ID: 339119
Sample Name: Quotation.exe
Cookbook: default.jbs
Time: 15:12:52
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

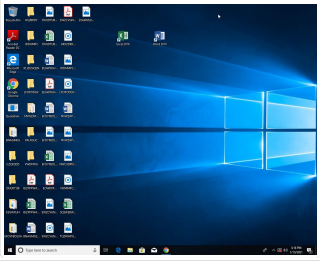
Analysis Report Quotation.exe

Overview

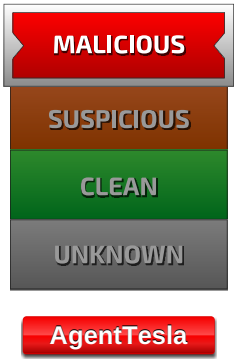
General Information

Sample Name:	Quotation.exe
Analysis ID:	339119
MD5:	c478a9dd6e72ac..
SHA1:	e9084e9ccbcfb91..
SHA256:	e178d0ed3b308b..
Tags:	exe

Most interesting Screenshot:



Detection

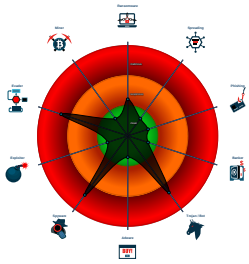


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- 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…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- Quotation.exe (PID: 6084 cmdline: 'C:\Users\user\Desktop\Quotation.exe' MD5: C478A9DD6E72AC0E96AA0BD90D7B9EC2)
  - Quotation.exe (PID: 5288 cmdline: 'C:\Users\user\Desktop\Quotation.exe' MD5: C478A9DD6E72AC0E96AA0BD90D7B9EC2)
  - Quotation.exe (PID: 5824 cmdline: C:\Users\user\Desktop\Quotation.exe MD5: C478A9DD6E72AC0E96AA0BD90D7B9EC2)
    - Quotation.exe (PID: 5852 cmdline: C:\Users\user\Desktop\Quotation.exe MD5: C478A9DD6E72AC0E96AA0BD90D7B9EC2)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "rOPNbWS",
  "URL: ": "https://OKmk0UVQzAElqL6wiCX.net",
  "To: ": "mauro.aguiari@tthyssenkrupp.com",
  "ByHost: ": "smtp.tthyssenkrupp.com:587",
  "Password: ": "4nH0rm",
  "From: ": "mauro.aguiari@tthyssenkrupp.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.588164369.0000000000F39000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.233917057.0000000000B80000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.589076176.0000000002AE2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.585204726.0000000000400000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.589457084.0000000002B6 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

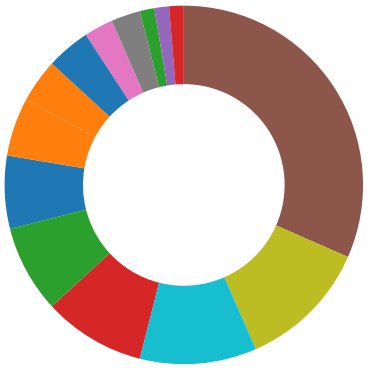
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.Quotation.exe.2970000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.Quotation.exe.2970000.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.Quotation.exe.b80000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.Quotation.exe.400000.0.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.Quotation.exe.b80000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- 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:

Antivirus / Scanner detection for submitted sample

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)

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

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:

Maps a DLL or memory area into another process

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:

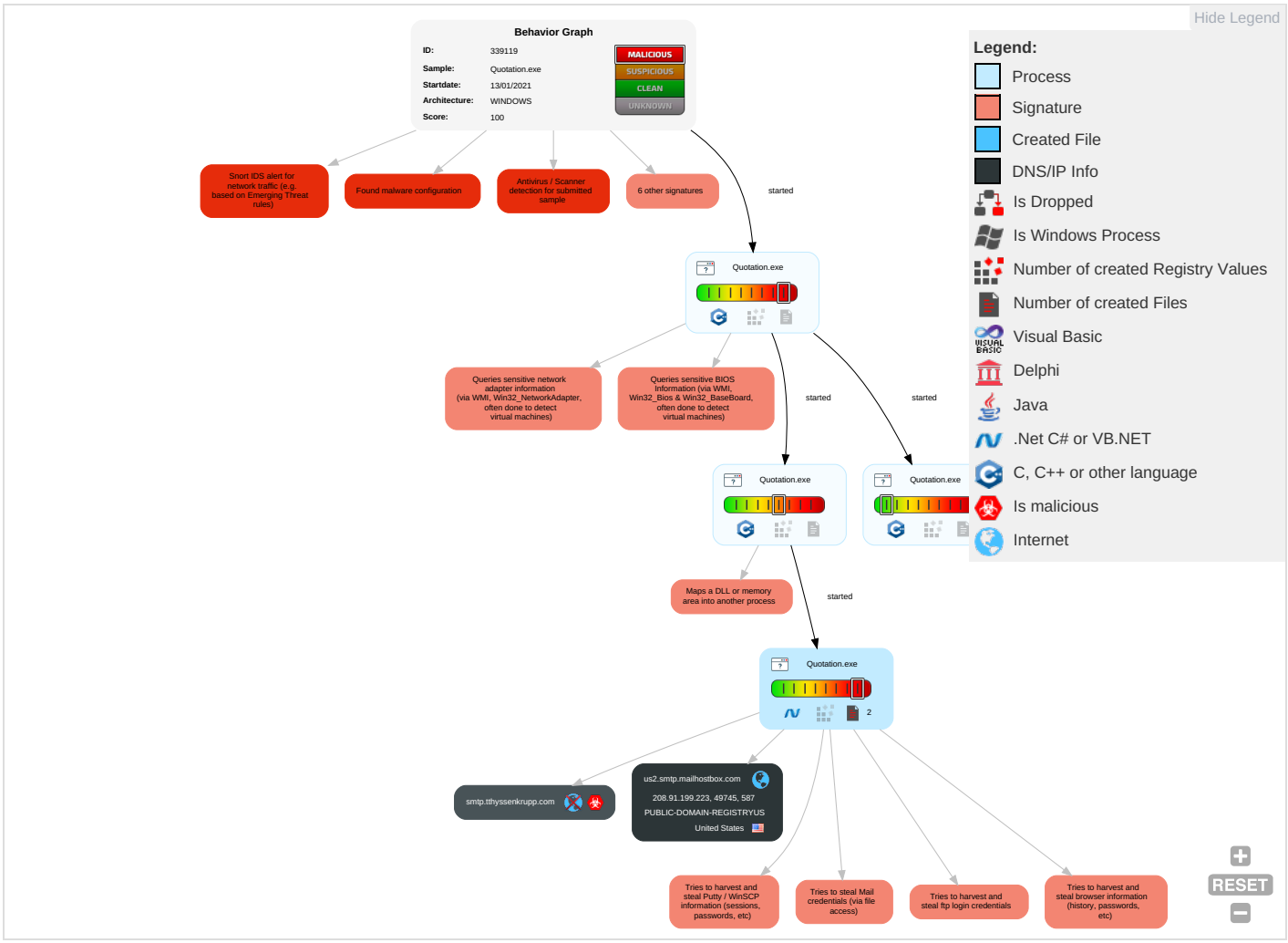
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standarc Port 1
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	System Information Discovery 1 2 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applicati Layer Protocc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application La Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 3	LSA Secrets	Security Software Discovery 1 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Us Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application La Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	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.exe	37%	Virustotal		Browse
Quotation.exe	43%	ReversingLabs	Win32.Trojan.Pwsx	
Quotation.exe	100%	Avira	HEUR/AGEN.1106536	
Quotation.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.Quotation.exe.2ae0000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.Quotation.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://ShQsty.com	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://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://OKmk0UVQzAElqL6wiCX.net	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://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%$	0%	Avira URL Cloud	safe	
http://smtp.tthyssenkrupp.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
smtp.tthyssenkrupp.com	unknown	unknown	true		unknown

