ID: 458829
Sample Name: Quotation From Asia Tianjin Steel Co.Ltd.exe
Cookbook: default.jbs
Time: 19:28:01
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

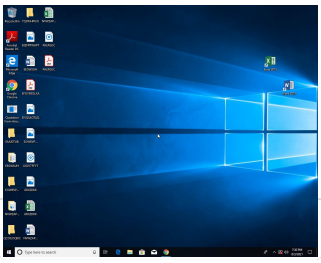
Windows Analysis Report Quotation From Asia Tianjin S…

Overview

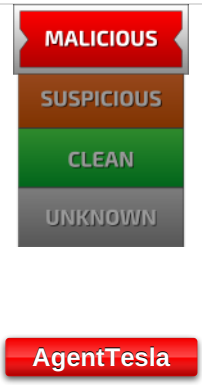
General Information

Sample Name:	Quotation From Asia Tianjin Steel Co.Ltd.exe
Analysis ID:	458829
MD5:	0fcf33a3980c44c…
SHA1:	f2aebb3e351e165.
SHA256:	6d877514b8301c..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

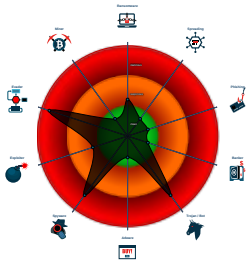


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- Found evasive API chain (trying to d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Quotation From Asia Tianjin Steel Co.Ltd.exe (PID: 5476 cmdline: 'C:\Users\user\Desktop\Quotation From Asia Tianjin Steel Co.Ltd.exe' MD5: 0FCF33A3980C44C176D519A4589028AA)
  - Quotation From Asia Tianjin Steel Co.Ltd.exe (PID: 1900 cmdline: C:\Users\user\Desktop\Quotation From Asia Tianjin Steel Co.Ltd.exe MD5: 0FCF33A3980C44C176D519A4589028AA)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "usernamegood@vivaldi.net",
  "Password": "aaaAAaaaawGoodPass@123@",
  "Host": "smtp.vivaldi.net"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.246514460.0000000003AF3000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.493730793.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.493730793.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.254121480.000000000A591000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.254121480.000000000A591000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.Quotation From Asia Tianjin Steel Co.Ltd.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.Quotation From Asia Tianjin Steel Co.Ltd.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Quotation From Asia Tianjin Steel Co.Ltd.exe.a6324b8.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Quotation From Asia Tianjin Steel Co.Ltd.exe.a6324b8.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Quotation From Asia Tianjin Steel Co.Ltd.exe.a6324b8.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM3

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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

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:

