ID: 830454
Sample Name:
FeDex_shipping_document.exe
Cookbook: default.jbs
Time: 11:50:40
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

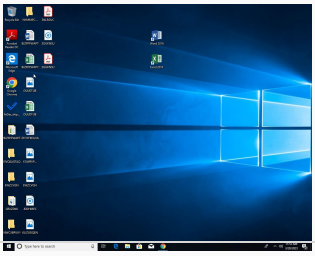
Windows Analysis Report

FeDex_shipping_document.exe

Overview

General Information

Sample Name:	FeDex_shipping_document.exe
Analysis ID:	830454
MD5:	5cf87a160007a..
SHA1:	e11d7467bc96…
SHA256:	91e74ee16f622..
Tags:	AgentTesla exe FedEx
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

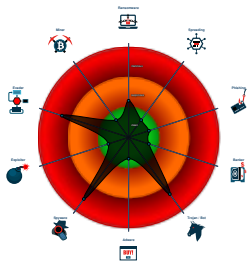
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Contains functionality to register a lo…
- Machine Learning detection for sam…
- May check the online IP address of…
- Injects a PE file into a foreign proce…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- FeDex_shipping_document.exe (PID: 5300 cmdline: C:\Users\user\Desktop\FeDex_shipping_document.exe MD5: 5CF87A160007A5E6C7A4D24E1D831327)
  - FeDex_shipping_document.exe (PID: 3628 cmdline: C:\Users\user\Desktop\FeDex_shipping_document.exe MD5: 5CF87A160007A5E6C7A4D24E1D831327)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "Discord",
  "Discord url": "https://discord.com/api/webhooks/1085961054116380784/6mOHAJEbhkHvMnx5Lupuieun02GlpoDDe4vKN3n-OIFv4DLpFFRiyRBhgIyiXf6D4mYj"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.521394788.000000000305B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: FeDex_shipping_document.exe PID: 3628	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: FeDex_shipping_document.exe PID: 3628	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.7 - Destination IP: 162.159.138.232

Timestamp:	192.168.2.7162.159.138.232497014432851779 03/20/23-11:52:05.074477
SID:	2851779
Source Port:	49701
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion

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

Injects a PE file into a foreign processes

Stealing of Sensitive Information

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 browser information (history, passwords, etc)

