview:	....!.....{.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....WW..... .....kr;.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.3.0.2.0.8._.0.4.0.4.1.9._.2.0.7...e.t.l.....P.P.....{..... .....

C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe (copy)

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12343296
Entropy (8bit):	3.4208454596549234
Encrypted:	false
SSDEEP:	6144:4JMjbyLY3DuTsP8d2nQO0o7MFGU15Ts+XAW:4JMjbyM3DW8qQa5TsV
MD5:	D83D3102AEE8419201BF810DE2A41992
SHA1:	30EC9FD8B35C5FEC5366FE52C7BF77E57A0C67A2
SHA-256:	4F8B000276DE586232FC912CDB72B497C305E8E13A8DEF72D3A2B0BA2FB7E0C9
SHA-512:	F3E9CEF20B8751716F1426DCACDA675F2672F60FF55218CB4A9BEC141A736D2B12E8761BCFC7115CD5F46DF3E5A83F3D399BD110EF37000F31EAEABDAE3BD CA2
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w...a.....q.....t....Rich.....PE.. L.....a.....>.....or.....@.....I...P.....@.....p9..@.....text... ....`.data...0.....8.....@....rsrc..... .....@..@.reloc..n'.....x.....@..B..... ....

\Device\ConDrv

Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3773
Entropy (8bit):	4.7109073551842435
Encrypted:	false
SSDEEP:	48:VHILZNfrI7WFY32iIiNOmV/HToZV9It199hiALIIg39bWA1RvTBi/g2eB:VoLr0y9iIiNOoHTou7bhBIIydWALLt2w
MD5:	DA3247A302D70819F10BCEEBAF400503
SHA1:	2857AA198EE76C86FC929CC3388A56D5FD051844
SHA-256:	5262E1EE394F329CD1F87EA31BA4A396C4A76EDC3A87612A179F81F21606ABC8
SHA-512:	48FFEC059B4E88F21C2AA4049B7D9E303C0C93D1AD771E405827149EDDF986A72EF49C0F6D8B70F5839DCDBD6B1EA8125C8B300134B7F71C47702B577AD090 8
Malicious:	false
Preview:	..A specified value is not valid.....Usage: add rule name=<string>.. dir=in|out.. action=allow|block|bypass.. [program=<program path>].. [service=<service short name>|any].. [description=<string>].. [enable=yes|no (default=yes)].. [profile=public|private|domain|any[,...]].. [localip=any|<IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [remoteip=any|localsubnet|dns|dhcp|wins|defaultgateway|.. <IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [localport=0-65535|<port range>[,...]|RPC|RPC-EPMap|IPHTTPS|any (default=any)].. [remoteport=0-65535|<port range>[,...]|any (default=any)].. [protocol=0-255|icmpv4|icmpv6|icmpv4:type,code|icmpv6:type,code|.. tcp|udp|any (default=any)].. [interfacetype=wireless|lan|ras|any].. [rmtcomputergrp=<SDDL string>].. [rmtusrgrp=<SDDL string>].. [edge=yes|deferapp|deferuser|no (default=no)].. [security=authenticate|authenc|authdynenc|authnoencap|

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.033590531786374
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	198656
MD5:	546a040e4479958f7c6b862dead9a269
SHA1:	69a99c8f2fbfc316140690be348d6b54d6c01d7d
SHA256:	229d8701db31564e7eccab699121e96fe75d70896daa87323e9c59da3be74be0
SHA512:	459623eced397b36d3bbb5fa01d78789a172f16c72bffaa58f7ffda59ce3378f2c5a4c8e4c7f1a3864ac6469c0c3e51b5cab21ed10f22d2c379e5bb893a84f0b
SSDEEP:	6144:1JMjbyLY3DuTsP8d2nQO0o7MFGU15Ts+XAW:1JMjbyM3DW8qQa5TsV
TLSH:	8F14CF323A90C072C17B15745C64DAA56BBEB83046B9C9BB776807BE4F306D1523A37B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w.....a.....q.....t.....Rich.....PE..L.....a.....