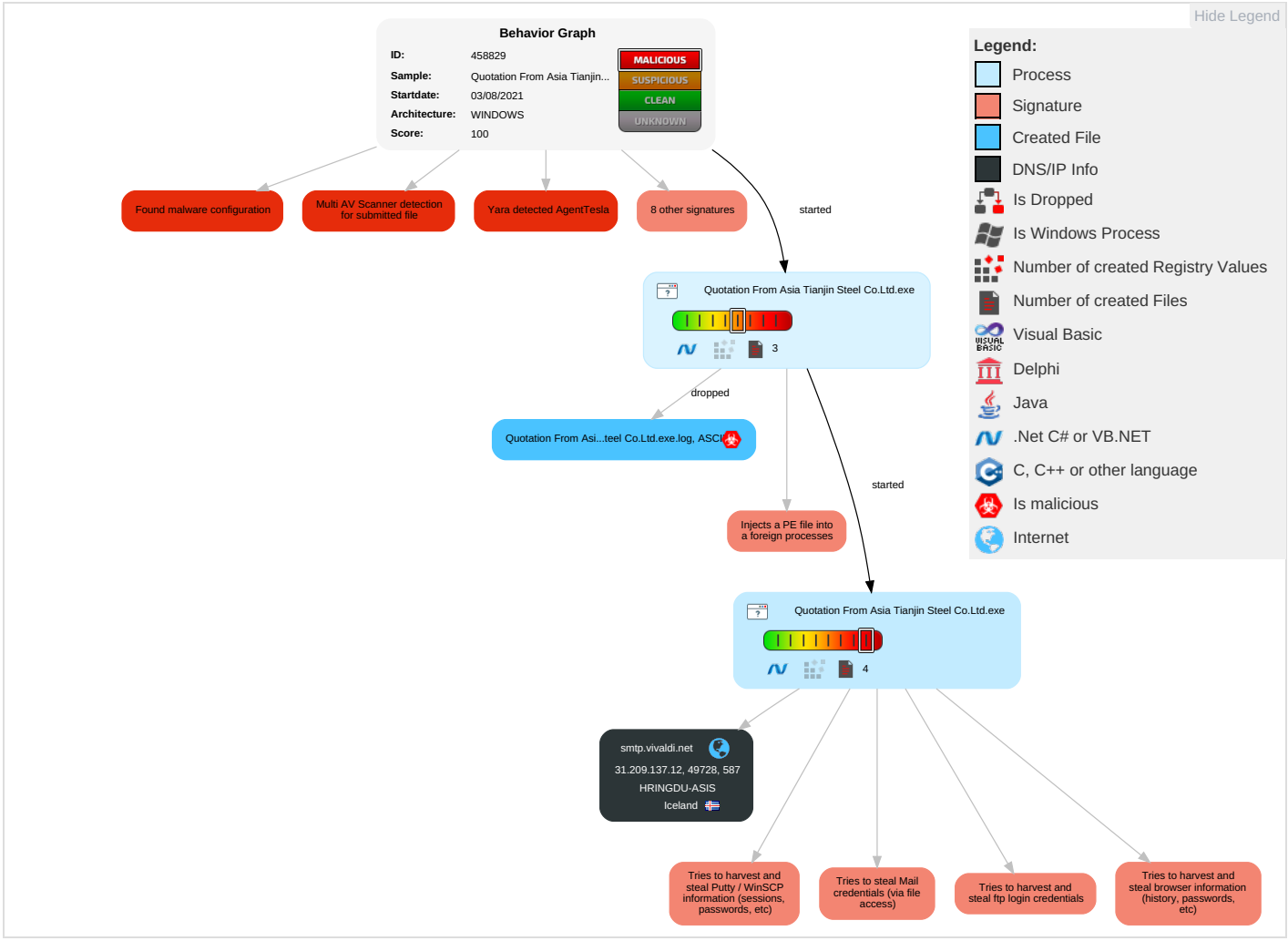
Yara detected AgentTesla

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	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Obfuscated Files or Information 3	Credentials in Registry 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Software Packing 3	Security Account Manager	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

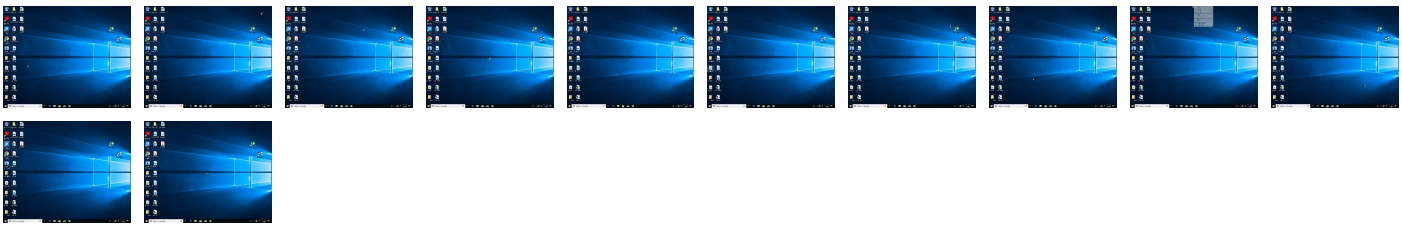
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Quotation From Asia Tianjin Steel Co.Ltd.exe	38%	Virustotal		Browse
Quotation From Asia Tianjin Steel Co.Ltd.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Quotation From Asia Tianjin Steel Co.Ltd.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Quotation From Asia Tianjin Steel Co.Ltd.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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.com1Fc	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/m_	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com/	0%	Virustotal		Browse
http://www.carterandcone.com/	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/Vo	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://10QLtVeXGPiyPS.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/2_	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d_	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	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://www.jiyu-kobo.co.jp/;_	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://www.fontbureau.commta	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://https://10QLtVeXGPiyPS.netd	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	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://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://r3.o.lencr.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/__	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/l_	0%	Avira URL Cloud	safe	
http://www.fontbureau.com;_	0%	Avira URL Cloud	safe	
http://JWsVGd.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.carterandcone.comn-upa	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.carterandcone.comgo	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.fontbureau.com__	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/l_	0%	Avira URL Cloud	safe	
http://www.fontbureau.comI.TTFV_	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsief	0%	URL Reputation	safe	
http://www.founder.com.cn/cntU	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.vivaldi.net	31.209.137.12	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.209.137.12	smtp.vivaldi.net	Iceland		51896	HRINGDU-ASIS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458829
Start date:	03.08.2021
Start time:	19:28:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation From Asia Tianjin Steel Co.Ltd.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:	25
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@3/1@1/1
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