Contacted URLs

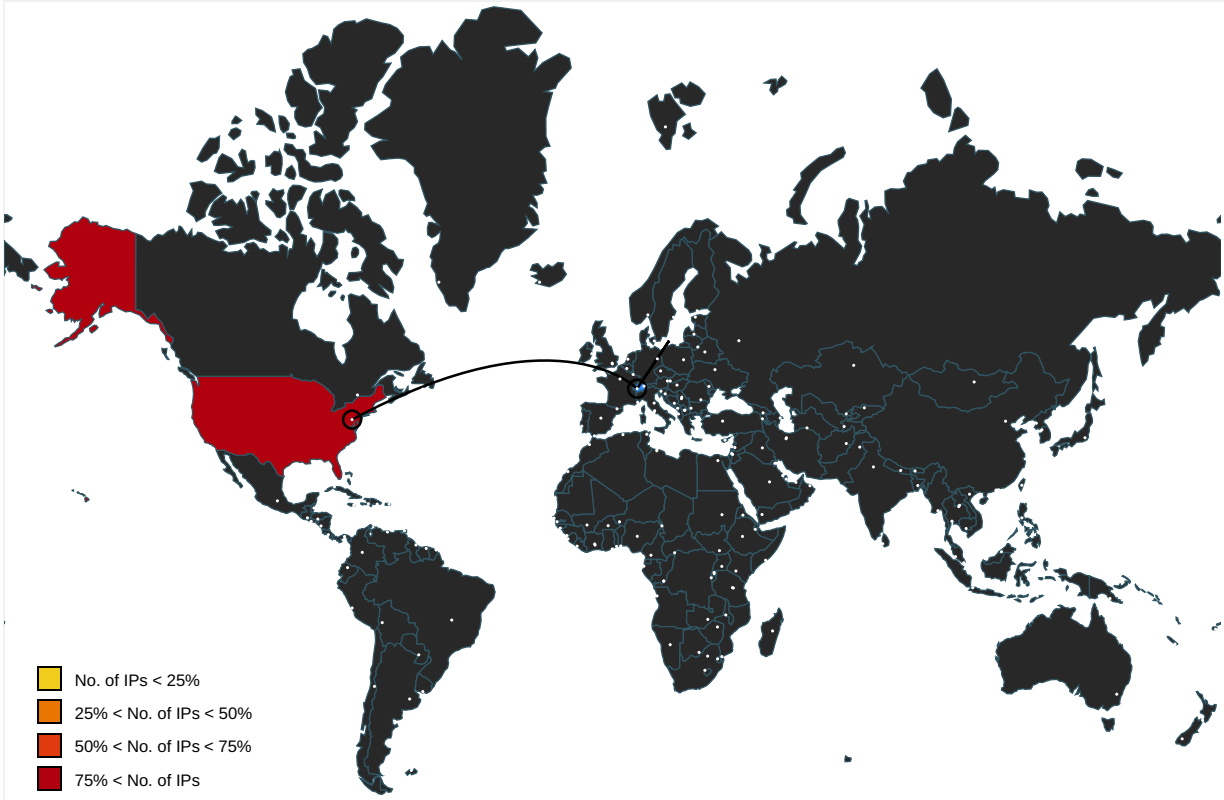
Name	Malicious	Antivirus Detection	Reputation
http://https://OKmk0UVQzAElqL6wiCX.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Quotation.exe, 00000003.00000002.589457084.0000000002B61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ShQsty.com	Quotation.exe, 00000003.00000002.589457084.0000000002B61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	Quotation.exe, 00000003.00000002.589457084.0000000002B61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	Quotation.exe, 00000003.00000002.589457084.0000000002B61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	Quotation.exe, 00000003.00000002.591947363.0000000002E76000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Quotation.exe, 00000003.00000002.589457084.0000000002B61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Quotation.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%$	Quotation.exe, 00000003.00000002.589457084.0000000002B61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://smtp.tthyssenkrupp.com	Quotation.exe, 00000003.00000002.591947363.0000000002E76000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.223	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339119
Start date:	13.01.2021
Start time:	15:12:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation.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:	31
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@7/0@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.6% (good quality ratio 22.6%) • Quality average: 78% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.42.151.234, 104.43.139.144, 23.210.248.85, 51.104.139.180, 92.122.213.194, 92.122.213.247, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.103.5.159, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.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, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.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
15:14:01	API Interceptor	979x Sleep call for process: Quotation.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	Booking.exe	Get hash	malicious	Browse	
	C.V. - application letter.exe	Get hash	malicious	Browse	
	AWB & Shipping Document.exe	Get hash	malicious	Browse	
	Y3fwLpzaXNZPaT6.exe	Get hash	malicious	Browse	
	XyZQ7im2Dv.exe	Get hash	malicious	Browse	
	FB-108N & FB-108NK #U8a62#U50f9 - #U7530#U52e4.exe	Get hash	malicious	Browse	
	ESrYdvhNfV.exe	Get hash	malicious	Browse	
	KBC Enquiry No.20201228.xlsx	Get hash	malicious	Browse	
	LR8meXRan7.exe	Get hash	malicious	Browse	
	Proforma Invoice.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	181c6640-693e-417a-bc21-8e1fe6302632.exe	Get hash	malicious	Browse	
	QUOTATION OAED QUOTATION PRESENTATION.exe	Get hash	malicious	Browse	
	erew-436.exe	Get hash	malicious	Browse	
	Statement of Account.doc	Get hash	malicious	Browse	
	vsl particulars.exe	Get hash	malicious	Browse	
	swift-advise.exe	Get hash	malicious	Browse	
	CHEMEX DUBAI.exe	Get hash	malicious	Browse	
	RFQ16-03-2020YT.exe	Get hash	malicious	Browse	
	SR 16-30 nOV-2020 GULF AIR.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Booking.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV. Double Miracle.exe	Get hash	malicious	Browse	• 208.91.199.225
	MV Double Miracle.exe	Get hash	malicious	Browse	• 208.91.199.224
	C.V. - application letter.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO-SOT215006A.exe	Get hash	malicious	Browse	• 208.91.199.224
