ID: 780217
Sample Name: file.exe
Cookbook: default.jbs
Time: 16:13:30
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

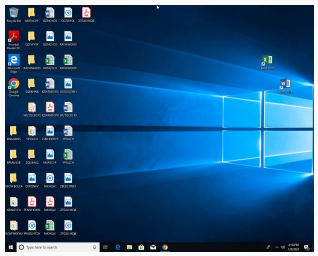
Windows Analysis Report

file.exe

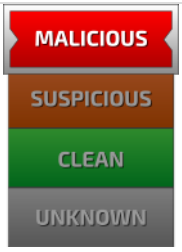
Overview

General Information

Sample Name:	file.exe
Analysis ID:	780217
MD5:	4c085e942806b5..
SHA1:	208d04b2528058.
SHA256:	283b0f136d2696..
Tags:	exe
Infos:	



Detection



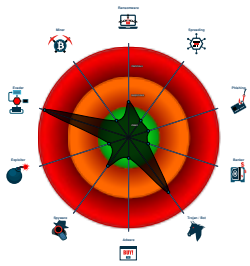
Tofsee

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- System process connects to networ…
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for dom…
- Yara detected Tofsee
- Snort IDS alert for network traffic
- Uses netsh to modify the Windows …
- Writes to foreign memory regions
- Found API chain indicative of debug…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 4516 cmdline: C:\Users\user\Desktop\file.exe MD5: 4C085E942806B5C8D972695451AA8F48)
  - cmd.exe (PID: 5252 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\tsqtjgfo\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 2824 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\qtcnnjjg.exe" C:\Windows\SysWOW64\tsqtjgfo\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 2328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 1352 cmdline: C:\Windows\System32\sc.exe" create tsqtjgfo binPath= "C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe /d\"C:\Users\user\Desktop\file.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
    - conhost.exe (PID: 1348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 5936 cmdline: C:\Windows\System32\sc.exe" description tsqtjgfo "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
    - conhost.exe (PID: 4696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 5228 cmdline: "C:\Windows\System32\sc.exe" start tsqtjgfo MD5: 24A3E2603E63BCB9695A2935D3B24695)
    - conhost.exe (PID: 5020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - netsh.exe (PID: 3648 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: 4352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- qtcnnjjg.exe (PID: 5940 cmdline: C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe /d"C:\Users\user\Desktop\file.exe" MD5: 3D0E87BA5B0B7BA4C2F68898214F5106)
  - svchost.exe (PID: 3232 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- **cleanup**

Malware Configuration

Threatname: Tofsee

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

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.344749194.0000000002DA8000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x2800:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.342422923.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000000.00000002.342422923.0000000000400000.00000040.00000001.01000000.00000003.sdmp	MALWARE_Win_Tofsee	Detects Tofsee	ditekSHen	• 0x1123e:$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
00000000.00000002.342422923.0000000000400000.00000040.00000001.01000000.00000003.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 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
00000000.00000002.344302410.0000000002D20000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	

Click to see the 24 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.file.exe.2d40000.0.unpack	MALWARE_Win_Tofsee	Detects Tofsee	ditekSHen	• 0xe110:$s2: loader_id • 0xe140:$s3: start_srv • 0xe170:$s4: lid_file_upd • 0xe164:$s5: localcfg • 0xe894:$s6: Incorrect respons
0.3.file.exe.2d40000.0.unpack	Windows_Trojan_Tofsee_26124fe4	unknown	unknown	• 0xd44:$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:$b: 8B 44 24 04 53 8A 18 84 DB 74 2D 8B D0 2B 54 24 0C 8B 4C 24 0C 84 DB 74 12 8A 19 84 DB 74 1B 38 1C 0A 75 07 41 80 3C 0A 00 75 EE 80 39 00 74 0A 40 8A 18 42 84 DB 75 D9 33 C0 5B C3
0.2.file.exe.2d20e67.1.unpack	MALWARE_Win_Tofsee	Detects Tofsee	ditekSHen	• 0xe110:$s2: loader_id • 0xe140:$s3: start_srv • 0xe170:$s4: lid_file_upd • 0xe164:$s5: localcfg • 0xe894:$s6: Incorrect respons
0.2.file.exe.2d20e67.1.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
11.2.qtcnnjjg.exe.400000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	

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: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.851441532023883 01/08/23-16:14:55.286794
SID:	2023883
Source Port:	51441
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.863446532023883 01/08/23-16:15:35.449008
SID:	2023883
Source Port:	63446
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.856682532023883 01/08/23-16:16:57.387452
SID:	2023883
Source Port:	56682
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.859220532023883 01/08/23-16:16:15.738842
SID:	2023883
Source Port:	59220
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.862659532023883 01/08/23-16:17:37.662206
SID:	2023883
Source Port:	62659
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

