ID: 404170
Sample Name:
pd9EeXdsQtNb3dQ.exe
Cookbook: default.jbs
Time: 19:12:16
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

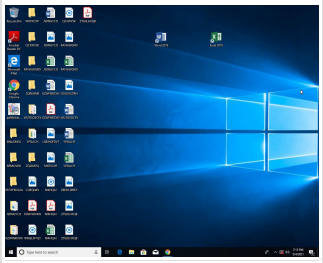
Analysis Report pd9EeXdsQtNb3dQ.exe

Overview

General Information

Sample Name:	pd9EeXdsQtNb3dQ.exe
Analysis ID:	404170
MD5:	3dad3d4918e28d..
SHA1:	8b16dba4992b75..
SHA256:	1b61b157db5065..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

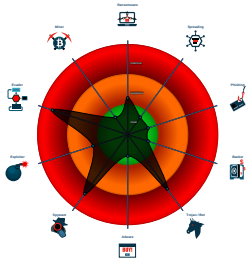
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Injects a PE file into a foreign proce…
- 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…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…
- Antivirus or Machine Learning detec…
- Contains functionality for execution …

Classification



Startup

- **System is w10x64**
- pd9EeXdsQtNb3dQ.exe (PID: 6472 cmdline: 'C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe' MD5: 3DAD3D4918E28DED77C3E2E93A42665F)
  - pd9EeXdsQtNb3dQ.exe (PID: 6620 cmdline: C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe MD5: 3DAD3D4918E28DED77C3E2E93A42665F)
  - pd9EeXdsQtNb3dQ.exe (PID: 6636 cmdline: C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe MD5: 3DAD3D4918E28DED77C3E2E93A42665F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "office5@iykmoreentrprise.orgrwkWCM328mail.iykmoreentrprise.org"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.587167948.000000000303 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.587167948.000000000303 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000000.00000002.333313035.00000000037F 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.582976077.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.332108343.000000000284 8000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

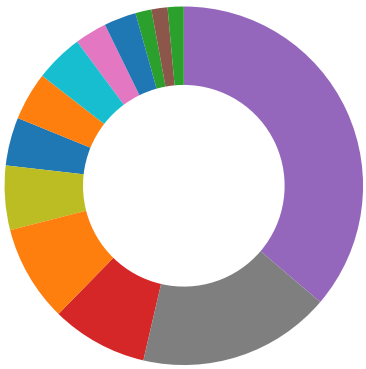
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.pd9EeXdsQtNb3dQ.exe.390c790.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.pd9EeXdsQtNb3dQ.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.pd9EeXdsQtNb3dQ.exe.390c790.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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)