File Icon

Icon Hash:	70d0eeeacacaeadd

Static PE Info

General

Entrypoint:	0x40726f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x61B896C8 [Tue Dec 14 13:06:16 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	87e1f4e32d01d5a52e605f27fd138118

Entrypoint Preview

Instruction
call 00007F13A86C951Ch
jmp 00007F13A86C2E8Eh
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F13A86C3036h

Instruction
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F13A86C3060h
test ecx, 00000003h
jne 00007F13A86C3001h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F13A86C2FFAh
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F13A86C3044h
test ah, ah
je 00007F13A86C3036h
test eax, 00FF0000h
je 00007F13A86C3025h
test eax, FF000000h
je 00007F13A86C3014h
jmp 00007F13A86C2FDFh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
cmp ecx, dword ptr [0042C320h]
jne 00007F13A86C3014h
rep ret
jmp 00007F13A86C950Ch
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [0042C320h]

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1876c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x15a000	0x1ee8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x15c000	0xf10	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1240	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3970	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1f4	.text
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	0x1831a	0x18400	False	0.5320050740979382	data	6.368267998766109	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x13f430	0x13800	False	0.9405548878205128	data	7.828510878154685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x15a000	0x1ee8	0x2000	False	0.6080322265625	data	5.762900764852552	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x15c000	0x276e	0x2800	False	0.32080078125	data	3.3362844081949086	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x15a1c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Tibetan	Tibet
RT_ICON	0x15a1c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Tibetan	Nepal
RT_ICON	0x15a1c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Tibetan	India
RT_ICON	0x15aa68	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Tibetan	Tibet
RT_ICON	0x15aa68	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Tibetan	Nepal
RT_ICON	0x15aa68	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Tibetan	India
RT_STRING	0x15bd90	0x4e	data	Tibetan	Tibet
RT_STRING	0x15bd90	0x4e	data	Tibetan	Nepal
RT_STRING	0x15bd90	0x4e	data	Tibetan	India
RT_STRING	0x15bde0	0x50	data	Tibetan	Tibet
RT_STRING	0x15bde0	0x50	data	Tibetan	Nepal
RT_STRING	0x15bde0	0x50	data	Tibetan	India
RT_STRING	0x15be30	0xb6	data	Tibetan	Tibet
RT_STRING	0x15be30	0xb6	data	Tibetan	Nepal
RT_STRING	0x15be30	0xb6	data	Tibetan	India

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0x15bb10	0x22	data	Tibetan	Tibet
RT_GROUP_ICON	0x15bb10	0x22	data	Tibetan	Nepal
RT_GROUP_ICON	0x15bb10	0x22	data	Tibetan	India
RT_VERSION	0x15bb38	0x258	data		

Imports

DLL	Import
KERNEL32.dll	RequestWakeupLatency, CreateFileA, FindActCtxSectionStringA, WriteConsoleInputA, ClearCommBreak, WriteFile, FindFirstVolumeMountPointW, CreateDirectoryExA, LocalSize, WaitForMultipleObjects, ReadConsoleInputA, GetProcessId, FreeUserPhysicalPages, WriteConsoleOutputAttribute, DebugActiveProcessStop, GetLocaleInfoW, GetProcAddress, LocalAlloc, GetCommandLineW, GetBinaryTypeW, InterlockedExchange, OpenMutexW, GetConsoleTitleA, SearchPathA, FreeConsole, EndUpdateResourceA, GetLastError, GetProfileSectionA, SetConsoleCursorInfo, GetConsoleAliasW, CreateSemaphoreA, GlobalFlags, GetConsoleAliasesLengthA, FindResourceW, SetVolumeMountPointW, GetModuleHandleW, HeapAlloc, GetComputerNameA, GetCurrentProcessId, CreateNamedPipeA, EnumResourceLanguagesA, SetHandleInformation, _hwrite, CreateActCtxA, DeleteVolumeMountPointA, MoveFileWithProgressA, AddRefActCtx, WritePrivateProfileStringA, GetUserDefaultLangID, QueryMemoryResourceNotification, WaitForSingleObject, GetLongPathNameW, InterlockedDecrement, VerifyVersionInfoA, EnumCalendarInfoW, FindNextFileW, EnumTimeFormatsA, SetLastError, SetCriticalSectionSpinCount, WritePrivateProfileSectionA, LoadLibraryA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RaiseException, RtlUnwind, HeapFree, DeleteFileA, GetStartupInfoW, GetModuleHandleA, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, HeapCreate, VirtualFree, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, VirtualAlloc, HeapReAlloc, Sleep, ExitProcess, GetStdHandle, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, GetStartupInfoA, QueryPerformanceCounter, GetTickCount, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, HeapSize, InitializeCriticalSectionAndSpinCount, WideCharToMultiByte, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, GetConsoleCP, GetConsoleMode, FlushFileBuffers, SetFilePointer, CloseHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetStdHandle
USER32.dll	GetComboBoxInfo
GDI32.dll	GetTextFaceW