AV Detection

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

Anti Debugging

Found API chain indicative of debugger detection

HIPS / PFW / Operating System Protection Evasion

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

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information

Yara detected Tofsee

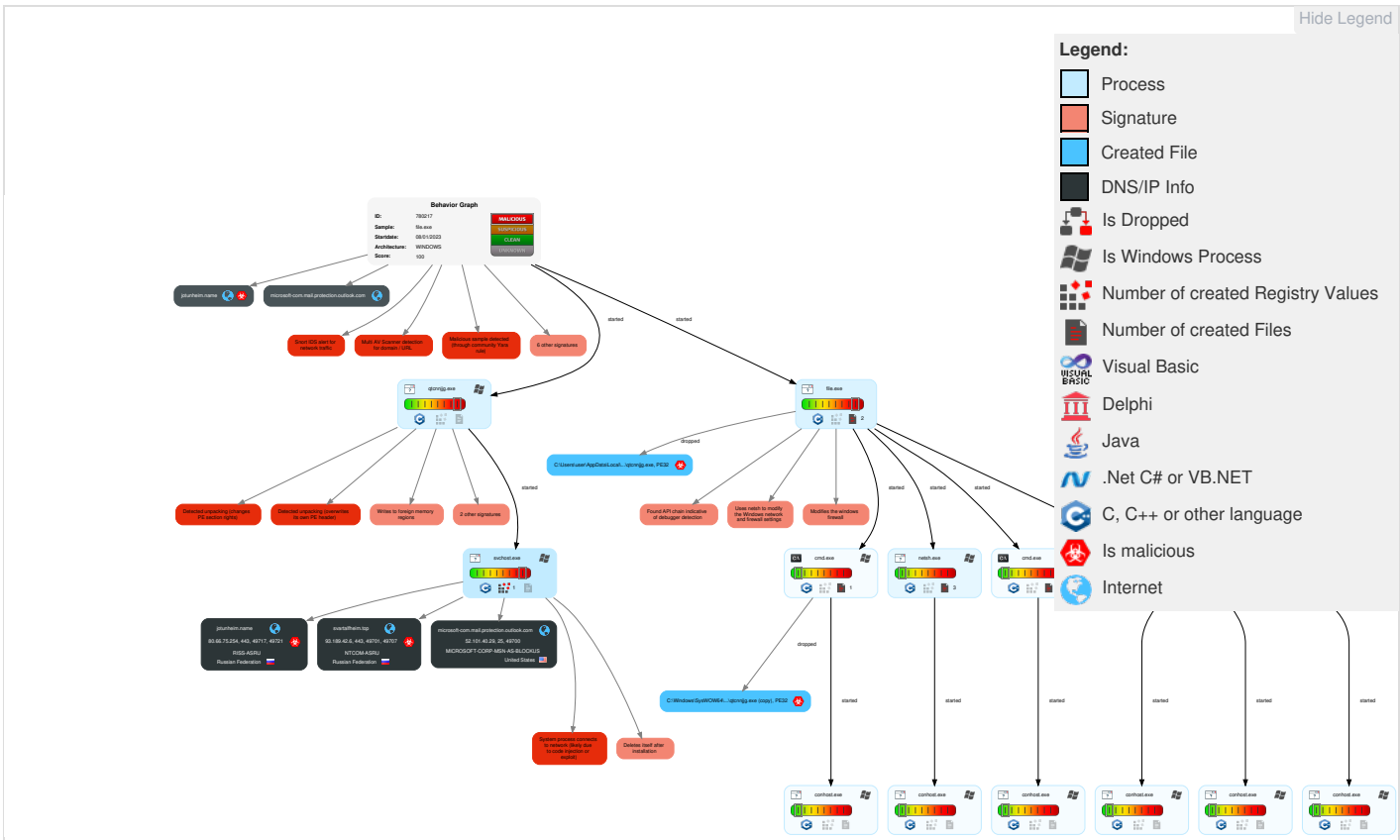
Remote Access Functionality

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	4 1 Native API	1 Valid Accounts	1 Valid Accounts	2 Disable or Modify Tools	OS Credential Dumping	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	2 Command and Scripting Interpreter	1 4 Windows Service	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	3 Service Execution	Logon Script (Windows)	1 4 Windows Service	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	At (Windows)	Logon Script (Mac)	4 1 2 Process Injection	2 1 Software Packing	NTDS	1 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	Network Logon Script	1 File Deletion	LSA Secrets	1 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 2 Masquerading	Cached Domain Credentials	1 1 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 Valid Accounts	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 1 Virtualization/Sandbox Evasion	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 Access Token Manipulation	/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)	4 1 2 Process Injection	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