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.225
	invoice No 8882.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping document.exe	Get hash	malicious	Browse	• 208.91.199.225
	Y3fwLpzaXNZPaT6.exe	Get hash	malicious	Browse	• 208.91.199.223
	XyZQ7im2Dv.exe	Get hash	malicious	Browse	• 208.91.199.223
	FB-108N & FB-108NK #U8a62#U50f9 - #U7530#U52e4.exe	Get hash	malicious	Browse	• 208.91.199.223
	Ldz62seIo3.exe	Get hash	malicious	Browse	• 208.91.199.225
	VPAPvqgfkf.exe	Get hash	malicious	Browse	• 208.91.199.225
	TTR payment amount 131,000 USD.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	ESrYdvhNfV.exe	Get hash	malicious	Browse	• 208.91.199.223
	DHL Delivery Confirmation.exe	Get hash	malicious	Browse	• 208.91.198.143
	KBC Enquiry No.20201228.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	LR8meXRan7.exe	Get hash	malicious	Browse	• 208.91.199.223
	Proforma Invoice.exe	Get hash	malicious	Browse	• 208.91.199.223
	ThyssenKrupp AG Supplier Vendor Registration.exe	Get hash	malicious	Browse	• 208.91.199.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Doc_18420540.doc	Get hash	malicious	Browse	• 103.76.228.18
	Booking.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV. Double Miracle.exe	Get hash	malicious	Browse	• 208.91.199.225
	MV Double Miracle.exe	Get hash	malicious	Browse	• 208.91.199.224
	RFQ0128SR20KWT_DEUNGJU_FAKRU_AND_NAVEED.exe	Get hash	malicious	Browse	• 162.222.225.57
	C.V. - application letter.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO-SOT215006A.exe	Get hash	malicious	Browse	• 208.91.199.224
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.223
	invoice No 8882.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping document.exe	Get hash	malicious	Browse	• 208.91.199.225
	Y3fwLpzaXNZPaT6.exe	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rib.exe	Get hash	malicious	Browse	• 208.91.199.108
	XyZQ7im2Dv.exe	Get hash	malicious	Browse	• 208.91.199.223
	FB-108N & FB-108NK #U8a62#U50f9 - #U7530#U52e4.exe	Get hash	malicious	Browse	• 208.91.199.223
	Ldz62seIo3.exe	Get hash	malicious	Browse	• 208.91.199.225
	VPAPvqgfkf.exe	Get hash	malicious	Browse	• 208.91.199.225
	TTR payment amount 131,000 USD.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	ESrYdvhNfV.exe	Get hash	malicious	Browse	• 208.91.199.223
	DHL Delivery Confirmation.exe	Get hash	malicious	Browse	• 208.91.199.225
	KBC Enquiry No.20201228.xlsx	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.764174747045879
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Quotation.exe
File size:	440320
MD5:	c478a9dd6e72ac0e96aa0bd90d7b9ec2
SHA1:	e9084e9ccbcfb91547d292be1e76985b353d7ecd
SHA256:	e178d0ed3b308beca605b9b5f71fd420bb438dc2c12e375 23982982d57df22a3
SHA512:	0a3f3adc1d153768c4542897a868d0a94043dac205e89d c923b993572bccbf98041c5aa68d70e561213769c0fbf9b b0973c5f586f2506dce3c9c580edb381650
SSDEEP:	6144:sr1I5DbAQcHAORYANcUR+pWGxFGvRmGYu7j qb1Ssa9OFznr8UUqLRmhbHdgGA:Q1I5fAPHXR+UbZd Y51Tao17Fmhb9c
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....tj.m'j. m'j.m'.Q.'k.m'.4.'I.m'.4.'r.m'.4.'..m'j.I'..m'...'..m'M7.'k.m'M7 .'k.m'M7.'k.m'Richj.m'.....PE..L...C._...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4088a7
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFEC843 [Wed Jan 13 10:15:31 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e7da020c2fad0c59a3d5e97971484548