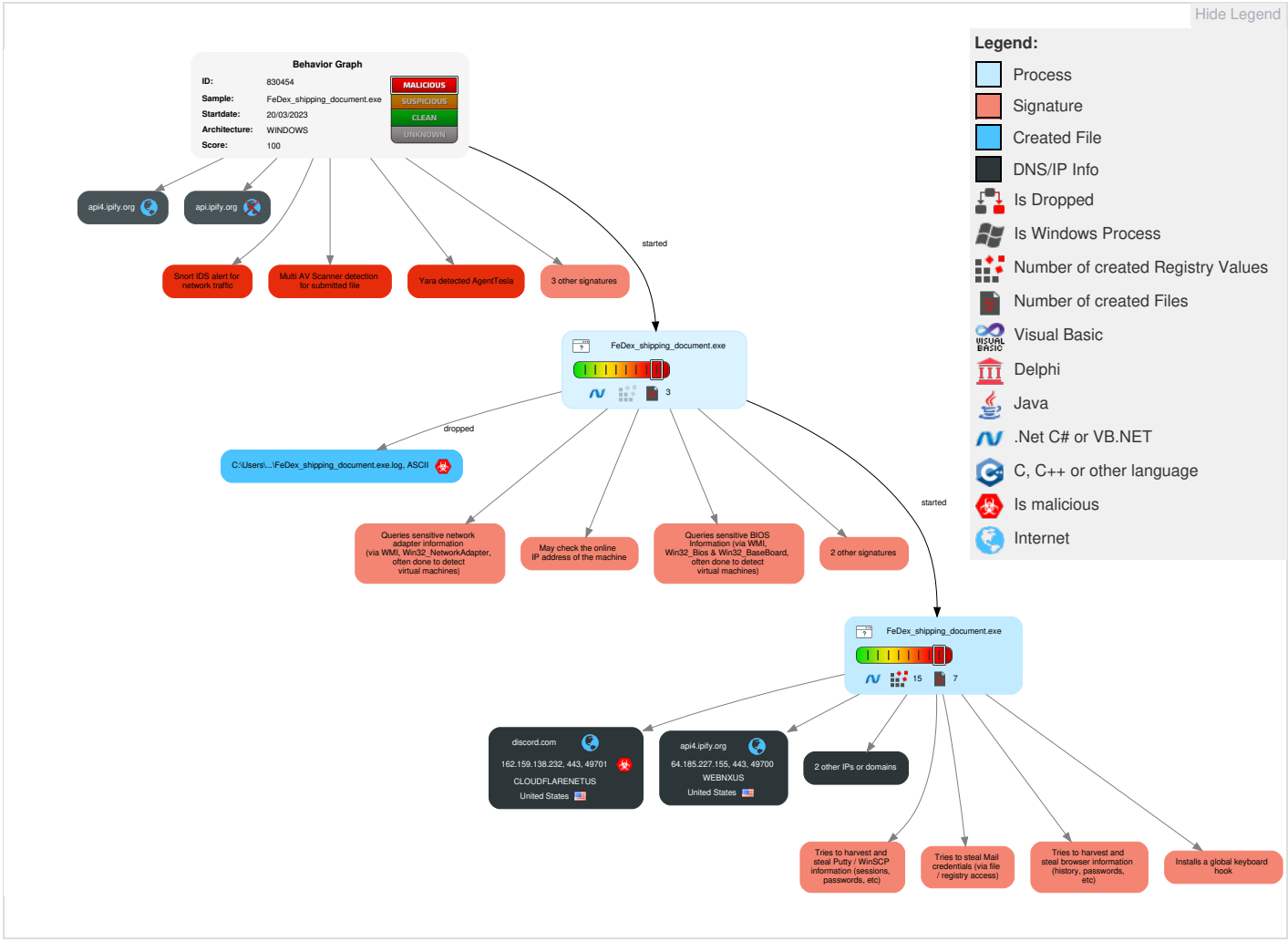
Remote Access Functionality

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	2 1 Input Capture	1 3 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 Application Window Discovery	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	1 Data from Local System	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 System Network Configuration Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Software Packing	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

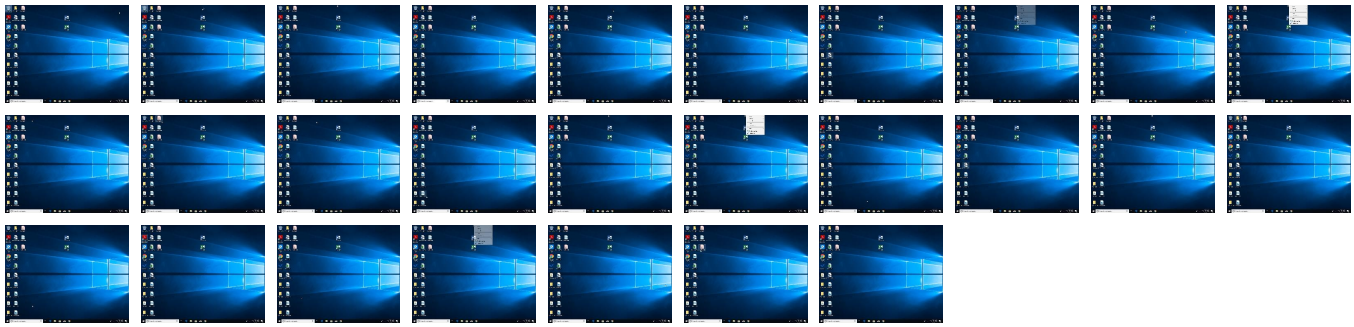
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FeDex_shipping_document.exe	38%	ReversingLabs	Win32.Trojan.Generic	
FeDex_shipping_document.exe	34%	Virustotal		Browse
FeDex_shipping_document.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.FeDex_shipping_document.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File