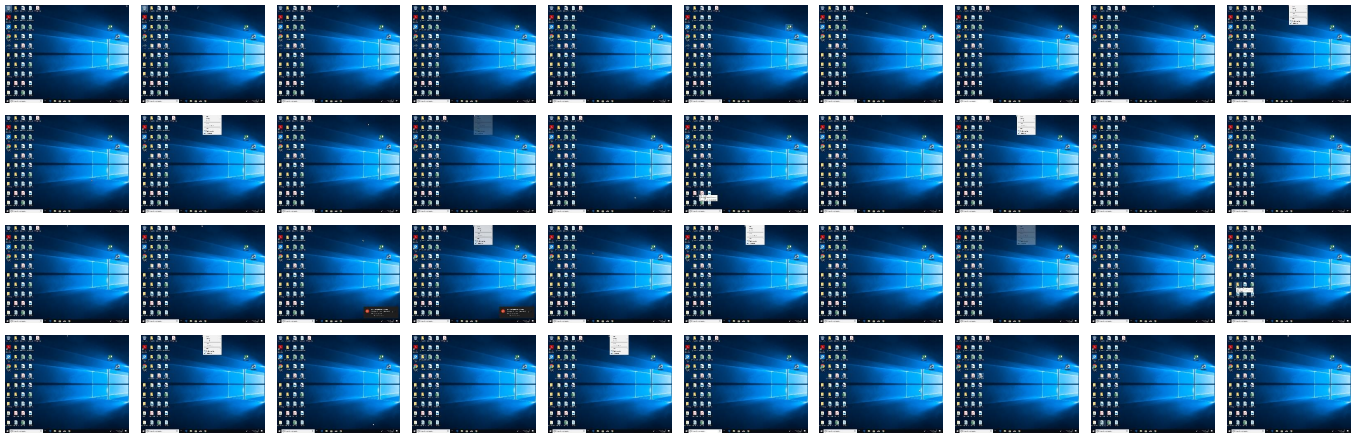
Behavior Graph



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	46%	ReversingLabs	Win32.Backdoor.Convagent	
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\qtcnnjjg.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.file.exe.2d40000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.svchost.exe.84b000.1.unpack	100%	Avira	HEUR/AGEN.1253311		Download File
11.2.qtcnnjjg.exe.2c40e67.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.svchost.exe.84b000.2.unpack	100%	Avira	HEUR/AGEN.1253311		Download File
0.2.file.exe.2d20e67.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.qtcnnjjg.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
14.2.svchost.exe.4d0000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
11.2.qtcnnjjg.exe.2da0000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
11.3.qtcnnjjg.exe.2d40000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
svartalfheim.top	17%	Virustotal		Browse
jotunheim.name	16%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
svartalfheim.top:443	0%	URL Reputation	safe	
svartalfheim.top:443	0%	URL Reputation	safe	
jotunheim.name:443	0%	URL Reputation	safe	

Domains and IPs

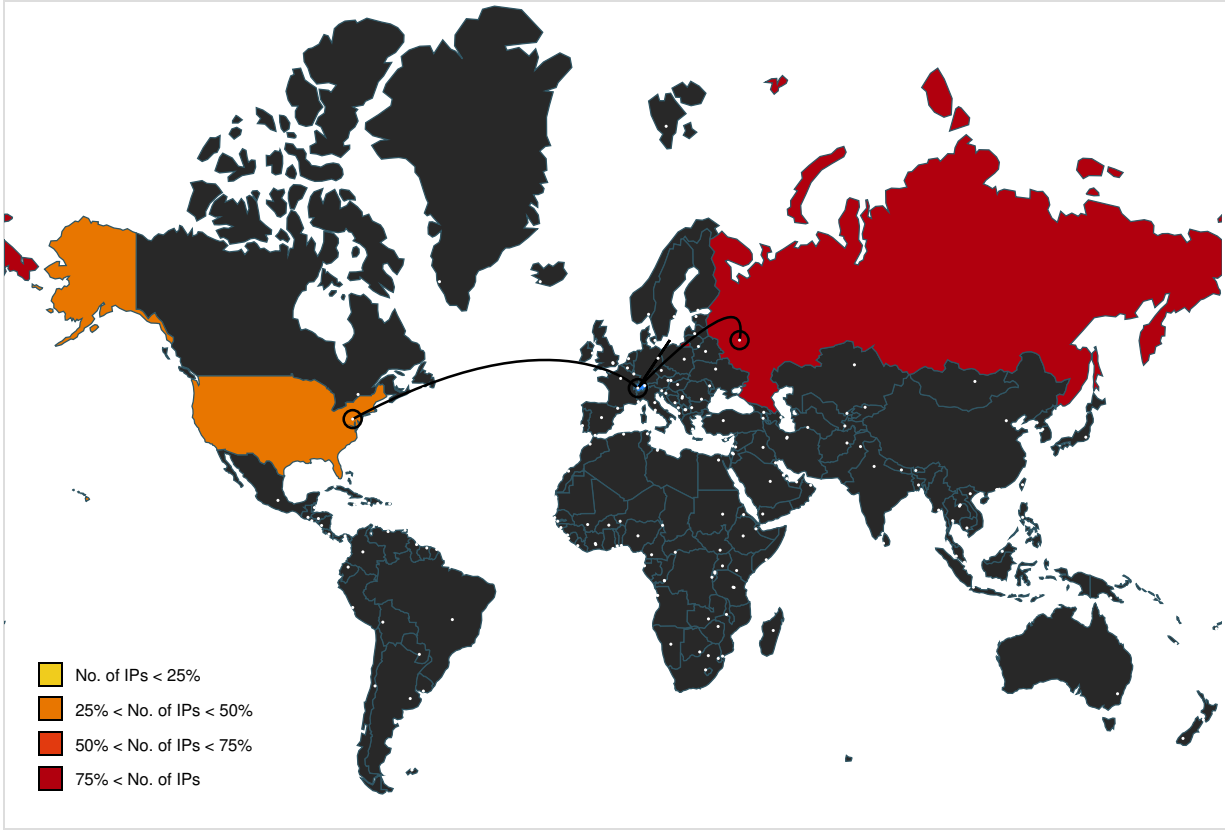
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
svartalfheim.top	93.189.42.6	true	true	• 17%, Virustotal, Browse	unknown
jotunheim.name	80.66.75.254	true	true	• 16%, Virustotal, Browse	unknown
microsoft-com.mail.protection.outlook.com	52.101.40.29	true	false		high

Contacted URLs

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

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.66.75.254	jotunheim.name	Russian Federation		20803	RISS-ASRU	true
93.189.42.6	svartalfheim.top	Russian Federation		41853	NTCOM-ASRU	true
52.101.40.29	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:	780217
Start date and time:	2023-01-08 16:13:30 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@22/3@9/3
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 61.9% (good quality ratio 59%) • Quality average: 86.9% • Quality standard deviation: 25.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, conhost.exe
- 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, 40.126.32.75, 20.190.160.23, 20.190.160.12, 20.190.160.21, 20.190.160.15, 40.126.32.73, 40.126.32.132, 40.126.32.67, 40.127.240.158, 20.73.194.208
- Excluded domains from analysis (whitelisted): client.wns.windows.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, prda.aadg.msidentity.com, atm-settingsfe-prod-geo2.trafficmanager.net, login.live.com, settings-prod-weu-2.westeurope.cloudapp.azure.com, settings-prod-neu-1.northeurope.cloudapp.azure.com, microsoft.com, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior 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
16:15:35	API Interceptor	5x Sleep call for process: svchost.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:\Users\user\AppData\Local\Temp\qtcnnjjg.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	15645184

Entropy (8bit):	5.291152040640698
Encrypted:	false
SSDEEP:	49152:FZsrgsLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL:FZsr
MD5:	3D0E87BA5B0B7BA4C2F68898214F5106
SHA1:	8BFFC54A6633126CFA4118B382E4C3A3F63A432A
SHA-256:	010FDCDEE7594911E51CFCBFAA6DEACB3F8306A20537FF3F11F9DFC41BB0FA72
SHA-512:	7A9C495FC0AC66D68E553A9090B6B61E59864DB3FC75477C44B85CD582B93DCDC859CA74B5D015B1E7C3988E97CD3430B84E5D3FB6082EBDEE608D2C76041 EE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........u...............................x`.........1.....................Rich....................P E..L...?Qia.................z...py......_............@...........................z.............................................}..P.....y..`.......................... ....C..@.................................... ....text...fx.......z.................. ..`.data....vw..........~..............@....rsrc...`.....y..".................@..@.. ....

C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe (copy)

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	15645184
Entropy (8bit):	5.291152040640698
Encrypted:	false
SSDEEP:	49152:FZsrgsLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL:FZsr
MD5:	3D0E87BA5B0B7BA4C2F68898214F5106
SHA1:	8BFFC54A6633126CFA4118B382E4C3A3F63A432A
SHA-256:	010FDCDEE7594911E51CFCBFAA6DEACB3F8306A20537FF3F11F9DFC41BB0FA72
SHA-512:	7A9C495FC0AC66D68E553A9090B6B61E59864DB3FC75477C44B85CD582B93DCDC859CA74B5D015B1E7C3988E97CD3430B84E5D3FB6082EBDEE608D2C76041 EE
Malicious:	**true**
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........u...............................x`.........1.....................Rich....................P E..L...?Qia.................z...py......_............@...........................z.............................................}..P.....y..`.......................... ....C..@.................................... ....text...fx.......z.................. ..`.data....vw..........~..............@....rsrc...`.....y..".................@..@.. ....

\Device\ConDrv

<table>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\netsh.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>3773</td></tr>
<tr><td>Entropy (8bit):</td><td>4.7109073551842435</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>48:VHILZNfrI7WFY32iIiNOmV/HToZV9It199hiALlIg39bWA1RvTBi/g2eB:VoLr0y9iIiNOoHTou7bhBIlydWALLt2w</td></tr>
<tr><td>MD5:</td><td>DA3247A302D70819F10BCEEBAF400503</td></tr>
<tr><td>SHA1:</td><td>2857AA198EE76C86FC929CC3388A56D5FD051844</td></tr>
<tr><td>SHA-256:</td><td>5262E1EE394F329CD1F87EA31BA4A396C4A76EDC3A87612A179F81F21606ABC8</td></tr>
<tr><td>SHA-512:</td><td>48FFEC059B4E88F21C2AA4049B7D9E303C0C93D1AD771E405827149EDDF986A72EF49C0F6D8B70F5839DCDBD6B1EA8125C8B300134B7F71C47702B577AD090 8</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>..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 a ddress>|<subnet>|<range>|<list>].. [remoteip=any|localsubnet|dns|dhcp|wins|defaultgateway|.. <IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [l ocalport=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|</td></tr>
</table>

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.575762280828874

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:	269824
MD5:	4c085e942806b5c8d972695451aa8f48
SHA1:	208d04b2528058609221c87cf1272d420099c493
SHA256:	283b0f136d26968786e7a0abe1354758de4cdade534ddee63b93569c282f2299
SHA512:	71711540d02295de9afd3f5f9a2e1affcade41bf09e91f30da6674c2f3e1b610cb3b723a6d46605b5eb1975523d108282c5f68d6ac01eff19974ab972768b9fd
SSDEEP:	3072:EXhfi0CLr5NToLP0S5/NvXVarnGlEzSCdx4q5ofB9bjXpxOYDUZNTKXWPr0sd6:AkLrwLP0OqnOgSCdxpuZFjXTlOuN
TLSH:	12448C313693CC72C156E57099259AF8EFB6BC739B2489C327443B6E6E702D39272712
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.....x`.....1.....Rich.....PE..L...?Qia.....

File Icon

Icon Hash:	9062e098c6e73144

Static PE Info

General

Entrypoint:	0x405fbf
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6169513F [Fri Oct 15 10:00:31 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:	b49d1773872141620d6e88f1989600b7

Entrypoint Preview

Instruction
call 00007FF854CD7ED8h
jmp 00007FF854CD1C4Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov esi, ecx
mov byte ptr [esi+0Ch], 00000000h
test eax, eax
jne 00007FF854CD1E35h
call 00007FF854CD7BB5h
mov dword ptr [esi+08h], eax
mov ecx, dword ptr [eax+6Ch]
mov dword ptr [esi], ecx
mov ecx, dword ptr [eax+68h]
mov dword ptr [esi+04h], ecx