Entrypoint Preview

Instruction
call 00007FA96CC53A71h
jmp 00007FA96CC4C6D5h
push 00000014h
push 0041D838h
call 00007FA96CC4CF78h
call 00007FA96CC4FE26h
movzx esi, ax
push 00000002h
call 00007FA96CC53A04h
pop ecx
mov eax, 00005A4Dh
cmp word ptr [00400000h], ax
je 00007FA96CC4C6D6h
xor ebx, ebx
jmp 00007FA96CC4C705h
mov eax, dword ptr [0040003Ch]
cmp dword ptr [eax+00400000h], 00004550h
jne 00007FA96CC4C6BDh
mov ecx, 0000010Bh
cmp word ptr [eax+00400018h], cx
jne 00007FA96CC4C6AFh
xor ebx, ebx
cmp dword ptr [eax+00400074h], 0Eh
jbe 00007FA96CC4C6DBh
cmp dword ptr [eax+004000E8h], ebx
setne bl
mov dword ptr [ebp-1Ch], ebx
call 00007FA96CC50E13h
test eax, eax
jne 00007FA96CC4C6DAh
push 0000001Ch
call 00007FA96CC4C7A5h
pop ecx
call 00007FA96CC5147Ch
test eax, eax
jne 00007FA96CC4C6DAh
push 00000010h
call 00007FA96CC4C794h
pop ecx
call 00007FA96CC4FBB8h
and dword ptr [ebp-04h], 00000000h
call 00007FA96CC4E353h
call dword ptr [004180C8h]
mov dword ptr [00424080h], eax
call 00007FA96CC53A62h
mov dword ptr [00422284h], eax

Instruction
call 00007FA96CC53663h
test eax, eax
jns 00007FA96CC4C6DAh
push 00000008h
call 00007FA96CC4B28Ah
pop ecx
call 00007FA96CC5387Fh