Domains

Source	Detection	Scanner	Label	Link
discord.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://discord.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://discord.com	0%	URL Reputation	safe	
http://discord.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://discord.com4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://discord.com/api/webhooks/1085961054116380784/6mOHAJEbhkHvMnx5Lupuieun02GlpoDDe4vKN3n-OIFv4DL	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://discord.com/api/webhooks/1085961054116380784/6mOHAJEbhkHvMnx5Lupuieun02GlpoDDe4vKN3n-OIFv4DLpFFRiyRBhgIyiXf6D4mYj	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://discord.comD8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.138.232	true	true	• 0%, Virustotal, Browse	unknown
api4.ipify.org	64.185.227.155	true	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high
http://https://discord.com/api/webhooks/1085961054116380784/6mOHAJEbhkHvMnx5Lupuieun02GlpoDDe4vKN3n-OIFv4DLpFFRiyRBhgIyiXf6D4mYj	true	• Avira URL Cloud: safe	unknown

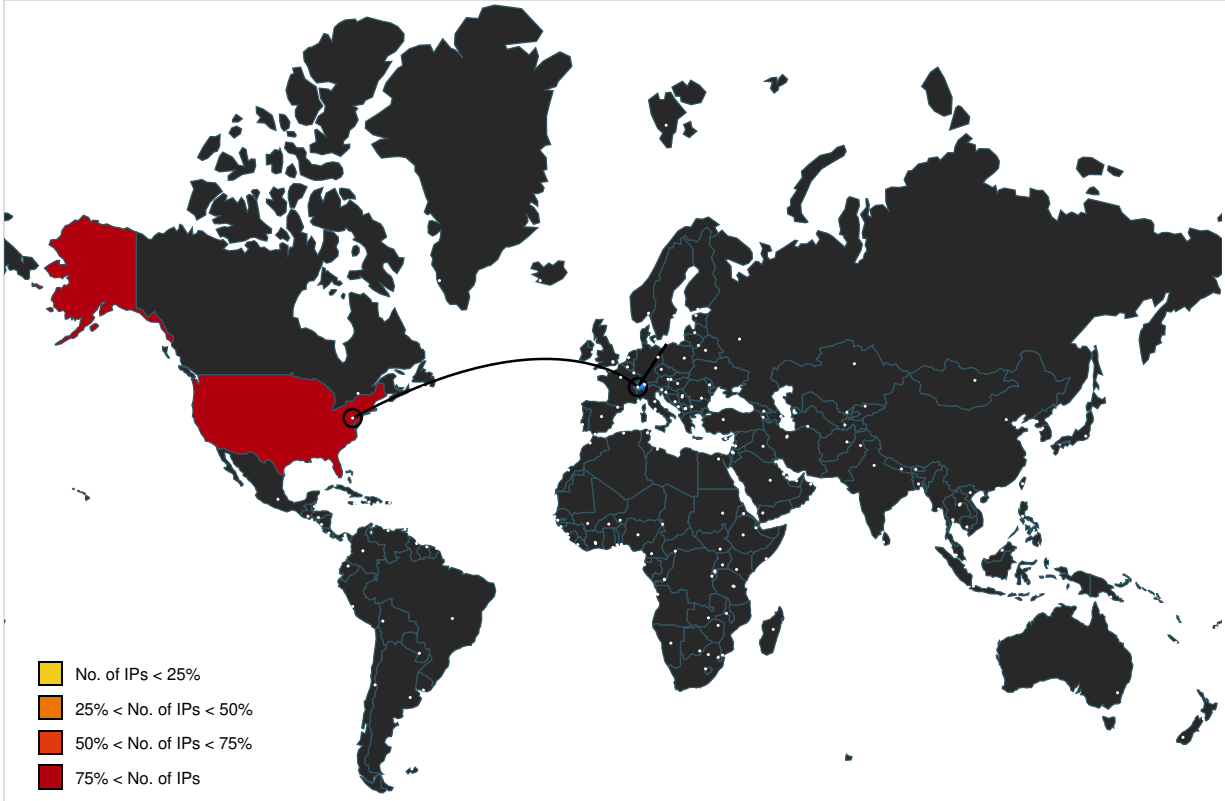
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://discord.com	FeDex_shipping_document.exe, 00000001.00000002.521394788.0000000003074000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://media.discordapp.net/attachments/1085960984071524425/1087327699887980574/user-128757_20	FeDex_shipping_document.exe, 00000001.00000002.521394788.0000000003098000.00000004.00000800.00020000.00000000.sdmp, FeDex_shipping_document.exe, 00000001.00000002.521394788.0000000003057000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://discord.com/api/webhooks/1085961054116380784/6mOHAJEbhkHvMnx5Lupuieun02GlpoDDe4vKN3n-OIFv4DL	FeDex_shipping_document.exe, 00000001.00000002.521394788.0000000003011000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://cdn.discordapp.com/attachments/1085960984071524425/1087327704275234847/user-128757_2023	FeDex_shipping_document.exe, 00000001.00000002.521394788.0000000003169000.00000004.00000800.00020000.00000000.sdmp	false		high
http://discord.com	FeDex_shipping_document.exe, 00000001.00000002.521394788.00000000030B0000.00000004.00000800.00020000.00000000.sdmp, FeDex_shipping_document.exe, 00000001.00000002.521394788.0000000003074000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://discord.comD8	FeDex_shipping_document.exe, 00000001.00000002.521394788.00000000030B0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://media.discordapp.net/attachments/1085960984071524425/1087327704275234847/user-128757_20	FeDex_shipping_document.exe, 00000001.00000002.521394788.0000000003169000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org	FeDex_shipping_document.exe, 00000001.00000002.521394788.0000000003011000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	FeDex_shipping_document.exe, 00000000.00000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/1085960984071524425/1087327699887980574/user-128757_2023	FeDex_shipping_document.exe, 00000001.000000002.521394788.0000000003098000.00000004.00000800.00020000.00000000.sdmp, FeDex_shipping_document.exe, 00000001.000000002.521394788.0000000003057000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://discord.com4	FeDex_shipping_document.exe, 00000001.000000002.521394788.0000000003074000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	FeDex_shipping_document.exe, 00000000.000000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	FeDex_shipping_document.exe, 00000000.000000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	FeDex_shipping_document.exe, 00000000.000000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	FeDex_shipping_document.exe, 00000000.000000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	FeDex_shipping_document.exe, 00000000.000000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	FeDex_shipping_document.exe, 00000000.000000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	FeDex_shipping_document.exe, 00000000.000000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	FeDex_shipping_document.exe, 00000001.000000002.521394788.0000000003011000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	FeDex_shipping_document.exe, 00000000.000000002.272021390.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.138.232	discord.com	United States		13335	CLOUDFLARENETUS	true
64.185.227.155	api4.ipify.org	United States		18450	WEBNXUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.135.232	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830454
Start date and time:	2023-03-20 11:50:40 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	FeDex_shipping_document.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/2@4/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.10.249.147, 23.10.249.178, 93.184.221.240, 8.238.85.126, 8.241.126.121, 8.248.137.254, 67.26.75.254, 8.238.88.254
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net, download.windowsupdate.com.edgesuite.net
- Not all processes where analyzed, report is 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
11:51:45	API Interceptor	683x Sleep call for process: FeDex_shipping_document.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FeDex_shipping_document.exe.log