Possible Origin

Language of compilation system	Country where language is spoken	Map
Tibetan	Tibet	
Tibetan	Nepal	
Tibetan	India	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8569245 32023883 02/07/23-20:05:14.210188	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	56924	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8523875 32023883 02/07/23-20:04:33.939091	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	52387	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8606255 32023883 02/07/23-20:05:54.726769	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	60625	53	192.168.2.3	8.8.8.8

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 20:04:31.294190884 CET	49703	25	192.168.2.3	104.47.54.36
Feb 7, 2023 20:04:31.428320885 CET	25	49703	104.47.54.36	192.168.2.3
Feb 7, 2023 20:04:31.428772926 CET	49703	25	192.168.2.3	104.47.54.36
Feb 7, 2023 20:04:31.429225922 CET	49703	25	192.168.2.3	104.47.54.36
Feb 7, 2023 20:04:31.562918901 CET	25	49703	104.47.54.36	192.168.2.3
Feb 7, 2023 20:04:31.565531969 CET	25	49703	104.47.54.36	192.168.2.3
Feb 7, 2023 20:04:31.565643072 CET	49703	25	192.168.2.3	104.47.54.36
Feb 7, 2023 20:04:31.566819906 CET	25	49703	104.47.54.36	192.168.2.3
Feb 7, 2023 20:04:31.566896915 CET	49703	25	192.168.2.3	104.47.54.36
Feb 7, 2023 20:04:34.049882889 CET	49704	443	192.168.2.3	176.124.192.220
Feb 7, 2023 20:04:34.049942017 CET	443	49704	176.124.192.220	192.168.2.3
Feb 7, 2023 20:04:34.050019979 CET	49704	443	192.168.2.3	176.124.192.220
Feb 7, 2023 20:05:14.064105988 CET	49704	443	192.168.2.3	176.124.192.220
Feb 7, 2023 20:05:14.064233065 CET	443	49704	176.124.192.220	192.168.2.3
Feb 7, 2023 20:05:14.064335108 CET	49704	443	192.168.2.3	176.124.192.220
Feb 7, 2023 20:05:14.562938929 CET	49705	443	192.168.2.3	176.124.192.220
Feb 7, 2023 20:05:14.562999964 CET	443	49705	176.124.192.220	192.168.2.3
Feb 7, 2023 20:05:14.563118935 CET	49705	443	192.168.2.3	176.124.192.220
Feb 7, 2023 20:05:54.581402063 CET	49705	443	192.168.2.3	176.124.192.220
Feb 7, 2023 20:05:54.581485033 CET	443	49705	176.124.192.220	192.168.2.3
Feb 7, 2023 20:05:54.581589937 CET	49705	443	192.168.2.3	176.124.192.220
Feb 7, 2023 20:05:55.068969965 CET	49706	443	192.168.2.3	176.124.192.220
Feb 7, 2023 20:05:55.069030046 CET	443	49706	176.124.192.220	192.168.2.3
Feb 7, 2023 20:05:55.069097042 CET	49706	443	192.168.2.3	176.124.192.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 20:04:31.258358002 CET	57990	53	192.168.2.3	8.8.8.8
Feb 7, 2023 20:04:31.288695097 CET	53	57990	8.8.8.8	192.168.2.3
Feb 7, 2023 20:04:33.939090967 CET	52387	53	192.168.2.3	8.8.8.8
Feb 7, 2023 20:04:34.046056986 CET	53	52387	8.8.8.8	192.168.2.3
Feb 7, 2023 20:05:14.210187912 CET	56924	53	192.168.2.3	8.8.8.8
Feb 7, 2023 20:05:14.561336040 CET	53	56924	8.8.8.8	192.168.2.3
Feb 7, 2023 20:05:54.726768970 CET	60625	53	192.168.2.3	8.8.8.8
Feb 7, 2023 20:05:55.066458941 CET	53	60625	8.8.8.8	192.168.2.3
Feb 7, 2023 20:06:14.241579056 CET	51139	53	192.168.2.3	8.8.8.8
Feb 7, 2023 20:06:14.387082100 CET	53	51139	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 20:04:31.258358002 CET	192.168.2.3	8.8.8.8	0x9480	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:04:33.939090967 CET	192.168.2.3	8.8.8.8	0xfd45	Standard query (0)	svartalfheim.top	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:14.210187912 CET	192.168.2.3	8.8.8.8	0x9585	Standard query (0)	svartalfheim.top	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:54.726768970 CET	192.168.2.3	8.8.8.8	0xc103	Standard query (0)	svartalfheim.top	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:06:14.241579056 CET	192.168.2.3	8.8.8.8	0x64c0	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)	false