Simulations

Behavior and APIs

Time	Type	Description
19:28:56	API Interceptor	904x Sleep call for process: Quotation From Asia Tianjin Steel Co.Ltd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
31.209.137.12	RE Outstanding SOA Settled.exe	Get hash	malicious	Browse	
	invoice.exe	Get hash	malicious	Browse	
	RFQ#775643.exe	Get hash	malicious	Browse	
	Payment $67,765.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.MSIL_Agent.CAC.genEldorado.5417.exe	Get hash	malicious	Browse	
	DHL SHIPPING INVOICE.pdf.exe	Get hash	malicious	Browse	
	URGENT REQUEST FOR QUOTATION.pdf.exe	Get hash	malicious	Browse	
	RE Outstanding SOA Settled.exe	Get hash	malicious	Browse	
	Swift Copy.exe	Get hash	malicious	Browse	
	Swift Copy.exe	Get hash	malicious	Browse	
	9872362-1926.exe	Get hash	malicious	Browse	
	invoice.exe	Get hash	malicious	Browse	
	Order.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis960D9DB7F7C9.7109.exe	Get hash	malicious	Browse	
	PREPAYMENT.exe	Get hash	malicious	Browse	
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	
	quo 4542.exe	Get hash	malicious	Browse	
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	
	Swift TT copy.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.ArtemisA47F39CCDFEA.14562.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.vivaldi.net	RE Outstanding SOA Settled.exe	Get hash	malicious	Browse	• 31.209.137.12
	invoice.exe	Get hash	malicious	Browse	• 31.209.137.12
	quotation.exe	Get hash	malicious	Browse	• 31.209.137.12
	RFQ#775643.exe	Get hash	malicious	Browse	• 31.209.137.12
	Payment $67,765.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.W32.MSIL_Agent.CAC.genEldorado.5417.exe	Get hash	malicious	Browse	• 31.209.137.12
	DHL SHIPPING INVOICE.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	URGENT REQUEST FOR QUOTATION.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	RE Outstanding SOA Settled.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift Copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift Copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	9872362-1926.exe	Get hash	malicious	Browse	• 31.209.137.12
	invoice.exe	Get hash	malicious	Browse	• 31.209.137.12
	Order.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.Artemis960D9DB7F7C9.7109.exe	Get hash	malicious	Browse	• 31.209.137.12
	PREPAYMENT.exe	Get hash	malicious	Browse	• 31.209.137.12
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 31.209.137.12
	quo 4542.exe	Get hash	malicious	Browse	• 31.209.137.12
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift TT copy.exe	Get hash	malicious	Browse	• 31.209.137.12

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HRINGDU-ASIS	RE Outstanding SOA Settled.exe	Get hash	malicious	Browse	• 31.209.137.12
	invoice.exe	Get hash	malicious	Browse	• 31.209.137.12
	RFQ#775643.exe	Get hash	malicious	Browse	• 31.209.137.12