Process:	C:\Users\user\Desktop\FeDex_shipping_document.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\ghkgpqzj.zir\Chrome\Default\Network\Cookies

Process:	C:\Users\user\Desktop\FeDex_shipping_document.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 10, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 10
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.4393511334109407
Encrypted:	false
SSDEEP:	24:TLqlj1czkwubXYFpFNYcw+6UwcYzHrSl:TyxcYwuLopFgU1YzLSl
MD5:	8C31C5487A97BBE73711C5E20600C1F6
SHA1:	D4D6B04226D8FFC894749B3963E7DB7068D6D773
SHA-256:	A1326E74262F4B37628F2E712EC077F499B113181A1E937E752D046E43F1689A
SHA-512:	394391350524B994504F4E748CCD5C3FA8EF980AED850A5A60F09250E8261AC8E300657CBB1DBF305729637BC0E1F043E57799E2A35C82EEA3825CE5C9E7051D
Malicious:	false
Reputation:	high, very likely benign file

Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.864054907684923
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:	FeDex_shipping_document.exe
File size:	746496
MD5:	5cf87a160007a5e6c7a4d24e1d831327
SHA1:	e11d7467bc961d5ff16c3541200be1ad5083cefa
SHA256:	91e74ee16f6229b18ef4f973494b8ec68bad3420e90fd3f1ee6d835048421fcf
SHA512:	c11e2c571817ac519ef89019529171d64e9f3faa17a2ccd51a55770113eff83e27f3a53133cec3daa096f989fafedd378e759cc4030b83489ebccbd7aa425237
SSDEEP:	12288:EDBmYMUnFW/NMbbjHAaBvaDzGkSjT+vbuxiZQ7GiPLbk6jdoVx2ye6yb:EDBUibAXPGD+zKiri/kCGVYye6q
TLSH:	66F402342FEA6239F57657BDD9E43295236E77B22703D95E04B121CA4B63B028DC092F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....0..N.....Rm... .....@.. .....@.....