DNS Answers

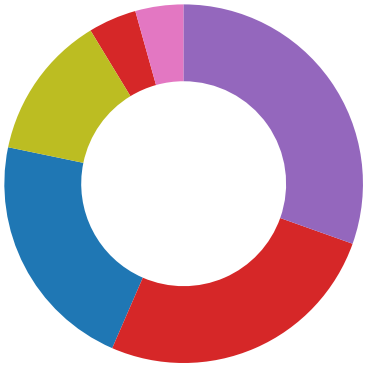
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 20:04:31.288695097 CET	8.8.8.8	192.168.2.3	0x9480	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:04:31.288695097 CET	8.8.8.8	192.168.2.3	0x9480	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:04:31.288695097 CET	8.8.8.8	192.168.2.3	0x9480	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.40.29	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:04:31.288695097 CET	8.8.8.8	192.168.2.3	0x9480	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.2	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:04:31.288695097 CET	8.8.8.8	192.168.2.3	0x9480	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:04:34.046056986 CET	8.8.8.8	192.168.2.3	0xfd45	No error (0)	svartalfheim.top		176.124.192.220	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:14.561336040 CET	8.8.8.8	192.168.2.3	0x9585	No error (0)	svartalfheim.top		176.124.192.220	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:55.066458941 CET	8.8.8.8	192.168.2.3	0xc103	No error (0)	svartalfheim.top		176.124.192.220	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:06:14.387082100 CET	8.8.8.8	192.168.2.3	0x64c0	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.2	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:06:14.387082100 CET	8.8.8.8	192.168.2.3	0x64c0	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:06:14.387082100 CET	8.8.8.8	192.168.2.3	0x64c0	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:06:14.387082100 CET	8.8.8.8	192.168.2.3	0x64c0	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:06:14.387082100 CET	8.8.8.8	192.168.2.3	0x64c0	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.40.29	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 7, 2023 20:04:31.565531969 CET	25	49703	104.47.54.36	192.168.2.3	220 DM3NAM06FT007.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Tue, 7 Feb 2023 19:04:30 +0000