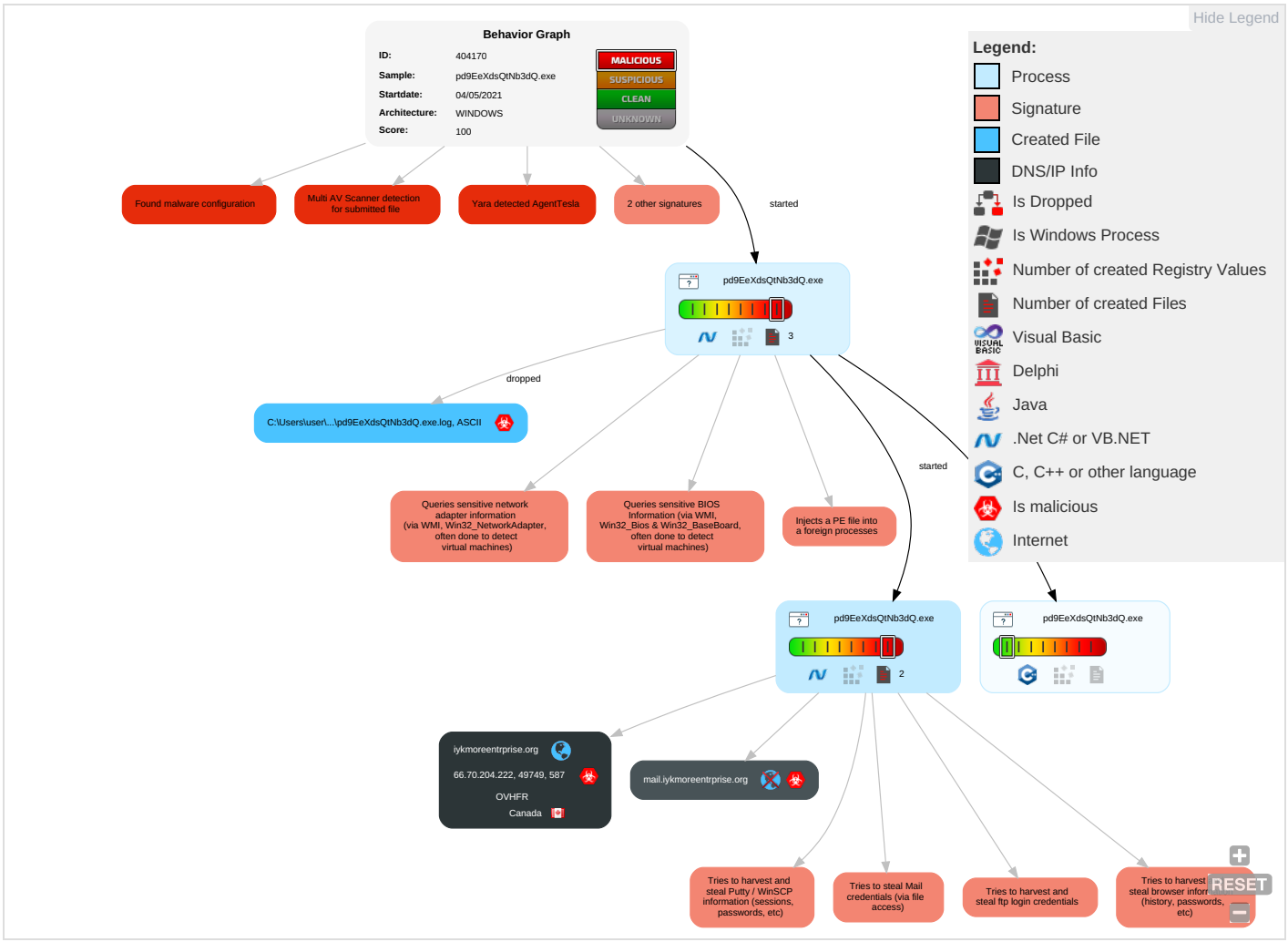
Remote Access Functionality:

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 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	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	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)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

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
pd9EeXdsQtNb3dQ.exe	14%	Virustotal		Browse
pd9EeXdsQtNb3dQ.exe	52%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.pd9EeXdsQtNb3dQ.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://iykmoreentrprise.org	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://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://NtZtA8FE2WmoFQd.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%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://DXvqav.com	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://tempuri.org/Shops_DBDataSet.xsd9WinForms_RecursiveFormCreate5WinForms_SeeInnerExceptionGProp ope	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://mail.iykmoreentrprise.org	0%	Avira URL Cloud	safe	
http://tempuri.org/Shops_DBDataSet.xsd	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