File Icon

Icon Hash:	209480e66eb84902

Static PE Info

General

Entrypoint:	0x4b6d52
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6417BCAC [Mon Mar 20 01:53:48 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb6cfd	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x1110	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xba000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb58e8	0x54	.text
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	0xb4d58	0xb4e00	False	0.9268084290774016	data	7.872797130775443	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0xb8000	0x1110	0x1200	False	0.73046875	data	6.631473125860904	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xba000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb8100	0xa79	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xb8b8c	0x14	data		
RT_VERSION	0xb8bb0	0x360	data		
RT_MANIFEST	0xb8f20	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

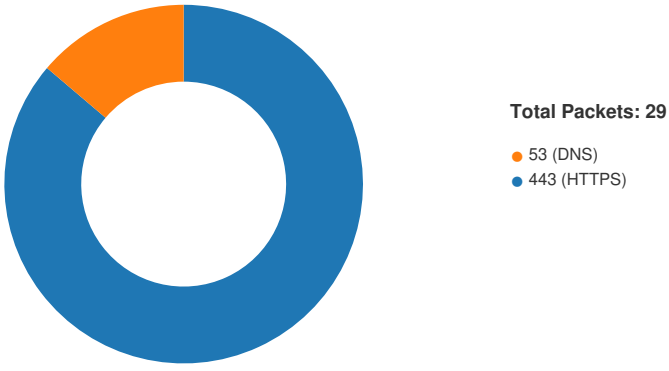
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7162.159.138.232497014432851779 03/20/23-11:52:05.074477	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49701	443	192.168.2.7	162.159.138.232

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:51:49.157324076 CET	49700	443	192.168.2.7	64.185.227.155
Mar 20, 2023 11:51:49.157382011 CET	443	49700	64.185.227.155	192.168.2.7
Mar 20, 2023 11:51:49.157479048 CET	49700	443	192.168.2.7	64.185.227.155
Mar 20, 2023 11:51:49.196374893 CET	49700	443	192.168.2.7	64.185.227.155
Mar 20, 2023 11:51:49.196409941 CET	443	49700	64.185.227.155	192.168.2.7
Mar 20, 2023 11:51:57.077124119 CET	443	49700	64.185.227.155	192.168.2.7
Mar 20, 2023 11:51:57.077359915 CET	49700	443	192.168.2.7	64.185.227.155