Instruction
mov ecx, dword ptr [esi]
cmp ecx, dword ptr [0042A118h]
je 00007FF854CD1DE4h
mov ecx, dword ptr [0042A034h]
test dword ptr [eax+70h], ecx
jne 00007FF854CD1DD9h
call 00007FF854CD88EBh
mov dword ptr [esi], eax
mov eax, dword ptr [esi+04h]
cmp eax, dword ptr [00429F38h]
je 00007FF854CD1DE8h
mov eax, dword ptr [esi+08h]
mov ecx, dword ptr [0042A034h]
test dword ptr [eax+70h], ecx
jne 00007FF854CD1DDAh
call 00007FF854CD815Fh
mov dword ptr [esi+04h], eax
mov eax, dword ptr [esi+08h]
test byte ptr [eax+70h], 00000002h
jne 00007FF854CD1DE6h
or dword ptr [eax+70h], 02h
mov byte ptr [esi+0Ch], 00000001h
jmp 00007FF854CD1DDCh
mov ecx, dword ptr [eax]
mov dword ptr [esi], ecx
mov eax, dword ptr [eax+04h]
mov dword ptr [esi+04h], eax
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 10h
push esi
push dword ptr [ebp+0Ch]
lea ecx, dword ptr [ebp-10h]
call 00007FF854CD1D3Ah
mov esi, dword ptr [ebp+08h]
movsx eax, byte ptr [esi]
push eax
call 00007FF854CD8B93h
cmp eax, 65h
jmp 00007FF854CD1DDEh
inc esi
movzx eax, byte ptr [esi]
push eax
call 00007FF854CD893Ch
test eax, eax
pop ecx
jne 00007FF854CD1DC3h
movsx eax, byte ptr [esi]

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	0x17dec	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2791000	0x18460	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	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	0x43b8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.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	0x17866	0x17a00	False	0.5360139715608465	OpenPGP Public Key	6.402318242015286	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x19000	0x27776b4	0x11a00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2791000	0x18460	0x18600	False	0.47464943910256413	data	5.261333907966325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x27a6b58	0x2	data		
AFX_DIALOG_LAYOUT	0x27a6b50	0x2	data		
AFX_DIALOG_LAYOUT	0x27a6b60	0x2	data		
AFX_DIALOG_LAYOUT	0x27a6b68	0x2	data		
AFX_DIALOG_LAYOUT	0x27a6b70	0x2	data		
RT_CURSOR	0x27a6b78	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x27a6cc0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x27a6df0	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		
RT_CURSOR	0x27a6ee0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_CURSOR	0x27a7fb8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x27919e0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x27920a8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x2792610	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x27936b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x2793b60	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Spanish	Venezuela

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2794a08	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Spanish	Venezuela
RT_ICON	0x27952b0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Spanish	Venezuela
RT_ICON	0x2795978	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Spanish	Venezuela
RT_ICON	0x2795ee0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Spanish	Venezuela
RT_ICON	0x2798488	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Spanish	Venezuela
RT_ICON	0x2799530	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Spanish	Venezuela
RT_ICON	0x2799eb8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Spanish	Venezuela
RT_ICON	0x279a398	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x279b240	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x279b908	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x279be70	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x279e418	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x279f4c0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x279fe48	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x27a0318	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Spanish	Venezuela
RT_ICON	0x27a11c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Spanish	Venezuela
RT_ICON	0x27a1a68	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Spanish	Venezuela
RT_ICON	0x27a2130	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Spanish	Venezuela
RT_ICON	0x27a2698	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Spanish	Venezuela
RT_ICON	0x27a4c40	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Spanish	Venezuela
RT_ICON	0x27a5ce8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Spanish	Venezuela
RT_ICON	0x27a6670	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Spanish	Venezuela
RT_STRING	0x27a89c8	0x38c	data	Spanish	Venezuela
RT_STRING	0x27a8d58	0x53c	data	Spanish	Venezuela
RT_STRING	0x27a9298	0x1c8	data	Spanish	Venezuela
RT_GROUP_CURSOR	0x27a6ca8	0x14	data		
RT_GROUP_CURSOR	0x27a8860	0x14	data		
RT_GROUP_CURSOR	0x27a7f88	0x30	data		
RT_GROUP_ICON	0x279a320	0x76	data	Spanish	Venezuela
RT_GROUP_ICON	0x2793b20	0x3e	data	Spanish	Venezuela
RT_GROUP_ICON	0x27a02b0	0x68	data	Spanish	Venezuela
RT_GROUP_ICON	0x27a6ad8	0x76	data	Spanish	Venezuela
RT_VERSION	0x27a8878	0x150	data		

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetModuleHandleA, CreateDirectoryExA, ReadConsoleInputA, GetTempPathW, GetCurrentDirectoryW, RemoveDirectoryW, OutputDebugStringA, GetProcAddress, LocalAlloc, GetBinaryTypeW, SearchPathA, VerifyVersionInfoA, GetProcessPriorityBoost, EndUpdateResourceW, FindNextFileW, FindFirstVolumeW, LocalFree, GlobalFlags, UpdateResourceW, CreateActCtxA, CopyFileW, InterlockedExchangeAdd, GetConsoleAliasW, VerSetConditionMask, CreateMutexA, DeactivateActCtx, GetDiskFreeSpaceA, MoveFileW, GetLogicalDriveStringsA, ResetEvent, MoveFileExW, CreateMailslotA, WriteConsoleInputA, QueryDosDeviceW, InterlockedDecrement, EnumTimeFormatsW, lstrcatW, FindFirstFileA, FreeEnvironmentStringsA, SetErrorMode, GetTickCount, SetLastError, AllocateUserPhysicalPages, GetPrivateProfileStructA, CopyFileExA, MoveFileWithProgressA, LoadLibraryA, GetLastError, DeleteFileA, GetStartupInfoW, HeapAlloc, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, HeapCreate, VirtualFree, HeapFree, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, RaiseException, VirtualAlloc, HeapReAlloc, SetFilePointer, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, InitializeCriticalSectionAndSpinCount, RtlUnwind, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, ReadFile, HeapSize, CloseHandle, CreateFileA
GDI32.dll	GetTextFaceA
WINHTTP.dll	WinHttpWriteData