Rich Headers

Programming Language:	• [LNK] VS2012 build 50727 • [RES] VS2012 build 50727 • [C] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1db94	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x25000	0x1a78	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x27000	0x1150	.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	0x1d6e0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x18000	0x1c8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16d9a	0x16e00	False	0.571209016393	data	6.67400094026	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x18000	0x64f8	0x6600	False	0.572227328431	data	6.01779519415	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x5098	0x3400	False	0.285531850962	data	4.70097691284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x25000	0x1a78	0x1c00	False	0.937918526786	data	7.70017907043	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x27000	0x1798	0x1800	False	0.606770833333	data	5.55502371105	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x25070	0x1a05	data	English	United States

Imports

DLL	Import
KERNEL32.dll	RaiseException, ReadConsoleW, ReadFile, CreateFileW, WriteConsoleW, GetStringTypeW, LCMapStringEx, SetConsoleCursorPosition, LoadLibraryW, GetModuleHandleW, HeapReAlloc, HeapSize, OutputDebugStringW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, FlushFileBuffers, SetStdHandle, WideCharToMultiByte, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetProcessHeap, HeapAlloc, GetStdHandle, GetTickCount64, GetSystemTimeAsFileTime, QueryPerformanceCounter, GetModuleFileNameA, GetCurrentThreadId, SetLastError, GetCPInfo, GetOEMCP, GetACP, EncodePointer, DecodePointer, GetLastError, InterlockedDecrement, ExitProcess, GetModuleHandleExW, GetProcAddress, AreFileApisANSI, MultiByteToWideChar, GetLocalTime, GetCommandLineA, IsDebuggerPresent, IsProcessorFeaturePresent, EnterCriticalSection, LeaveCriticalSection, CloseHandle, HeapFree, InitializeCriticalSectionAndSpinCount, RtlUnwind, GetFileType, DeleteCriticalSection, InitOnceExecuteOnce, GetStartupInfoW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, GetCurrentProcess, TerminateProcess, WriteFile, GetModuleFileNameW, Sleep, LoadLibraryExW, InterlockedIncrement, IsValidCodePage, SetEndOfFile

DLL	Import
msi.dll	
loadperf.dll	LoadPerfCounterTextStringsA, UnloadPerfCounterTextStringsW, UnloadPerfCounterTextStringsA
MSVFW32.dll	StretchDIB
AVIFIL32.dll	AVIFileExit, AVIStreamReadData
pdh.dll	PdhEnumObjectsW, PdhSetQueryTimeRange, PdhGetDllVersion
WSOCK32.dll	WSASetBlockingHook, WSACancelAsyncRequest, bind, ord1104, ord1108, ord1130
GDI32.dll	StartDocW, GdiGetSpoolFileHandle, PolyBezier
MAPI32.dll	
MSACM32.dll	acmDriverPriority, acmFilterTagDetailsA

Possible Origin

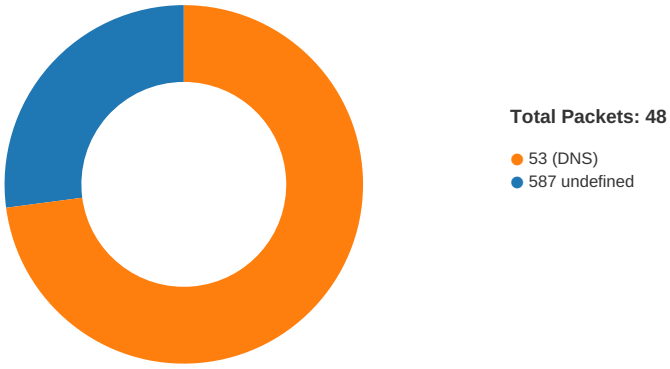
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-15:15:38.966414	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49745	587	192.168.2.3	208.91.199.223

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 15:15:35.314064026 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:35.478625059 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:35.478744030 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:36.806340933 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:36.807004929 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:36.971457958 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:36.971508026 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:36.975511074 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:37.140980005 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:37.142096996 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:37.308986902 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:37.310220003 CET	49745	587	192.168.2.3	208.91.199.223