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:51:57.808013916 CET	49700	443	192.168.2.7	64.185.227.155
Mar 20, 2023 11:51:57.808080912 CET	443	49700	64.185.227.155	192.168.2.7
Mar 20, 2023 11:51:57.808967113 CET	443	49700	64.185.227.155	192.168.2.7
Mar 20, 2023 11:51:57.874470949 CET	49700	443	192.168.2.7	64.185.227.155
Mar 20, 2023 11:51:58.269769907 CET	49700	443	192.168.2.7	64.185.227.155
Mar 20, 2023 11:51:58.269812107 CET	443	49700	64.185.227.155	192.168.2.7
Mar 20, 2023 11:51:59.014796972 CET	49700	443	192.168.2.7	64.185.227.155
Mar 20, 2023 11:51:59.014924049 CET	443	49700	64.185.227.155	192.168.2.7
Mar 20, 2023 11:51:59.014995098 CET	49700	443	192.168.2.7	64.185.227.155
Mar 20, 2023 11:52:04.950087070 CET	49701	443	192.168.2.7	162.159.138.232
Mar 20, 2023 11:52:04.950215101 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:04.950337887 CET	49701	443	192.168.2.7	162.159.138.232
Mar 20, 2023 11:52:04.952203989 CET	49701	443	192.168.2.7	162.159.138.232
Mar 20, 2023 11:52:04.952301979 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:05.009949923 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:05.010083914 CET	49701	443	192.168.2.7	162.159.138.232
Mar 20, 2023 11:52:05.014666080 CET	49701	443	192.168.2.7	162.159.138.232
Mar 20, 2023 11:52:05.014695883 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:05.015054941 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:05.018209934 CET	49701	443	192.168.2.7	162.159.138.232
Mar 20, 2023 11:52:05.018237114 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:05.073689938 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:05.074287891 CET	49701	443	192.168.2.7	162.159.138.232
Mar 20, 2023 11:52:05.074341059 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:05.421833992 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:05.422219038 CET	443	49701	162.159.138.232	192.168.2.7
Mar 20, 2023 11:52:05.422296047 CET	49701	443	192.168.2.7	162.159.138.232
Mar 20, 2023 11:52:05.424500942 CET	49701	443	192.168.2.7	162.159.138.232
Mar 20, 2023 11:52:06.002155066 CET	49702	443	192.168.2.7	162.159.135.232
Mar 20, 2023 11:52:06.002207994 CET	443	49702	162.159.135.232	192.168.2.7
Mar 20, 2023 11:52:06.002302885 CET	49702	443	192.168.2.7	162.159.135.232
Mar 20, 2023 11:52:06.003519058 CET	49702	443	192.168.2.7	162.159.135.232
Mar 20, 2023 11:52:06.003566027 CET	443	49702	162.159.135.232	192.168.2.7
Mar 20, 2023 11:52:06.051467896 CET	443	49702	162.159.135.232	192.168.2.7
Mar 20, 2023 11:52:06.055735111 CET	49702	443	192.168.2.7	162.159.135.232
Mar 20, 2023 11:52:06.055769920 CET	443	49702	162.159.135.232	192.168.2.7
Mar 20, 2023 11:52:06.124003887 CET	443	49702	162.159.135.232	192.168.2.7
Mar 20, 2023 11:52:06.124957085 CET	49702	443	192.168.2.7	162.159.135.232
Mar 20, 2023 11:52:06.125015020 CET	443	49702	162.159.135.232	192.168.2.7
Mar 20, 2023 11:52:06.437938929 CET	443	49702	162.159.135.232	192.168.2.7
Mar 20, 2023 11:52:06.438318968 CET	443	49702	162.159.135.232	192.168.2.7
Mar 20, 2023 11:52:06.438410997 CET	49702	443	192.168.2.7	162.159.135.232
Mar 20, 2023 11:52:06.440745115 CET	49702	443	192.168.2.7	162.159.135.232

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:51:49.083699942 CET	59477	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:51:49.103337049 CET	53	59477	8.8.8.8	192.168.2.7
Mar 20, 2023 11:51:49.115154028 CET	55752	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:51:49.135409117 CET	53	55752	8.8.8.8	192.168.2.7
Mar 20, 2023 11:52:04.919559956 CET	50330	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:52:04.941693068 CET	53	50330	8.8.8.8	192.168.2.7
Mar 20, 2023 11:52:05.979279041 CET	56588	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:52:06.000864029 CET	53	56588	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 11:51:49.083699942 CET	192.168.2.7	8.8.8.8	0xd371	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:51:49.115154028 CET	192.168.2.7	8.8.8.8	0x7dd7	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:04.919559956 CET	192.168.2.7	8.8.8.8	0x8554	Standard query (0)	discord.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:05.979279041 CET	192.168.2.7	8.8.8.8	0xf5ae	Standard query (0)	discord.com	A (IP address)	IN (0x0001)	false