Possible Origin

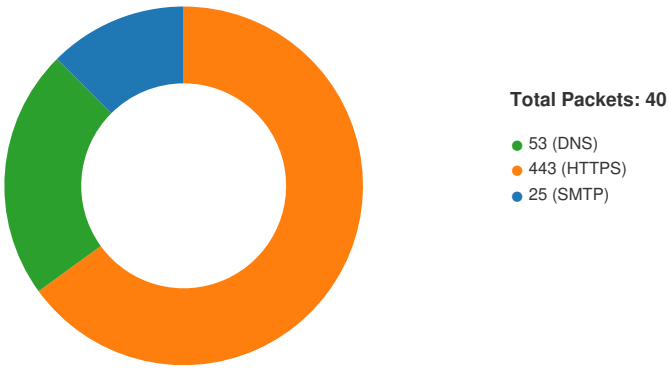
Language of compilation system	Country where language is spoken	Map
Spanish	Venezuela	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8514415 32023883 01/08/23-16:14:55.286794	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	51441	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8634465 32023883 01/08/23-16:15:35.449008	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	63446	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8566825 32023883 01/08/23-16:16:57.387452	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	56682	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8592205 32023883 01/08/23-16:16:15.738842	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	59220	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8626595 32023883 01/08/23-16:17:37.662206	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	62659	53	192.168.2.5	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:14:52.816046000 CET	49700	25	192.168.2.5	52.101.40.29
Jan 8, 2023 16:14:52.964148045 CET	25	49700	52.101.40.29	192.168.2.5
Jan 8, 2023 16:14:52.964273930 CET	49700	25	192.168.2.5	52.101.40.29
Jan 8, 2023 16:14:52.966342926 CET	49700	25	192.168.2.5	52.101.40.29
Jan 8, 2023 16:14:53.115010023 CET	25	49700	52.101.40.29	192.168.2.5
Jan 8, 2023 16:14:53.115042925 CET	25	49700	52.101.40.29	192.168.2.5
Jan 8, 2023 16:14:53.115148067 CET	49700	25	192.168.2.5	52.101.40.29
Jan 8, 2023 16:14:53.116215944 CET	25	49700	52.101.40.29	192.168.2.5
Jan 8, 2023 16:14:53.116290092 CET	49700	25	192.168.2.5	52.101.40.29
Jan 8, 2023 16:14:55.308823109 CET	49701	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:14:55.308898926 CET	443	49701	93.189.42.6	192.168.2.5
Jan 8, 2023 16:14:55.309025049 CET	49701	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:15:35.300574064 CET	49701	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:15:35.300700903 CET	443	49701	93.189.42.6	192.168.2.5
Jan 8, 2023 16:15:35.300817966 CET	49701	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:15:35.474817038 CET	49707	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:15:35.474905014 CET	443	49707	93.189.42.6	192.168.2.5
Jan 8, 2023 16:15:35.475019932 CET	49707	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:16:15.518754959 CET	49707	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:16:15.518908978 CET	443	49707	93.189.42.6	192.168.2.5
Jan 8, 2023 16:16:15.519073963 CET	49707	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:16:16.034245968 CET	49711	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:16:16.034348965 CET	443	49711	93.189.42.6	192.168.2.5
Jan 8, 2023 16:16:16.034431934 CET	49711	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:16:56.099965096 CET	49711	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:16:56.100171089 CET	443	49711	93.189.42.6	192.168.2.5
Jan 8, 2023 16:16:56.100471020 CET	49711	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:16:57.495203972 CET	49713	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:16:57.495263100 CET	443	49713	93.189.42.6	192.168.2.5
Jan 8, 2023 16:16:57.495353937 CET	49713	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:17:37.493819952 CET	49713	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:17:37.494014025 CET	443	49713	93.189.42.6	192.168.2.5
Jan 8, 2023 16:17:37.494110107 CET	49713	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:17:37.683511972 CET	49715	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:17:37.683573008 CET	443	49715	93.189.42.6	192.168.2.5
Jan 8, 2023 16:17:37.683675051 CET	49715	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:18:17.684156895 CET	49715	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:18:17.684248924 CET	443	49715	93.189.42.6	192.168.2.5
Jan 8, 2023 16:18:17.684341908 CET	49715	443	192.168.2.5	93.189.42.6
Jan 8, 2023 16:18:17.888770103 CET	49717	443	192.168.2.5	80.66.75.254
Jan 8, 2023 16:18:17.888814926 CET	443	49717	80.66.75.254	192.168.2.5
Jan 8, 2023 16:18:17.888916969 CET	49717	443	192.168.2.5	80.66.75.254
Jan 8, 2023 16:18:57.890940905 CET	49717	443	192.168.2.5	80.66.75.254
Jan 8, 2023 16:18:57.893198967 CET	443	49717	80.66.75.254	192.168.2.5
Jan 8, 2023 16:18:57.893291950 CET	49717	443	192.168.2.5	80.66.75.254
Jan 8, 2023 16:19:04.759143114 CET	49721	443	192.168.2.5	80.66.75.254
Jan 8, 2023 16:19:04.759206057 CET	443	49721	80.66.75.254	192.168.2.5
Jan 8, 2023 16:19:04.759340048 CET	49721	443	192.168.2.5	80.66.75.254