Statistics

Behavior



- file.exe
- svchost.exe
- svchost.exe
- cmd.exe
- conhost.exe
- svchost.exe
- cmd.exe
- conhost.exe
- svchost.exe
- sc.exe
- conhost.exe
- svchost.exe
- sc.exe
- conhost.exe
- SgrmBroker.exe
- sc.exe
- conhost.exe
- qbxctmyn.exe
- netsh.exe
- conhost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: file.exe PID: **5128**, Parent PID: **3452**

General

Target ID:	0
Start time:	20:04:09
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	198656 bytes
MD5 hash:	546A040E4479958F7C6B862DEAD9A269
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000000.00000002.289443639.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 00000000.00000002.289443639.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000000.00000002.289443639.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.290625632.00000000007B6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000000.00000002.292424042.0000000002080000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.292424042.0000000002080000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000000.00000002.292424042.0000000002080000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000000.00000003.279056535.00000000021C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 00000000.00000003.279056535.00000000021C0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000000.00000003.279056535.00000000021C0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: svchost.exe PID: **6120**, Parent PID: **580**

General

Target ID:	1
Start time:	20:04:17
Start date:	07/02/2023
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
Reputation:	high

Analysis Process: svchost.exe PID: **3592**, Parent PID: **580**

General

Target ID:	2
Start time:	20:04:17
Start date:	07/02/2023
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
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3076, Parent PID: 5128

General

Target ID:	3
Start time:	20:04:17
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\htdzdeug\
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\htdzdeug\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	BBFE7	CreateDirectoryW

Analysis Process: conhost.exe PID: 3176, Parent PID: 3076

General

Target ID:	4
Start time:	20:04:17
Start date:	07/02/2023
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: svchost.exe PID: 5064, Parent PID: 580

General

Target ID:	5
Start time:	20:04:18
Start date:	07/02/2023
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
Reputation:	high

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: cmd.exe PID: 2432, Parent PID: 5128

General

Target ID:	6
Start time:	20:04:18
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\qbxctmyn.exe" C:\Windows\SysWOW64\htdzdeug\
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qbxctmyn.exe	C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe	success or wait	1	BB966	MoveFileExW

Analysis Process: conhost.exe PID: 5260, Parent PID: 2432

General

Target ID:	7
Start time:	20:04:18
Start date:	07/02/2023
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

Analysis Process: svchost.exe PID: 5400, Parent PID: 580

General

Target ID:	8
Start time:	20:04:18
Start date:	07/02/2023
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: sc.exe PID: **1020**, Parent PID: **5128**

General

Target ID:	9
Start time:	20:04:19
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create htdzdeug binPath= "C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe /d\"C:\Users\user\Desktop\file.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0xca0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
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

Analysis Process: conhost.exe PID: **5036**, Parent PID: **1020**

General

Target ID:	10
Start time:	20:04:19
Start date:	07/02/2023
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

Analysis Process: svchost.exe PID: **1764**, Parent PID: **580**

General	
Target ID:	11
Start time:	20:04:19
Start date:	07/02/2023
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: sc.exe PID: **5828**, Parent PID: **5128**

General	
Target ID:	12
Start time:	20:04:19
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description htdzdeug "wifi internet conection
Imagebase:	0xca0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
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

Analysis Process: conhost.exe PID: **5800**, Parent PID: **5828**

General	
Target ID:	13
Start time:	20:04:19
Start date:	07/02/2023
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

Analysis Process: SgrmBroker.exe PID: **1652**, Parent PID: **580**

General

Target ID:	14
Start time:	20:04:20
Start date:	07/02/2023
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6d1310000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **3108**, Parent PID: **5128**

General

Target ID:	15
Start time:	20:04:20
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start htdzdeug
Imagebase:	0xca0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
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

Analysis Process: conhost.exe PID: **4952**, Parent PID: **3108**

General

Target ID:	16
Start time:	20:04:20
Start date:	07/02/2023
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