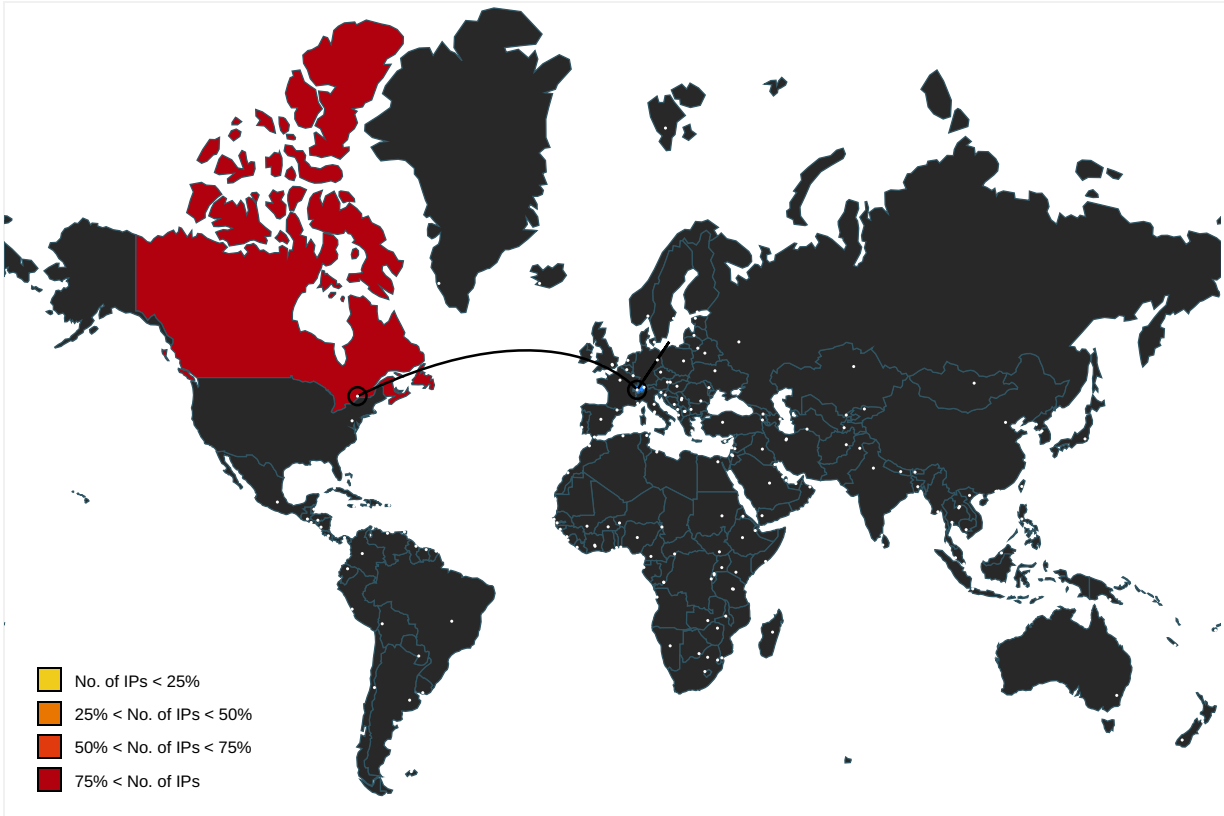
Name	IP	Active	Malicious	Antivirus Detection	Reputation
iykmoreentrprise.org	66.70.204.222	true	true		unknown
mail.iykmoreentrprise.org	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.587167948.0000000003031000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iykmoreentrprise.org	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.588712219.0000000003398000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.587167948.0000000003031000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.588755539.00000000033A6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://NtZtA8FE2WmoFQd.com	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.587167948.0000000003031000.00000004.00000001.sdmp, pd9EeXdsQtNb3dQ.exe, 00000003.00000002.588834930.00000000033C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.587167948.0000000003031000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DXvqav.com	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.587167948.0000000003031000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.588755539.00000000033A6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Shops_DBDataSet.xsd9WinForms_RecursiveFormCreate5WinForms_SeeInnerExceptionGPrope	pd9EeXdsQtNb3dQ.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.587167948.0000000003031000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	pd9EeXdsQtNb3dQ.exe, 00000000.00000002.331949813.00000000027F1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	pd9EeXdsQtNb3dQ.exe, 00000000.00000002.333313035.00000000037F9000.00000004.00000001.sdmp, pd9EeXdsQtNb3dQ.exe, 00000003.00000002.582976077.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	pd9EeXdsQtNb3dQ.exe, 00000000.00000002.332108343.0000000002848000.00000004.00000001.sdmp	false		high
http://mail.iykmoreentrprise.org	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.588712219.0000000003398000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/Shops_DBDataSet.xsd	pd9EeXdsQtNb3dQ.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%$	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.587167948.0000000003031000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://cps.root-x1.letsencrypt.org0	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.588712219.0000000003398000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0	pd9EeXdsQtNb3dQ.exe, 00000003.00000002.588755539.00000000033A6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.70.204.222	iykmoreentrprise.org	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404170
Start date:	04.05.2021
Start time:	19:12:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pd9EeXdsQtNb3dQ.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/1@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 104.43.139.144, 92.122.145.220, 13.64.90.137, 104.43.193.48, 2.23.155.184, 2.23.155.241, 2.23.155.219, 2.23.155.240, 20.82.210.154, 92.122.213.247, 92.122.213.194, 205.185.216.10, 205.185.216.42, 52.155.217.156, 20.54.26.129, 23.57.80.111 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, a767.dspw65.akamai.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, download.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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
19:13:04	API Interceptor	677x Sleep call for process: pd9EeXdsQtNb3dQ.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.70.204.222	SecuriteInfo.com.W32.MSIL_Troj.ASI.genEldorado.27642.exe	Get hash	malicious	Browse	
	MZyeln5mSFOjxMx.exe	Get hash	malicious	Browse	
	FFrIJMwrI9cxeIZ.exe	Get hash	malicious	Browse	
	cljz48xwqb2VSBN.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QTY 98657 RFQ MANDATE 020521.0003YDK.exe	Get hash	malicious	Browse	
	foakTEjUOvL9nBY.exe	Get hash	malicious	Browse	
	n4QstFh7YkjVcrU.exe	Get hash	malicious	Browse	
	AVuOP2vLzIMRG88.exe	Get hash	malicious	Browse	
	316e3796_by_Libranalysis.exe	Get hash	malicious	Browse	
	GQTY 98657 RFQ MANDATE 28421.02AWYD.exe	Get hash	malicious	Browse	
	VJNPltkyHyI3CCo.exe	Get hash	malicious	Browse	
	0L2qr7kJMh40sxq.exe	Get hash	malicious	Browse	
	ApuE9QrdQxe7Um6.exe	Get hash	malicious	Browse	
	77iET1jNLJyV8ez.exe	Get hash	malicious	Browse	
	bOkrXdoYekZPyWI.exe	Get hash	malicious	Browse	
	ayZYB5SkqMPA06M.exe	Get hash	malicious	Browse	
	fyZ6iHys7ClIHFR.exe	Get hash	malicious	Browse	
	uMLNLd9kgPez84h.exe	Get hash	malicious	Browse	
	YQfInBo2DDpDfIX.exe	Get hash	malicious	Browse	
	ORDER 700198.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	SecuriteInfo.com.W32.MSIL_Troj.ASI.genEldorado.27642.exe	Get hash	malicious	Browse	• 66.70.204.222
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	New Order Request_0232147.exe	Get hash	malicious	Browse	• 149.202.85.210
	Transcation03232016646pdf.exe	Get hash	malicious	Browse	• 79.137.109.121
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	MZyeln5mSFOjxMx.exe	Get hash	malicious	Browse	• 66.70.204.222
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	51086cc4_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	8aa43191_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	51086cc4_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	8aa43191_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	840e7dfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	840e7dfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	94765446_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	d192feb6_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	7bc33f1c_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	94765446_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pd9EeXdsQtNb3dQ.exe.log