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:14:52.559065104 CET	60649	53	192.168.2.5	8.8.8.8
Jan 8, 2023 16:14:52.804296970 CET	53	60649	8.8.8.8	192.168.2.5
Jan 8, 2023 16:14:55.286793947 CET	51441	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:14:55.306782007 CET	53	51441	8.8.8.8	192.168.2.5
Jan 8, 2023 16:15:35.449007988 CET	63446	53	192.168.2.5	8.8.8.8
Jan 8, 2023 16:15:35.466605902 CET	53	63446	8.8.8.8	192.168.2.5
Jan 8, 2023 16:16:15.738842010 CET	59220	53	192.168.2.5	8.8.8.8
Jan 8, 2023 16:16:16.032886028 CET	53	59220	8.8.8.8	192.168.2.5
Jan 8, 2023 16:16:57.387451887 CET	56682	53	192.168.2.5	8.8.8.8
Jan 8, 2023 16:16:57.493288994 CET	53	56682	8.8.8.8	192.168.2.5
Jan 8, 2023 16:17:37.662205935 CET	62659	53	192.168.2.5	8.8.8.8
Jan 8, 2023 16:17:37.681801081 CET	53	62659	8.8.8.8	192.168.2.5
Jan 8, 2023 16:18:17.840845108 CET	56263	53	192.168.2.5	8.8.8.8
Jan 8, 2023 16:18:17.887387037 CET	53	56263	8.8.8.8	192.168.2.5
Jan 8, 2023 16:18:32.805587053 CET	64419	53	192.168.2.5	8.8.8.8
Jan 8, 2023 16:18:32.834148884 CET	53	64419	8.8.8.8	192.168.2.5
Jan 8, 2023 16:19:04.705599070 CET	61344	53	192.168.2.5	8.8.8.8
Jan 8, 2023 16:19:04.755404949 CET	53	61344	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 8, 2023 16:14:52.559065104 CET	192.168.2.5	8.8.8.8	0x9e65	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:14:55.286793947 CET	192.168.2.5	8.8.8.8	0xc8e5	Standard query (0)	svartalfheim.top	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.449007988 CET	192.168.2.5	8.8.8.8	0xe9fa	Standard query (0)	svartalfheim.top	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:16:15.738842010 CET	192.168.2.5	8.8.8.8	0x678a	Standard query (0)	svartalfheim.top	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:16:57.387451887 CET	192.168.2.5	8.8.8.8	0xa092	Standard query (0)	svartalfheim.top	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:17:37.662205935 CET	192.168.2.5	8.8.8.8	0x6193	Standard query (0)	svartalfheim.top	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:18:17.840845108 CET	192.168.2.5	8.8.8.8	0x54a4	Standard query (0)	jotunheim.name	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:18:32.805587053 CET	192.168.2.5	8.8.8.8	0xa3ff	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:19:04.705599070 CET	192.168.2.5	8.8.8.8	0x783d	Standard query (0)	jotunheim.name	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
Jan 8, 2023 16:14:52.804296970 CET	8.8.8.8	192.168.2.5	0x9e65	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.40.29	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:14:52.804296970 CET	8.8.8.8	192.168.2.5	0x9e65	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:14:52.804296970 CET	8.8.8.8	192.168.2.5	0x9e65	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:14:52.804296970 CET	8.8.8.8	192.168.2.5	0x9e65	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.2	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:14:52.804296970 CET	8.8.8.8	192.168.2.5	0x9e65	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:14:52.804296970 CET	8.8.8.8	192.168.2.5	0x9e65	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)	false

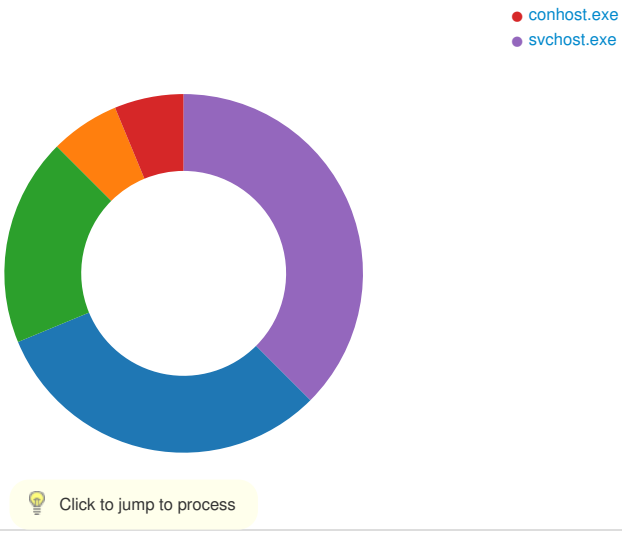
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:14:55.306782007 CET	8.8.8.8	192.168.2.5	0xc8e5	No error (0)	svartalfheim.top		93.189.42.6	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.466605902 CET	8.8.8.8	192.168.2.5	0xe9fa	No error (0)	svartalfheim.top		93.189.42.6	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:16:16.032886028 CET	8.8.8.8	192.168.2.5	0x678a	No error (0)	svartalfheim.top		93.189.42.6	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:16:57.493288994 CET	8.8.8.8	192.168.2.5	0xa092	No error (0)	svartalfheim.top		93.189.42.6	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:17:37.681801081 CET	8.8.8.8	192.168.2.5	0x6193	No error (0)	svartalfheim.top		93.189.42.6	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:18:17.887387037 CET	8.8.8.8	192.168.2.5	0x54a4	No error (0)	jotunheim.name		80.66.75.254	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:18:32.834148884 CET	8.8.8.8	192.168.2.5	0xa3ff	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:18:32.834148884 CET	8.8.8.8	192.168.2.5	0xa3ff	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:18:32.834148884 CET	8.8.8.8	192.168.2.5	0xa3ff	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.2	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:18:32.834148884 CET	8.8.8.8	192.168.2.5	0xa3ff	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.40.29	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:18:32.834148884 CET	8.8.8.8	192.168.2.5	0xa3ff	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:18:32.834148884 CET	8.8.8.8	192.168.2.5	0xa3ff	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:19:04.755404949 CET	8.8.8.8	192.168.2.5	0x783d	No error (0)	jotunheim.name		80.66.75.254	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 8, 2023 16:14:53.115042925 CET	25	49700	52.101.40.29	192.168.2.5	220 CY4PEPF00005055.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Sun, 8 Jan 2023 15:14:52 +0000