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 15:15:37.475601912 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:37.475989103 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:37.681689978 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:38.796554089 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:38.797127008 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:38.961848021 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:38.961930037 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:38.966413975 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:38.966749907 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:38.967384100 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:38.967585087 CET	49745	587	192.168.2.3	208.91.199.223
Jan 13, 2021 15:15:39.131251097 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:39.131844997 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:39.325953007 CET	587	49745	208.91.199.223	192.168.2.3
Jan 13, 2021 15:15:39.380476952 CET	49745	587	192.168.2.3	208.91.199.223

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 15:13:44.280971050 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:13:44.331659079 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 15:13:45.198905945 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:13:45.249743938 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 15:13:46.452153921 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:13:46.502955914 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 15:13:47.585551977 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:13:47.633511066 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 15:13:48.733051062 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:13:48.784104109 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 15:13:54.219192982 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:13:54.275454044 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 15:13:55.554056883 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:13:55.601938009 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 15:13:58.296257973 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:13:58.344077110 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:09.493856907 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:09.560898066 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:12.784993887 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:12.832830906 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:16.910830975 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:16.970999002 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:23.222948074 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:23.271013975 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:24.626652002 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:24.677258968 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:25.915412903 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:25.963491917 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:27.501863003 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:27.549911022 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:31.362889051 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:31.427084923 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:32.727749109 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:32.785964012 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:34.281919956 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:34.332604885 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:37.505099058 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:37.565355062 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 15:14:48.855766058 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:14:48.903816938 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 15:15:09.973148108 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:15:10.021362066 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 15:15:10.423557043 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:15:10.494976044 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 15:15:34.927287102 CET	61292	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 15:15:35.148483992 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 15:15:35.165376902 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:15:35.221530914 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 15:15:35.288636923 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:15:35.336599112 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:25.954849005 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:26.005656958 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:26.678599119 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:26.735167027 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:27.529829979 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:27.589039087 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:28.172056913 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:28.239115000 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:28.869467020 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:28.917346001 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:29.790409088 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:29.846630096 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:30.543559074 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:30.591561079 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:31.605684996 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:31.653654099 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:35.180238962 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:35.239662886 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 15:16:35.681768894 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 15:16:35.740520954 CET	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 15:15:34.927287102 CET	192.168.2.3	8.8.8.8	0xf95e	Standard query (0)	smtp.tthys senkrupp.com	A (IP address)	IN (0x0001)
Jan 13, 2021 15:15:35.165376902 CET	192.168.2.3	8.8.8.8	0x3e31	Standard query (0)	smtp.tthys senkrupp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 15:15:35.148483992 CET	8.8.8.8	192.168.2.3	0xf95e	No error (0)	smtp.tthys senkrupp.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 15:15:35.148483992 CET	8.8.8.8	192.168.2.3	0xf95e	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 13, 2021 15:15:35.148483992 CET	8.8.8.8	192.168.2.3	0xf95e	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 13, 2021 15:15:35.148483992 CET	8.8.8.8	192.168.2.3	0xf95e	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 13, 2021 15:15:35.148483992 CET	8.8.8.8	192.168.2.3	0xf95e	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 13, 2021 15:15:35.221530914 CET	8.8.8.8	192.168.2.3	0x3e31	No error (0)	smtp.tthys senkrupp.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 15:15:35.221530914 CET	8.8.8.8	192.168.2.3	0x3e31	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 13, 2021 15:15:35.221530914 CET	8.8.8.8	192.168.2.3	0x3e31	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 13, 2021 15:15:35.221530914 CET	8.8.8.8	192.168.2.3	0x3e31	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 13, 2021 15:15:35.221530914 CET	8.8.8.8	192.168.2.3	0x3e31	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