Process:	C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pd9EeXdsQtNb3dQ.exe.log	
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.607400063403851
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	pd9EeXdsQtNb3dQ.exe
File size:	2330624
MD5:	3dad3d4918e28ded77c3e2e93a42665f
SHA1:	8b16dba4992b75a303f63a09d8a41ac99f28ce5c
SHA256:	1b61b157db50652678e1e288cfce86f6c74e40f50a468f6d04d0010c84235210
SHA512:	57173561296c538c174c3299ea6b64156c48977d8f958f86f14578d4a630ea80e7b6b890e6d1a21f94a1d556173db442b953b685de910f25d886cdeda88b3132
SSDEEP:	24576:sPlzZc9mZUzZZE1XcEoLfOo5MkdoG1eJk14kocZmPBDmIO:sPlz2tZauEoL3McoG1gcw3d
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..J#..D.....i#.. ....#...@.. .....$.....@.....

File Icon

Icon Hash:	07032d1f0527471b

Static PE Info

General

Entrypoint:	0x636912
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:	0x60909F0A [Tue May 4 01:10:34 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General	
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2368c0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x238000	0x41e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x23e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x236788	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x234918	0x234a00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x238000	0x41e8	0x4200	False	0.514441287879	data	5.44364934449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x23e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x238140	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x2385b8	0x10a8	data		
RT_ICON	0x239670	0x25a8	data		
RT_GROUP_ICON	0x23bc28	0x30	data		
RT_VERSION	0x23bc68	0x380	data		
RT_MANIFEST	0x23bff8	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 Gilbert Adjin Frimpong
Assembly Version	1.0.0.0
InternalName	IMethodMessage.exe
FileVersion	1.0.0.0
CompanyName	Gilbert Adjin
LegalTrademarks	
Comments	
ProductName	Shop Manager
ProductVersion	1.0.0.0
FileDescription	Shop Manager
OriginalFilename	IMethodMessage.exe

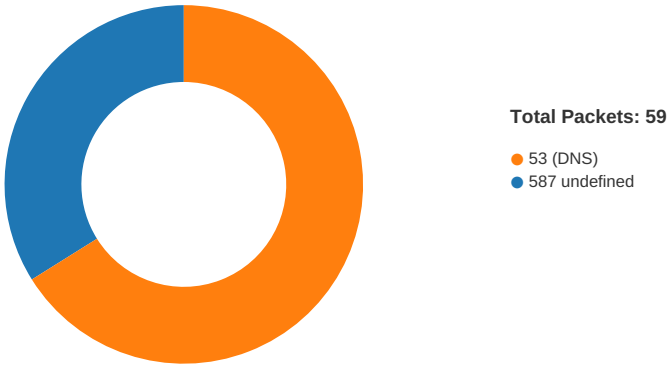
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-19:13:07.551654	ICMP	384	ICMP PING			192.168.2.6	2.23.155.184
05/04/21-19:13:07.586777	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/04/21-19:13:07.590236	ICMP	384	ICMP PING			192.168.2.6	2.23.155.184
05/04/21-19:13:07.625531	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6
05/04/21-19:13:07.628818	ICMP	384	ICMP PING			192.168.2.6	2.23.155.184
05/04/21-19:13:07.664673	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.49.165	192.168.2.6
05/04/21-19:13:07.665430	ICMP	384	ICMP PING			192.168.2.6	2.23.155.184

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-19:13:07.706276	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.18	192.168.2.6
05/04/21-19:13:07.706835	ICMP	384	ICMP PING			192.168.2.6	2.23.155.184
05/04/21-19:13:07.753450	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.53	192.168.2.6
05/04/21-19:13:07.754164	ICMP	384	ICMP PING			192.168.2.6	2.23.155.184
05/04/21-19:13:07.800340	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.15.66	192.168.2.6
05/04/21-19:13:07.800797	ICMP	384	ICMP PING			192.168.2.6	2.23.155.184
05/04/21-19:13:07.869203	ICMP	449	ICMP Time-To-Live Exceeded in Transit			195.22.208.79	192.168.2.6
05/04/21-19:13:07.869689	ICMP	384	ICMP PING			192.168.2.6	2.23.155.184
05/04/21-19:13:07.925619	ICMP	449	ICMP Time-To-Live Exceeded in Transit			93.186.128.39	192.168.2.6
05/04/21-19:13:07.926043	ICMP	384	ICMP PING			192.168.2.6	2.23.155.184
05/04/21-19:13:07.981484	ICMP	408	ICMP Echo Reply			2.23.155.184	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:14:51.980122089 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:52.110054970 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:52.110392094 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:52.364695072 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:52.367636919 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:52.497628927 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:52.500775099 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:52.632188082 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:52.688940048 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:52.813638926 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:52.951697111 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:52.951724052 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:52.951740980 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:52.952095985 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:52.962678909 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:53.092824936 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:53.151324987 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:53.413399935 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:53.543329954 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:53.546207905 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:53.676331997 CEST	587	49749	66.70.204.222	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:14:53.677742004 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:53.817493916 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:53.819114923 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:53.949096918 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:53.949945927 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:54.084723949 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:54.086483002 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:54.216568947 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:54.218698025 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:54.220149994 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:54.220159054 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:54.220666885 CEST	49749	587	192.168.2.6	66.70.204.222
May 4, 2021 19:14:54.348767996 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:54.349998951 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:54.350048065 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:54.350409985 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:54.352190018 CEST	587	49749	66.70.204.222	192.168.2.6
May 4, 2021 19:14:54.404773951 CEST	49749	587	192.168.2.6	66.70.204.222