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 4516, Parent PID: 3324

General

Target ID:	0
Start time:	16:14:26
Start date:	08/01/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	269824 bytes
MD5 hash:	4C085E942806B5C8D972695451AA8F48
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.344749194.0000000002DA8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000000.00000002.342422923.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 00000000.00000002.342422923.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000000.00000002.342422923.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000000.00000002.344302410.0000000002D20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.344302410.0000000002D20000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000000.00000002.344302410.0000000002D20000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000000.00000003.320355730.0000000002D40000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 00000000.00000003.320355730.0000000002D40000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 00000000.00000003.320355730.0000000002D40000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: 5252, Parent PID: 4516

General

Target ID:	1
Start time:	16:14:37
Start date:	08/01/2023

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\tsqtjgfo\
Imagebase:	0x11d0000
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\tsqtjgfo\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	11DBFE7	CreateDirectoryW

Analysis Process: conhost.exe PID: **5268**, Parent PID: **5252**

General

Target ID:	2
Start time:	16:14:37
Start date:	08/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **2824**, Parent PID: **4516**

General

Target ID:	3
Start time:	16:14:38
Start date:	08/01/2023
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\qtcnnjjg.exe" C:\Windows\SysWOW64\tsqtjgfo\
Imagebase:	0x11d0000
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 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\qtcnnjjg.exe	C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe	success or wait	1	11DB966	MoveFileExW

Analysis Process: conhost.exe PID: **2328**, Parent PID: **2824**

General	
Target ID:	4
Start time:	16:14:38
Start date:	08/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: sc.exe PID: **1352**, Parent PID: **4516**

General	
Target ID:	5
Start time:	16:14:38
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create tsqtjgfo binPath= "C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe /d\"C:\Users\user\Desktop\file.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0xd90000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
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: conhost.exe PID: **1348**, Parent PID: **1352**

General	
Target ID:	6
Start time:	16:14:38
Start date:	08/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: sc.exe PID: **5936**, Parent PID: **4516**

General

Target ID:	7
Start time:	16:14:39
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description tsqtjgfo "wifi internet conection
Imagebase:	0xd90000
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: **4696**, Parent PID: **5936**

General

Target ID:	8
Start time:	16:14:39
Start date:	08/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **5228**, Parent PID: **4516**

General

Target ID:	9
Start time:	16:14:40
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start tsqtjgfo
Imagebase:	0xd90000
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: 5020, Parent PID: 5228

General

Target ID:	10
Start time:	16:14:40
Start date:	08/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: qtcnnjjg.exe PID: 5940, Parent PID: 564

General

Target ID:	11
Start time:	16:14:42
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe /d"C:\Users\user\Desktop\file.exe"
Imagebase:	0x400000
File size:	15645184 bytes
MD5 hash:	3D0E87BA5B0B7BA4C2F68898214F5106
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: 0000000B.00000003.354409615.0000000002D40000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 0000000B.00000003.354409615.0000000002D40000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 0000000B.00000003.354409615.0000000002D40000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000000B.00000002.355868044.0000000002C40000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000B.00000002.355868044.0000000002C40000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 0000000B.00000002.355868044.0000000002C40000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000000B.00000002.355978031.0000000002DA0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 0000000B.00000002.355978031.0000000002DA0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 0000000B.00000002.355978031.0000000002DA0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000000B.00000002.355049753.0000000000400000.00000040.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 0000000B.00000002.355049753.0000000000400000.00000040.00000001.01000000.00000004.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 0000000B.00000002.355049753.0000000000400000.00000040.00000001.01000000.00000004.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000B.00000002.356106077.0000000002E23000.00000040.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: netsh.exe PID: **3648**, Parent PID: **4516**

General	
Target ID:	12
Start time:	16:14:42
Start date:	08/01/2023
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:	0x1280000
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	1287B1B	WriteFile
\Device\ConDrv	3771	3736	0d 0a		success or wait	1	1287B1B	WriteFile
\Device\ConDrv	3773	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	1287B1B	WriteFile

Analysis Process: conhost.exe PID: **4352**, Parent PID: **3648**

General	
Target ID:	13
Start time:	16:14:45
Start date:	08/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **3232**, Parent PID: **5940**

General	
Target ID:	14
Start time:	16:14:51
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0xa80000
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: 0000000E.00000002.826846421.00000000004D0000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Tofsee, Description: Detects Tofsee, Source: 0000000E.00000002.826846421.00000000004D0000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Tofsee_26124fe4, Description: unknown, Source: 0000000E.00000002.826846421.00000000004D0000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	4DA409	DeleteFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe	unknown	64	success or wait	1	4D6809	ReadFile
C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe	unknown	248	success or wait	1	4D6840	ReadFile
C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe	unknown	64	success or wait	23	4D6809	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\tsqtjgfo	dword	0	success or wait	1	4D8447	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\tsqtjgfo	ImagePath	expand unicode	C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe /d"C:\Users\user\Desktop\file.exe"	C:\Windows\SysWOW64\tsqtjgfo\qtcnnjjg.exe	success or wait	1	4D7D50	RegSetValueExA

Disassembly

No disassembly