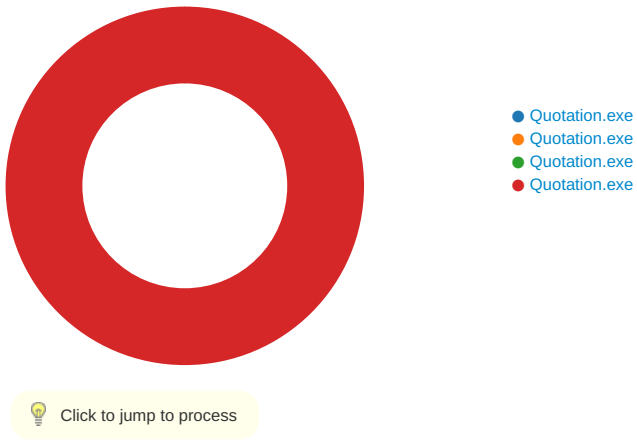
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 15:15:36.806340933 CET	587	49745	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 13, 2021 15:15:36.807004929 CET	49745	587	192.168.2.3	208.91.199.223	EHLO 287400
Jan 13, 2021 15:15:36.971508026 CET	587	49745	208.91.199.223	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 13, 2021 15:15:36.975511074 CET	49745	587	192.168.2.3	208.91.199.223	AUTH login bWF1cm8uYWd1aWFyaUB0dGh5c3NlbmtydXBwLmNvbQ==
Jan 13, 2021 15:15:37.140980005 CET	587	49745	208.91.199.223	192.168.2.3	334 UGFzc3dvcmQ6
Jan 13, 2021 15:15:37.308986902 CET	587	49745	208.91.199.223	192.168.2.3	235 2.7.0 Authentication successful
Jan 13, 2021 15:15:37.310220003 CET	49745	587	192.168.2.3	208.91.199.223	MAIL FROM:<mauro.aguiari@tthyssenkrupp.com>
Jan 13, 2021 15:15:37.475601912 CET	587	49745	208.91.199.223	192.168.2.3	250 2.1.0 Ok
Jan 13, 2021 15:15:37.475989103 CET	49745	587	192.168.2.3	208.91.199.223	RCPT TO:<mauro.aguiari@tthyssenkrupp.com>
Jan 13, 2021 15:15:38.796554089 CET	587	49745	208.91.199.223	192.168.2.3	250 2.1.5 Ok
Jan 13, 2021 15:15:38.797127008 CET	49745	587	192.168.2.3	208.91.199.223	DATA
Jan 13, 2021 15:15:38.961930037 CET	587	49745	208.91.199.223	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Jan 13, 2021 15:15:38.967585087 CET	49745	587	192.168.2.3	208.91.199.223	.
Jan 13, 2021 15:15:39.325953007 CET	587	49745	208.91.199.223	192.168.2.3	250 2.0.0 Ok: queued as B25781828A9

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Quotation.exe PID: 6084 Parent PID: 5716

General

Start time:	15:13:47
Start date:	13/01/2021

Path:	C:\Users\user\Desktop\Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation.exe'
Imagebase:	0xbe0000
File size:	440320 bytes
MD5 hash:	C478A9DD6E72AC0E96AA0BD90D7B9EC2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.226102208.0000000002D90000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Quotation.exe PID: 5288 Parent PID: 6084

General

Start time:	15:13:49
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Quotation.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Quotation.exe'
Imagebase:	0xbe0000
File size:	440320 bytes
MD5 hash:	C478A9DD6E72AC0E96AA0BD90D7B9EC2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Quotation.exe PID: 5824 Parent PID: 6084

General

Start time:	15:13:50
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Quotation.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation.exe
Imagebase:	0xbe0000
File size:	440320 bytes
MD5 hash:	C478A9DD6E72AC0E96AA0BD90D7B9EC2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.233917057.0000000000B80000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Quotation.exe PID: 5852 Parent PID: 5824

General

Start time:	15:13:51
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Quotation.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation.exe
Imagebase:	0xbe0000
File size:	440320 bytes
MD5 hash:	C478A9DD6E72AC0E96AA0BD90D7B9EC2
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: 00000003.00000002.588164369.0000000000F39000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.589076176.0000000002AE2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.585204726.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.589457084.0000000002B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.589457084.0000000002B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.592948035.0000000003B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.588949913.0000000002970000.00000004.00000001.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	6DA7CF06	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	6DA7CF06	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	6DA55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9B03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C8C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C8C1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C8C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C8C1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\61c4d17e-f3cd-4c23-8ea5-f3708039a956	unknown	4096	success or wait	1	6C8C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C8C1B4F	ReadFile

Disassembly

Code Analysis