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:12:55.261626959 CEST	53	55074	8.8.8.8	192.168.2.6
May 4, 2021 19:12:55.308217049 CEST	53	54513	8.8.8.8	192.168.2.6
May 4, 2021 19:12:55.551229000 CEST	62044	53	192.168.2.6	8.8.8.8
May 4, 2021 19:12:55.602710962 CEST	53	62044	8.8.8.8	192.168.2.6
May 4, 2021 19:12:56.129103899 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 19:12:56.178004980 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 19:12:57.219885111 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 19:12:57.268503904 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 19:12:58.298722029 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 19:12:58.347269058 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 19:12:59.664602041 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 19:12:59.716080904 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 19:13:00.875519037 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:00.924422979 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 19:13:01.798768997 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:01.847732067 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 19:13:02.920011044 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:02.977190018 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 19:13:05.301472902 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:05.353072882 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 19:13:06.209592104 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:06.261039972 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 19:13:07.310122013 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:07.358989000 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 19:13:07.479265928 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:07.547488928 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 19:13:08.400338888 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:08.449090004 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 19:13:09.320982933 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:09.378413916 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 19:13:10.372736931 CEST	52811	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:10.424382925 CEST	53	52811	8.8.8.8	192.168.2.6
May 4, 2021 19:13:11.464569092 CEST	55299	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:11.516076088 CEST	53	55299	8.8.8.8	192.168.2.6
May 4, 2021 19:13:12.625581026 CEST	63745	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:12.674526930 CEST	53	63745	8.8.8.8	192.168.2.6
May 4, 2021 19:13:13.907864094 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:13.956675053 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 19:13:14.833376884 CEST	61374	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:14.881973028 CEST	53	61374	8.8.8.8	192.168.2.6
May 4, 2021 19:13:29.440428972 CEST	50339	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:29.489309072 CEST	53	50339	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:13:33.206162930 CEST	63307	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:33.265320063 CEST	53	63307	8.8.8.8	192.168.2.6
May 4, 2021 19:13:50.792989016 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:50.841618061 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 19:13:50.977421045 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:51.106905937 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 19:13:51.666131020 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:51.879602909 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 19:13:52.023197889 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:52.095563889 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 19:13:52.414561033 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:52.474335909 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 19:13:52.947563887 CEST	63816	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:53.231540918 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 19:13:53.776989937 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:53.834268093 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 19:13:54.380311966 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:54.431982040 CEST	53	62208	8.8.8.8	192.168.2.6
May 4, 2021 19:13:55.107546091 CEST	57574	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:55.165186882 CEST	53	57574	8.8.8.8	192.168.2.6
May 4, 2021 19:13:56.469089031 CEST	51818	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:56.532123089 CEST	53	51818	8.8.8.8	192.168.2.6
May 4, 2021 19:13:58.452529907 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:58.512274027 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 19:13:59.010509968 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 19:13:59.059247017 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 19:14:05.857558966 CEST	53799	53	192.168.2.6	8.8.8.8
May 4, 2021 19:14:05.918920994 CEST	53	53799	8.8.8.8	192.168.2.6
May 4, 2021 19:14:37.559355021 CEST	54683	53	192.168.2.6	8.8.8.8
May 4, 2021 19:14:37.611212015 CEST	53	54683	8.8.8.8	192.168.2.6
May 4, 2021 19:14:38.171545029 CEST	59329	53	192.168.2.6	8.8.8.8
May 4, 2021 19:14:38.251847029 CEST	53	59329	8.8.8.8	192.168.2.6
May 4, 2021 19:14:39.192359924 CEST	64021	53	192.168.2.6	8.8.8.8
May 4, 2021 19:14:39.267153025 CEST	53	64021	8.8.8.8	192.168.2.6
May 4, 2021 19:14:51.694025040 CEST	56129	53	192.168.2.6	8.8.8.8
May 4, 2021 19:14:51.767874002 CEST	53	56129	8.8.8.8	192.168.2.6
May 4, 2021 19:14:51.796029091 CEST	58177	53	192.168.2.6	8.8.8.8
May 4, 2021 19:14:51.866108894 CEST	53	58177	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 19:14:51.694025040 CEST	192.168.2.6	8.8.8.8	0x9564	Standard query (0)	mail.iykmoreentrprise.org	A (IP address)	IN (0x0001)
May 4, 2021 19:14:51.796029091 CEST	192.168.2.6	8.8.8.8	0xaafe	Standard query (0)	mail.iykmoreentrprise.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 19:14:51.767874002 CEST	8.8.8.8	192.168.2.6	0x9564	No error (0)	mail.iykmoreentrprise.org	iykmoreentrprise.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:14:51.767874002 CEST	8.8.8.8	192.168.2.6	0x9564	No error (0)	iykmoreentrprise.org		66.70.204.222	A (IP address)	IN (0x0001)
May 4, 2021 19:14:51.866108894 CEST	8.8.8.8	192.168.2.6	0xaafe	No error (0)	mail.iykmoreentrprise.org	iykmoreentrprise.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:14:51.866108894 CEST	8.8.8.8	192.168.2.6	0xaafe	No error (0)	iykmoreentrprise.org		66.70.204.222	A (IP address)	IN (0x0001)