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment $67,765.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.W32.MSIL_Agent.CAC.genEldorado.5417.exe	Get hash	malicious	Browse	• 31.209.137.12
	DHL SHIPPING INVOICE.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	URGENT REQUEST FOR QUOTATION.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	RE Outstanding SOA Settled.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift Copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift Copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	9872362-1926.exe	Get hash	malicious	Browse	• 31.209.137.12
	invoice.exe	Get hash	malicious	Browse	• 31.209.137.12
	Order.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.Artemis960D9DB7F7C9.7109.exe	Get hash	malicious	Browse	• 31.209.137.12
	PREPAYMENT.exe	Get hash	malicious	Browse	• 31.209.137.12
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 31.209.137.12
	quo 4542.exe	Get hash	malicious	Browse	• 31.209.137.12
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift TT copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.ArtemisA47F39CCDFEA.14562.exe	Get hash	malicious	Browse	• 31.209.137.12

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Quotation From Asia Tianjin Steel Co.Ltd.exe.log

Process:	C:\Users\user\Desktop\Quotation From Asia Tianjin Steel Co.Ltd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.437526161568796

General

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:	Quotation From Asia Tianjin Steel Co.Ltd.exe
File size:	823296
MD5:	0fcf33a3980c44c176d519a4589028aa
SHA1:	f2aebb3e351e1654c49b8d1781d28ac8591721d1
SHA256:	6d877514b8301c2c5ec0655792599f127b2a1649f7483a584d5f7125171cf7a0
SHA512:	74b2fcf32136661792f9255e78f3bc2c2e5690182d964d103e44e5e34841b41386bd33905e23667b4be32652783cc164cb8a9091c77da515fde467c096b7423
SSDEEP:	12288:wo6as4J1zgVDU0QrAXDGZSIUf055blwR/0lcJsTtmEburWqpu6x7XM2iN:wo6asU1eBBXyqfgbyR/XKxsW36FXM1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ca5f2
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:	0xE7CA8BB4 [Wed Mar 25 09:15:32 2093 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc85f8	0xc8600	False	0.786352737056	data	7.44517704491	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xcc000	0x5cc	0x600	False	0.42578125	data	4.1279967586	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 19:30:37.330224037 CEST	192.168.2.5	8.8.8.8	0x72e7	Standard query (0)	smtp.vivaldi.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 19:30:37.366628885 CEST	8.8.8.8	192.168.2.5	0x72e7	No error (0)	smtp.vivaldi.net		31.209.137.12	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 19:30:39.118119001 CEST	587	49728	31.209.137.12	192.168.2.5	220 smtp.vivaldi.net ESMTP Postfix (Ubuntu)
Aug 3, 2021 19:30:39.118660927 CEST	49728	587	192.168.2.5	31.209.137.12	EHLO 910646
Aug 3, 2021 19:30:39.181740046 CEST	587	49728	31.209.137.12	192.168.2.5	250-smtp.vivaldi.net 250-PIPELINING 250-SIZE 36700160 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 SMTPUTF8
Aug 3, 2021 19:30:39.182279110 CEST	49728	587	192.168.2.5	31.209.137.12	STARTTLS
Aug 3, 2021 19:30:39.245362997 CEST	587	49728	31.209.137.12	192.168.2.5	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Quotation From Asia Tianjin Steel Co.Ltd.exe PID: 5476 Parent PID: 5556

General

Start time:	19:28:51
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Quotation From Asia Tianjin Steel Co.Ltd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation From Asia Tianjin Steel Co.Ltd.exe'
Imagebase:	0xfe0000
File size:	823296 bytes
MD5 hash:	0FCF33A3980C44C176D519A4589028AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.246514460.0000000003AF3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.254121480.000000000A591000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.254121480.000000000A591000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Quotation From Asia Tianjin Steel Co.Ltd.exe PID: 1900 Parent PID: 5476

General

Start time:	19:28:58
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Quotation From Asia Tianjin Steel Co.Ltd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation From Asia Tianjin Steel Co.Ltd.exe
Imagebase:	0x670000
File size:	823296 bytes
MD5 hash:	0FCF33A3980C44C176D519A4589028AA
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: 00000004.00000002.493730793.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.493730793.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.499241824.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.499241824.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.499523582.0000000002DA8000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis