ID: 339030
Sample Name: New FedEx paper work review.exe
Cookbook: default.jbs
Time: 09:41:23
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

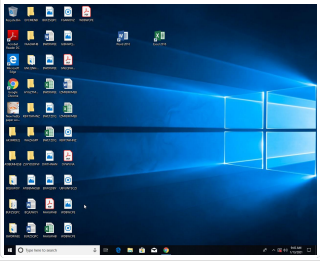
Analysis Report New FedEx paper work review.exe

Overview

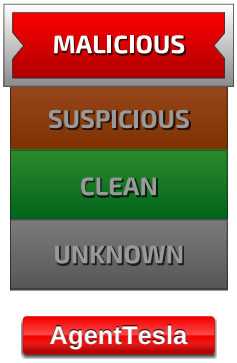
General Information

Sample Name:	New FedEx paper work review.exe
Analysis ID:	339030
MD5:	c359c954a7d104..
SHA1:	e647c8aa88a720..
SHA256:	306602e7317841..
Tags:	AgentTesla exe FedEx

Most interesting Screenshot:



Detection

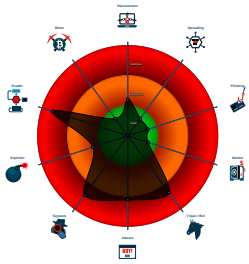


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Modifies the hosts file
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- New FedEx paper work review.exe (PID: 5956 cmdline: 'C:\Users\user\Desktop\New FedEx paper work review.exe' MD5: C359C954A7D104B0A1BDE867F86E73A5)
  - New FedEx paper work review.exe (PID: 3912 cmdline: C:\Users\user\Desktop\New FedEx paper work review.exe MD5: C359C954A7D104B0A1BDE867F86E73A5)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "mRy89v",
  "URL: ": "https://jeQsgpMQfgg21VTI.net",
  "To: ": "recieve@resulthome.xyz",
  "ByHost: ": "mail.privateemail.com:587",
  "Password: ": "HXIEqtBQ5tSBy",
  "From: ": "recieve@resulthome.xyz"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.675657030.000000000327 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.1028180638.0000000002E 61000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.1028180638.0000000002E 61000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.1026177897.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.677503823.000000000427 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright null 2021

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

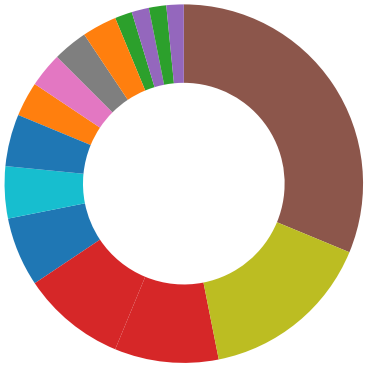
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.New FedEx paper work review.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Copyright null 2021

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:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

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)

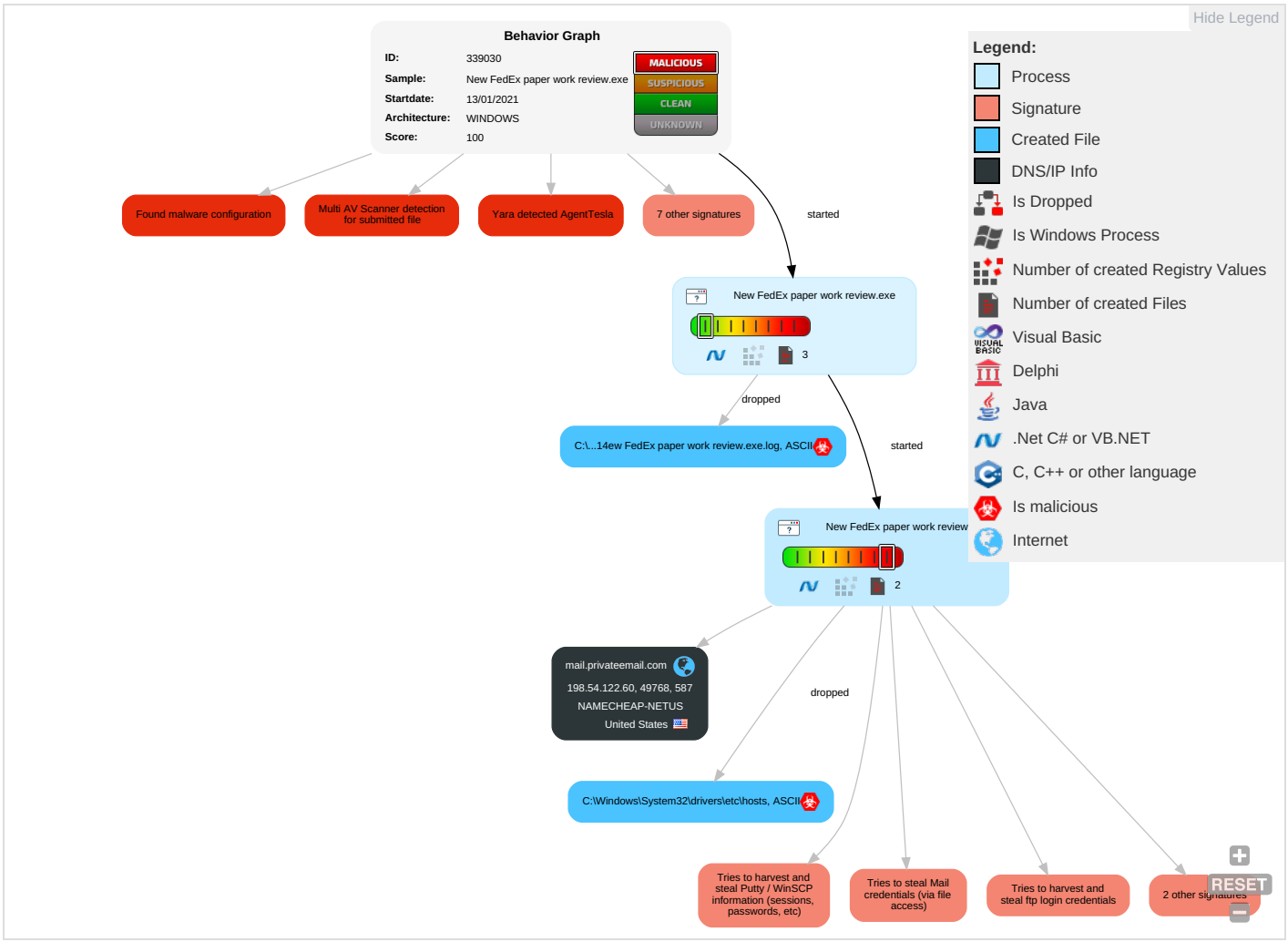
Remote Access Functionality:

Yara detected AgentTesla

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	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	File and Directory Permissions Modification 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3	Security Account Manager	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 1 1 4	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	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

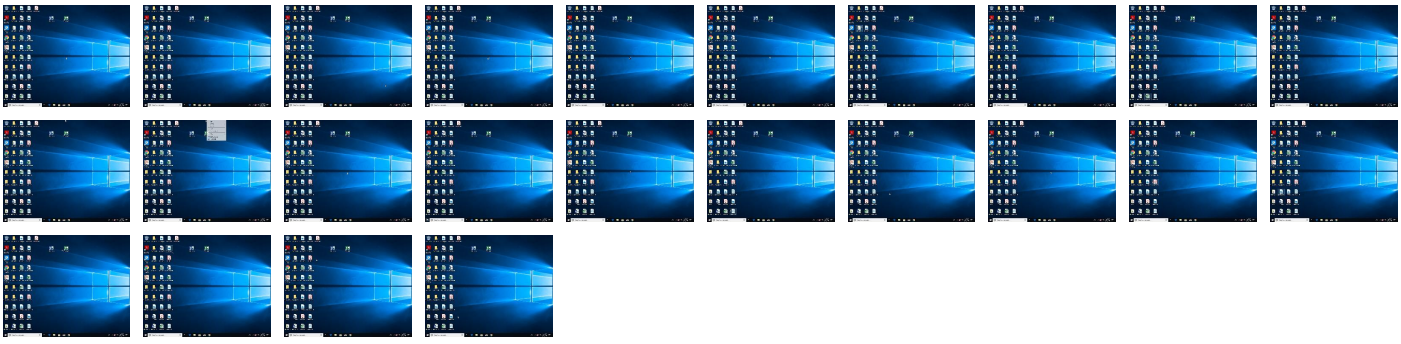
Behavior Graph



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
New FedEx paper work review.exe	31%	Virustotal		Browse
New FedEx paper work review.exe	25%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
New FedEx paper work review.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.New FedEx paper work review.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	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://jeQsgpMQfgg21VTI.net	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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://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://TSGxUW.com	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.privateemail.com	198.54.122.60	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://jeQsgpMQfgg21VTI.net	true	• Avira URL Cloud: safe	unknown

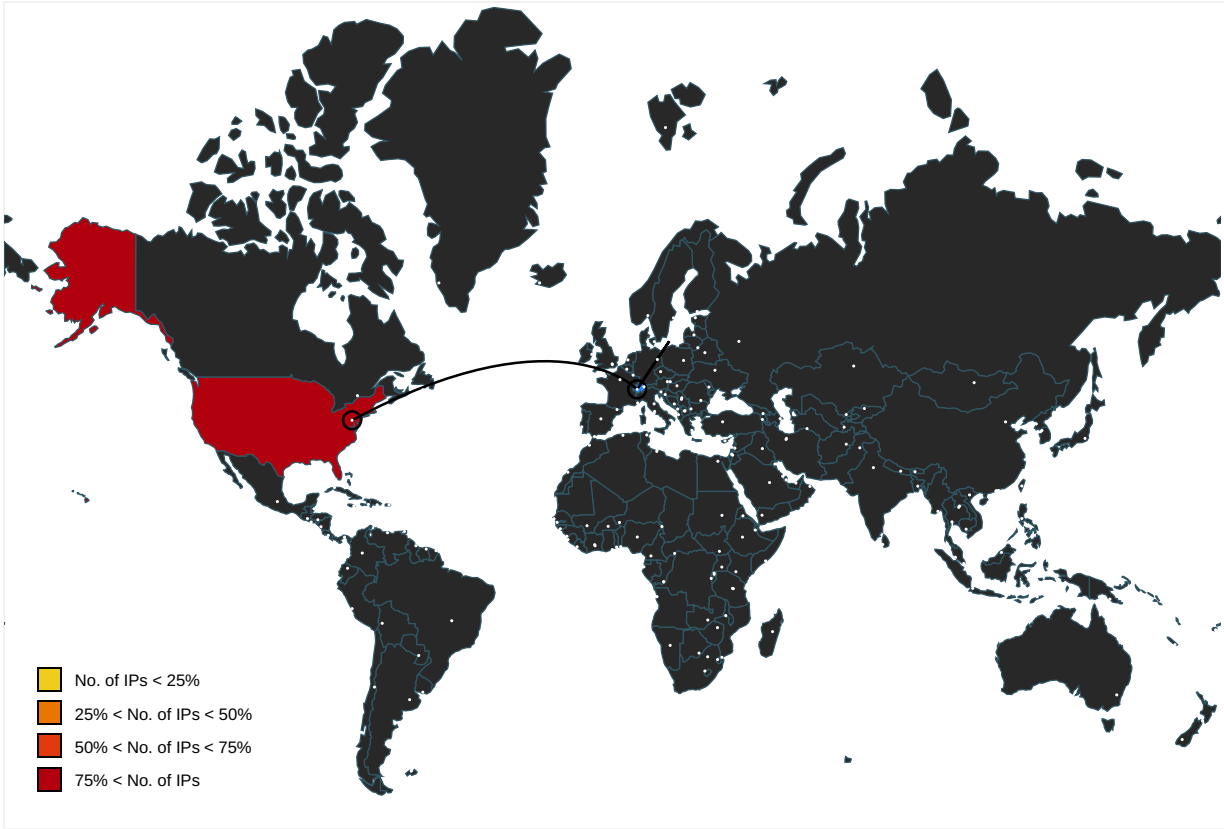
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	New FedEx paper work review.exe, 00000001.00000002.1028976039.00000000031CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	New FedEx paper work review.exe, 00000001.00000002.1028180638.0000000002E61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	New FedEx paper work review.exe, 00000001.00000002.1028180638.0000000002E61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	New FedEx paper work review.exe, 00000001.00000002.1028976039.00000000031CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	New FedEx paper work review.exe, 00000001.00000002.1028976039.00000000031CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Copyright null 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.privateemail.com	New FedEx paper work review.exe, 00000001.00000002.102895530 5.00000000031C8000.00000004.00 000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	New FedEx paper work review.exe, 00000001.00000002.102818063 8.0000000002E61000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	New FedEx paper work review.exe, 00000000.00000002.675657030 .0000000003271000.00000004.000 00001.sdmp	false		high
http://TSGxUW.com	New FedEx paper work review.exe, 00000001.00000002.102818063 8.0000000002E61000.00000004.00 000001.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	New FedEx paper work review.exe, 00000000.00000002.677503823 .0000000004271000.00000004.000 00001.sdmp, New FedEx paper work review.exe, 00000001.000000 02.1026177897.0000000000402000 .00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.122.60	unknown	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339030
Start date:	13.01.2021
Start time:	09:41:23
Joe Sandbox Product:	CloudBasic

Copyright null 2021

Overall analysis duration:	0h 9m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New FedEx paper work review.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:	14
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@3/2@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 55.7% • Quality standard deviation: 17.5%
HCA Information:	• Successful, ratio: 100% • 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 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 51.104.139.180, 52.147.198.201, 52.155.217.156, 20.54.26.129, 2.20.142.210, 2.20.142.209, 92.122.213.247, 92.122.213.194, 168.61.161.212, 51.11.168.160 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • 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
09:42:22	API Interceptor	1074x Sleep call for process: New FedEx paper work review.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.122.60	New paper work document attached.exe	Get hash	malicious	Browse	
	DHL_AWB_1928493383.exe	Get hash	malicious	Browse	
	PGXPHWCclJQdkUDcrlQETWlRbmXQw.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.tc.exe	Get hash	malicious	Browse	
	gc2hl6HPAVH5h1p.exe	Get hash	malicious	Browse	
	DHL7472579410110100.PDF.exe	Get hash	malicious	Browse	
	PO-104_171220.exe	Get hash	malicious	Browse	
	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	
	EOI5670995098732.exe	Get hash	malicious	Browse	
	INQUIRY- NET MACHINES-122020.doc	Get hash	malicious	Browse	
	EE09TR0098654.exe	Get hash	malicious	Browse	
	ENS003.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.6124.20146.exe	Get hash	malicious	Browse	
	RivHwa3Ral.exe	Get hash	malicious	Browse	
	HTML E-mail .doc	Get hash	malicious	Browse	
	dhl package delivery paperwork review for you.exe	Get hash	malicious	Browse	
	DOCUMENT.bat.exe	Get hash	malicious	Browse	
	SafeHashHandle.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis9C2423680592.exe	Get hash	malicious	Browse	
	4154038104 Quotation.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.privateemail.com	New paper work document attached.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL_AWB_1928493383.exe	Get hash	malicious	Browse	• 198.54.122.60
	PGXPHWCclJQdkUDcrlQETWlRbmXQw.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.tc.exe	Get hash	malicious	Browse	• 198.54.122.60
	gc2hl6HPAVH5h1p.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL7472579410110100.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO-104_171220.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	• 198.54.122.60
	P)141229202021.exe	Get hash	malicious	Browse	• 198.54.122.60
	EOI5670995098732.exe	Get hash	malicious	Browse	• 198.54.122.60
	INQUIRY- NET MACHINES-122020.doc	Get hash	malicious	Browse	• 198.54.122.60
	EE09TR0098654.exe	Get hash	malicious	Browse	• 198.54.122.60
	ENS003.xls	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.Inject4.6124.20146.exe	Get hash	malicious	Browse	• 198.54.122.60
	HTML E-mail .doc	Get hash	malicious	Browse	• 198.54.122.60
	dhl package delivery paperwork review for you.exe	Get hash	malicious	Browse	• 198.54.122.60
	DOCUMENT.bat.exe	Get hash	malicious	Browse	• 198.54.122.60
	SafeHashHandle.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Artemis9C2423680592.exe	Get hash	malicious	Browse	• 198.54.122.60
	4154038104 Quotation.xlsx	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	PO-000202112.exe	Get hash	malicious	Browse	• 63.250.34.114
	urgent specification request.exe	Get hash	malicious	Browse	• 198.54.117.210
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 198.54.117.210
	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Project review_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	mscthef-Fichero-ES.msi	Get hash	malicious	Browse	• 162.255.118.194
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order -263.exe	Get hash	malicious	Browse	• 162.0.232.59
	Duty checklist and PTP letter.exe	Get hash	malicious	Browse	• 162.255.119.136
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 162.0.238.245
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 198.54.117.216
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	RFQ 41680.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Invoice.exe	Get hash	malicious	Browse	• 162.213.255.55
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	• 199.193.7.228
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 68.65.122.35
	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	• 198.54.125.162
	al9LrOC8eM.exe	Get hash	malicious	Browse	• 162.213.253.37
	hcL39YT1CR.exe	Get hash	malicious	Browse	• 162.213.253.37