SMTP Packets

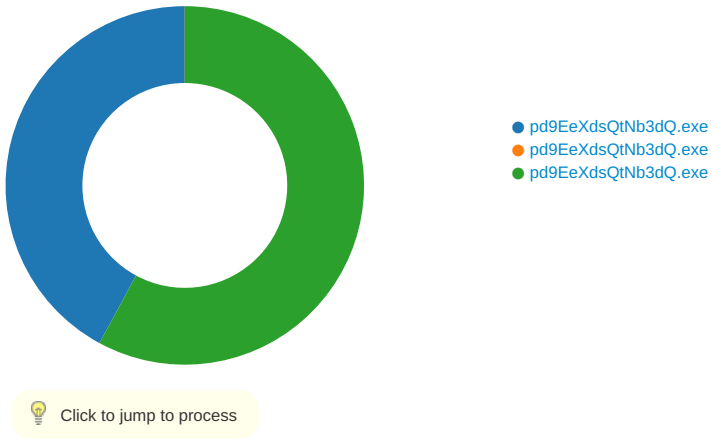
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 19:14:52.364695072 CEST	587	49749	66.70.204.222	192.168.2.6	220-server.wlcserver.com ESMTP Exim 4.94 #2 Tue, 04 May 2021 21:14:52 +0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 4, 2021 19:14:52.367636919 CEST	49749	587	192.168.2.6	66.70.204.222	EHLO 468325
May 4, 2021 19:14:52.497628927 CEST	587	49749	66.70.204.222	192.168.2.6	250-server.wlcserver.com Hello 468325 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-STARTTLS 250 HELP
May 4, 2021 19:14:52.500775099 CEST	49749	587	192.168.2.6	66.70.204.222	STARTTLS
May 4, 2021 19:14:52.632188082 CEST	587	49749	66.70.204.222	192.168.2.6	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: pd9EeXdsQtNb3dQ.exe PID: 6472 Parent PID: 5936

General

Start time:	19:13:01
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe'
Imagebase:	0x330000
File size:	2330624 bytes
MD5 hash:	3DAD3D4918E28DED77C3E2E93A42665F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.333313035.00000000037F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.332108343.0000000002848000.00000004.00000001.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	6E0ECF06	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	6E0ECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pd9EeXdsQtNb3dQ.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3FC78D	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\pd9EeXdsQtNb3dQ.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	6E3FC907	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	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0203DE	ReadFile

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	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	ReadFile

Analysis Process: pd9EeXdsQtNb3dQ.exe PID: 6620 Parent PID: 6472

General

Start time:	19:13:06
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe
Imagebase:	0x330000
File size:	2330624 bytes
MD5 hash:	3DAD3D4918E28DED77C3E2E93A42665F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: pd9EeXdsQtNb3dQ.exe PID: 6636 Parent PID: 6472

General

Start time:	19:13:07
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\pd9EeXdsQtNb3dQ.exe
Imagebase:	0xa90000
File size:	2330624 bytes
MD5 hash:	3DAD3D4918E28DED77C3E2E93A42665F
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: 00000003.00000002.587167948.0000000003031000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.587167948.0000000003031000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.582976077.0000000000402000.00000040.00000001.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	6E0ECF06	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	6E0ECF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CF31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\47964e06-8a01-45be-b8c0-c1d92431df55	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CF31B4F	ReadFile

Disassembly

Code Analysis