Analysis Process: qbxctmyn.exe PID: **4532**, Parent PID: **580**

General

Target ID:	17
Start time:	20:04:20
Start date:	07/02/2023

Path:	C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe /d"C:\Users\user\Desktop\file.exe"
Imagebase:	0x400000
File size:	12343296 bytes
MD5 hash:	D83D3102AEE8419201BF810DE2A41992
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000011.00000002.310301101.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 00000011.00000002.310301101.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000011.00000002.310301101.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000011.00000002.310875987.0000000000E30000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000011.00000002.310875987.0000000000E30000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000011.00000002.310875987.0000000000E30000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000011.00000002.310889841.0000000000E90000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 00000011.00000002.310889841.0000000000E90000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000011.00000002.310889841.0000000000E90000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000011.00000002.310684388.00000000005B1000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000011.00000003.309369013.0000000000E50000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 00000011.00000003.309369013.0000000000E50000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000011.00000003.309369013.0000000000E50000.00000004.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: netsh.exe PID: **5864**, Parent PID: **5128**

General

Target ID:	18
Start time:	20:04:20
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x10f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
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
\Device\ConDrv	35	35	0d 0a 55 73 61 67 65 3a 20 61 64 64 20 72 75 6c 65 20 6e 61 6d 65 3d 3c 73 74 72 69 6e 67 3e 0d 0a 20 20	Usage: add rule name= <string>	success or wait	1	10F7B1B	WriteFile
\Device\ConDrv	3771	3736	0d 0a		success or wait	1	10F7B1B	WriteFile
\Device\ConDrv	3773	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	10F7B1B	WriteFile

Analysis Process: conhost.exe PID: **4844**, Parent PID: **5864**

General	
Target ID:	19
Start time:	20:04:21
Start date:	07/02/2023
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

Analysis Process: svchost.exe PID: **1328**, Parent PID: **580**

General	
Target ID:	20
Start time:	20:04:22
Start date:	07/02/2023
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: **2140**, Parent PID: **580**

General	
Target ID:	21

Start time:	20:04:27
Start date:	07/02/2023
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: **4204**, Parent PID: **580**

General

Target ID:	22
Start time:	20:04:27
Start date:	07/02/2023
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: svchost.exe PID: **2888**, Parent PID: **4532**

General

Target ID:	23
Start time:	20:04:30
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0xe40000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000017.00000002.530839656.0000000000120000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 00000017.00000002.530839656.0000000000120000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000017.00000002.530839656.0000000000120000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	12A409	DeleteFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe	unknown	64	success or wait	1	126809	ReadFile
C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe	unknown	248	success or wait	1	126840	ReadFile
C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe	unknown	64	success or wait	10	126809	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\SysWOW64\htdzdeug	dword	0	success or wait	1	128447	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\htdzdeug	ImagePath	expand unicode	C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe /d"C:\Users\user\Desktop\file.exe"	C:\Windows\SysWOW64\htdzdeug\qbxctmyn.exe	success or wait	1	127D50	RegSetValueExA

Analysis Process: MpCmdRun.exe PID: **612**, Parent PID: **2140**

General

Target ID:	24
Start time:	20:05:29
Start date:	07/02/2023
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff6856c0000
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

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 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	------------------------------------- ------------------------------------- -----------	success or wait	1	7FF6856EBC96	WriteFile
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 75 00 65 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 30 00 37 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 32 00 30 00 3a 00 30 00 35 00 3a 00 32 00 39 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Tue Feb 07 2023 20:05 :29	success or wait	1	7FF6856EBC96	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	7FF6856EBC96	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	7FF6856EBC96	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	7FF6856EBC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 75 00 65 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 30 00 37 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 32 00 30 00 3a 00 30 00 35 00 3a 00 32 00 39 00 0d 00 0a 00	MpCmdRun: End Time: Tue Feb 07 2023 20:05:29	success or wait	1	7FF6856EBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10700	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF6856EBC96	WriteFile

Analysis Process: conhost.exe PID: **1500**, Parent PID: **612**

General

Target ID:	25
Start time:	20:05:29
Start date:	07/02/2023
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