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New FedEx paper work review.exe.log

Process:	C:\Users\user\Desktop\New FedEx paper work review.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:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\Desktop\New FedEx paper work review.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4

C:\Windows\System32\drivers\etc\hosts	
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.463428843466992
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:	New FedEx paper work review.exe
File size:	811520
MD5:	c359c954a7d104b0a1bde867f86e73a5
SHA1:	e647c8aa88a7209463b0dd0daa733759a529806d
SHA256:	306602e7317841b219d25b24ca14f9e50987fe9c9e48b3728bb548dea4557f9d
SHA512:	8f48d07be0342db4a946b5c74598eb5dbe565bbf0c7ed2a5f6b5ab7b99577f0e8463004f601d0286bcaebf5a673e18e83d9b8f319e5566f28b59e2ebc3a18644
SSDEEP:	12288:Ew+Bv0KOZFLUqAKtlvwHY+zOmO0GXpUaJNbKrYiYY:Ew+BvtOXvAK/Y4N0cUCNWEY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...C..._.....P..N.....m... .....@.. .....@.....

File Icon

Icon Hash:	e05060523000d88c

Static PE Info

General

Entrypoint:	0x4b6db2
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:	0x5FFDDC43 [Tue Jan 12 17:28:35 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
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

Copyright null 2021

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	0xb6d60	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x10ed8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	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	0xb4db8	0xb4e00	False	0.762650095024	data	7.44963037864	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x10ed8	0x11000	False	0.427949793199	data	6.36617798911	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Copyright null 2021

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb8130	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 4293061103, next used block 4292995310		
RT_GROUP_ICON	0xc8958	0x14	data		
RT_VERSION	0xc896c	0x380	data		
RT_MANIFEST	0xc8cec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

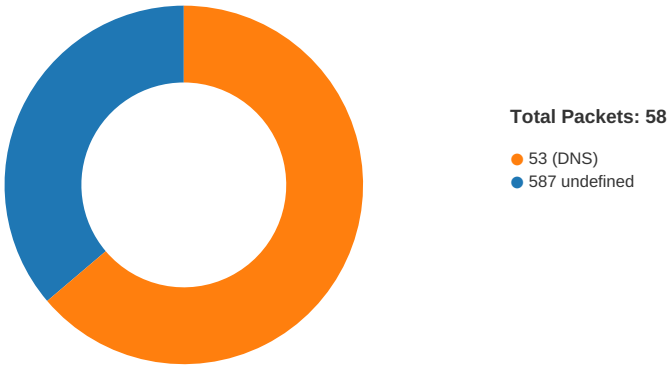
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hewlett-Packard 2016
Assembly Version	1.0.0.0
InternalName	StreamTokenReader.exe
FileVersion	1.0.0.0
CompanyName	Hewlett-Packard
LegalTrademarks	
Comments	
ProductName	GameManager
ProductVersion	1.0.0.0
FileDescription	GameManager
OriginalFilename	StreamTokenReader.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 09:44:05.861316919 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:06.054965019 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:06.055231094 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:06.250818014 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:06.251322985 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:06.444350958 CET	587	49768	198.54.122.60	192.168.2.4

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 09:44:06.444695950 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:06.444981098 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:06.637991905 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:06.681092024 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:06.723992109 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:06.917056084 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:06.918883085 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:06.918912888 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:06.918936968 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:06.918961048 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:06.919043064 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:06.919080019 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:06.942835093 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:07.136101007 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:07.136905909 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:07.136965036 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:07.137121916 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:07.424300909 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:07.617464066 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:07.618174076 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:07.620884895 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:07.813910007 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:07.815541983 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:07.816860914 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:08.009815931 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.013567924 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.014631987 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:08.207633018 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.212371111 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.213630915 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:08.406898975 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.445427895 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.446022987 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:08.639003992 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.640458107 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.643500090 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:08.643796921 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:08.644623041 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:08.644814014 CET	49768	587	192.168.2.4	198.54.122.60
Jan 13, 2021 09:44:08.836477041 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.836613894 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.837374926 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.837713957 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.885276079 CET	587	49768	198.54.122.60	192.168.2.4
Jan 13, 2021 09:44:08.931380033 CET	49768	587	192.168.2.4	198.54.122.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 09:42:18.746437073 CET	53097	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:18.802710056 CET	53	53097	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:21.820112944 CET	49257	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:21.870971918 CET	53	49257	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:36.840665102 CET	62389	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:36.891519070 CET	53	62389	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:44.771374941 CET	49910	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:44.819255114 CET	53	49910	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:45.866219997 CET	55854	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:45.922363997 CET	53	55854	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:46.736913919 CET	64549	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:46.784745932 CET	53	64549	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:53.475615978 CET	63153	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:53.542154074 CET	53	63153	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:54.387048960 CET	52991	53	192.168.2.4	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 09:42:54.421209097 CET	53700	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:54.434885979 CET	53	52991	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:54.469069958 CET	53	53700	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:55.070533991 CET	51726	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:55.126840115 CET	53	51726	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:55.552237034 CET	56794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:55.600234032 CET	53	56794	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:55.780966997 CET	56534	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:55.847170115 CET	53	56534	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:56.342020988 CET	56627	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:56.392725945 CET	53	56627	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:56.950464010 CET	56621	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:57.009727955 CET	53	56621	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:57.702738047 CET	63116	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:57.801652908 CET	53	63116	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:58.025569916 CET	64078	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:58.086752892 CET	53	64078	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:58.660417080 CET	64801	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:58.717272043 CET	53	64801	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:58.928756952 CET	61721	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:58.995296001 CET	53	61721	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:59.628201008 CET	51255	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:59.678992987 CET	53	51255	8.8.8.8	192.168.2.4
Jan 13, 2021 09:42:59.733860016 CET	61522	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:42:59.784651995 CET	53	61522	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:00.298059940 CET	52337	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:00.346180916 CET	53	52337	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:13.017586946 CET	55046	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:13.060118914 CET	49612	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:13.065568924 CET	53	55046	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:13.131640911 CET	53	49612	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:16.568377018 CET	49285	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:16.627130985 CET	53	49285	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:17.703425884 CET	50601	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:17.754086018 CET	53	50601	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:18.558366060 CET	60875	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:18.609303951 CET	53	60875	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:20.675477982 CET	56448	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:20.723412037 CET	53	56448	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:27.415399075 CET	59172	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:27.466418982 CET	53	59172	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:30.510581970 CET	62420	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:30.558646917 CET	53	62420	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:32.326744080 CET	60579	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:32.382956982 CET	53	60579	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:42.601813078 CET	50183	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:42.649622917 CET	53	50183	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:47.036323071 CET	61531	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:47.087133884 CET	53	61531	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:49.988044024 CET	49228	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:50.039341927 CET	53	49228	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:50.587236881 CET	59794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:50.635184050 CET	53	59794	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:51.574821949 CET	55916	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:51.631432056 CET	53	55916	8.8.8.8	192.168.2.4
Jan 13, 2021 09:43:57.725897074 CET	52752	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:43:57.776616096 CET	53	52752	8.8.8.8	192.168.2.4
Jan 13, 2021 09:44:05.706096888 CET	60542	53	192.168.2.4	8.8.8.8
Jan 13, 2021 09:44:05.756928921 CET	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 09:44:05.706096888 CET	192.168.2.4	8.8.8.8	0x8726	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 09:44:05.756928921 CET	8.8.8.8	192.168.2.4	0x8726	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

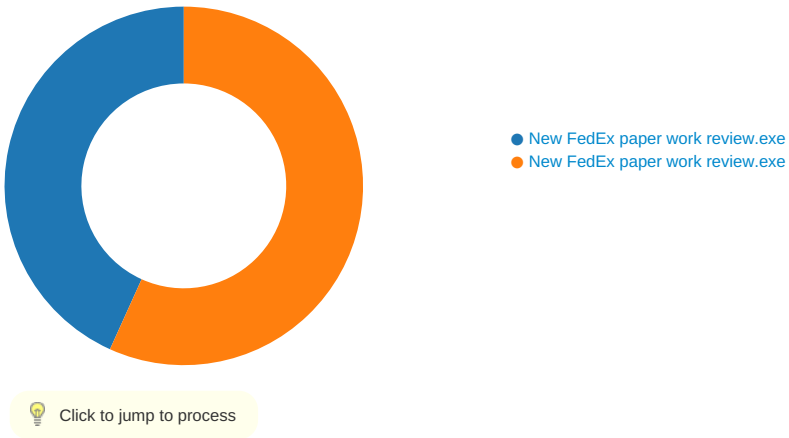
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 09:44:06.250818014 CET	587	49768	198.54.122.60	192.168.2.4	220 PrivateEmail.com prod Mail Node
Jan 13, 2021 09:44:06.251322985 CET	49768	587	192.168.2.4	198.54.122.60	EHLO 210979
Jan 13, 2021 09:44:06.444695950 CET	587	49768	198.54.122.60	192.168.2.4	250-mta-11.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 13, 2021 09:44:06.444981098 CET	49768	587	192.168.2.4	198.54.122.60	STARTTLS
Jan 13, 2021 09:44:06.637991905 CET	587	49768	198.54.122.60	192.168.2.4	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: New FedEx paper work review.exe PID: 5956 Parent PID: 6140

General

Start time:	09:42:15

Start date:	13/01/2021
Path:	C:\Users\user\Desktop\New FedEx paper work review.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New FedEx paper work review.exe'
Imagebase:	0xe00000
File size:	811520 bytes
MD5 hash:	C359C954A7D104B0A1BDE867F86E73A5
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: 00000000.00000002.675657030.0000000003271000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.677503823.0000000004271000.00000004.00000001.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	6D3DCF06	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	6D3DCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New FedEx paper work review.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\New FedEx paper work review.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	6D6EC907	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	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: New FedEx paper work review.exe PID: 3912 Parent PID: 5956

General

Start time:	09:42:23
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\New FedEx paper work review.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\New FedEx paper work review.exe
Imagebase:	0xa30000
File size:	811520 bytes
MD5 hash:	C359C954A7D104B0A1BDE867F86E73A5
Has elevated privileges:	true

Copyright null 2021

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.1028180638.0000000002E61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.1028180638.0000000002E61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.1026177897.0000000000402000.00000040.00000001.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	6D3DCF06	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	6D3DCF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	unknown	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	..127.0.0.1	success or wait	1	6C221B4F	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	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\693d5ee2-a966-4b94-9ffe-82d68baea1dc	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C221B4F	ReadFile

Disassembly

Copyright null 2021

Code Analysis