DNS Answers

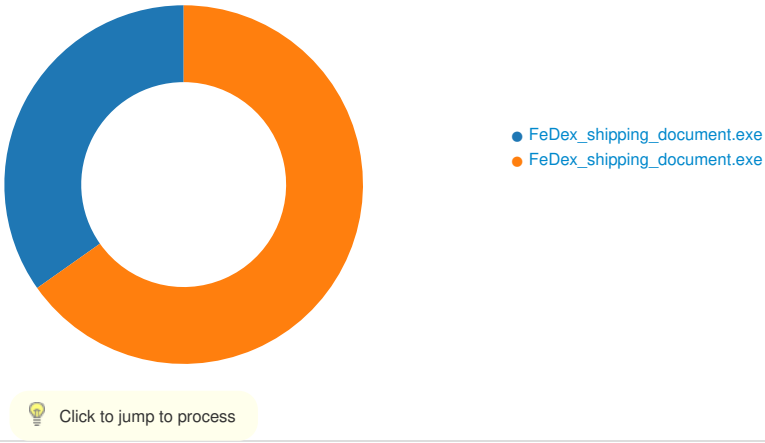
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:51:49.103337049 CET	8.8.8.8	192.168.2.7	0xd371	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:51:49.103337049 CET	8.8.8.8	192.168.2.7	0xd371	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:51:49.103337049 CET	8.8.8.8	192.168.2.7	0xd371	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:51:49.103337049 CET	8.8.8.8	192.168.2.7	0xd371	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:51:49.135409117 CET	8.8.8.8	192.168.2.7	0x7dd7	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:51:49.135409117 CET	8.8.8.8	192.168.2.7	0x7dd7	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:51:49.135409117 CET	8.8.8.8	192.168.2.7	0x7dd7	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:51:49.135409117 CET	8.8.8.8	192.168.2.7	0x7dd7	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:04.941693068 CET	8.8.8.8	192.168.2.7	0x8554	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:04.941693068 CET	8.8.8.8	192.168.2.7	0x8554	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:04.941693068 CET	8.8.8.8	192.168.2.7	0x8554	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:04.941693068 CET	8.8.8.8	192.168.2.7	0x8554	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:04.941693068 CET	8.8.8.8	192.168.2.7	0x8554	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:06.000864029 CET	8.8.8.8	192.168.2.7	0xf5ae	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:06.000864029 CET	8.8.8.8	192.168.2.7	0xf5ae	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:06.000864029 CET	8.8.8.8	192.168.2.7	0xf5ae	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:06.000864029 CET	8.8.8.8	192.168.2.7	0xf5ae	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:52:06.000864029 CET	8.8.8.8	192.168.2.7	0xf5ae	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org
- discord.com

Statistics

Behavior



System Behavior

Analysis Process: FeDex_shipping_document.exe PID: 5300, Parent PID: 3320

General

Target ID:	0
Start time:	11:51:39
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\FeDex_shipping_document.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\FeDex_shipping_document.exe
Imagebase:	0xe70000
File size:	746496 bytes
MD5 hash:	5CF87A160007A5E6C7A4D24E1D831327
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	72E3CF06	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	72E3CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FeDex_shipping_document.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7314C78D	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\FeDex_shipping_document.exe.log	0	1216	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7314C907	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	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C81B4F	ReadFile

Analysis Process: FeDex_shipping_document.exe PID: **3628**, Parent PID: **5300**

General

Target ID:	1
Start time:	11:51:46
Start date:	20/03/2023

Path:	C:\Users\user\Desktop\FeDex_shipping_document.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\FeDex_shipping_document.exe
Imagebase:	0xac0000
File size:	746496 bytes
MD5 hash:	5CF87A160007A5E6C7A4D24E1D831327
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: 00000001.00000002.521394788.000000000305B000.00000004.00000800.00020000.00000000.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	72E3CF06	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	72E3CF06	unknown
C:\Users\user\AppData\Roaming\ghkgpqzj.zir	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ghkgpqzj.zir\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	71C8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ghkgpqzj.zir\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	71C8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ghkgpqzj.zir\Chrome\Default\Network	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ghkgpqzj.zir\Chrome\Default\Network\Cookies	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	71C8DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ghkgpqzj.zir\Chrome\Default\Network\Cookies	success or wait	1	71C86A95	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\ghkgpqzj.zir\Chrome\Default\Network\Cookies	0	28672	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 0a 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 13 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 0a 00 2e 5b 35 0d 0a fd 00 04 09 fd 00 0f 67 0f fd 0d 24 09 fd 09 fd 09 fd 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 00 00 00	SQLite format 3@ .[5g$	success or wait	1	71C8DD66	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	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\3d3bfcea-a92d-4141-afde-fa1cf8edbed3	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\3d3bfcea-a92d-4141-afde-fa1cf8edbed3	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Roaming\ghkgpqzj.zir\Chrome\Default\Network\Cookies	unknown	16384	success or wait	2	71C81B4F	ReadFile
C:\Users\user\AppData\Roaming\ghkgpqzj.zir\Chrome\Default\Network\Cookies	unknown	16384	end of file	1	71C81B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly