ID: 491433
Sample Name: Inquiry - Specifications 002021.exe
Cookbook: default.jbs
Time: 15:29:07
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

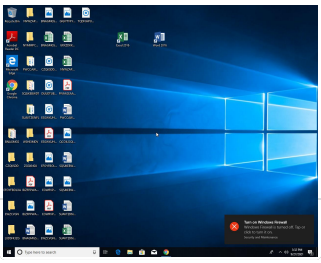
Windows Analysis Report Inquiry - Specifications 00202…

Overview

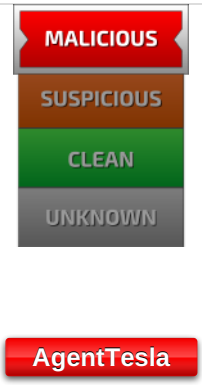
General Information

Sample Name:	Inquiry - Specifications 002021.exe
Analysis ID:	491433
MD5:	768a1127c11914..
SHA1:	afe86ab8d4a8b5b.
SHA256:	2442c3ecd04264..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

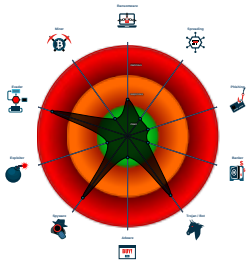


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- .NET source code contains very larg…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- Inquiry - Specifications 002021.exe (PID: 1360 cmdline: 'C:\Users\user\Desktop\Inquiry - Specifications 002021.exe' MD5: 768A1127C119149F96A29C0D0C0B56EC)
  - Inquiry - Specifications 002021.exe (PID: 6580 cmdline: C:\Users\user\Desktop\Inquiry - Specifications 002021.exe MD5: 768A1127C119149F96A29C0D0C0B56EC)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "annett.jalowi@vern-group.com",
  "Password": "HUSTLE2021",
  "Host": "smtp.vern-group.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.559497777.00000000030EF000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.553693912.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.553693912.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.558228658.0000000002E01000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.558228658.0000000002E01000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Inquiry - Specifications 002021.exe.35a8b58 .4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Inquiry - Specifications 002021.exe.35a8b58 .4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Inquiry - Specifications 002021.exe.2528614 .1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.Inquiry - Specifications 002021.exe.36d73e0 .3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Inquiry - Specifications 002021.exe.36d73e0 .3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 4 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

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 array initializations

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

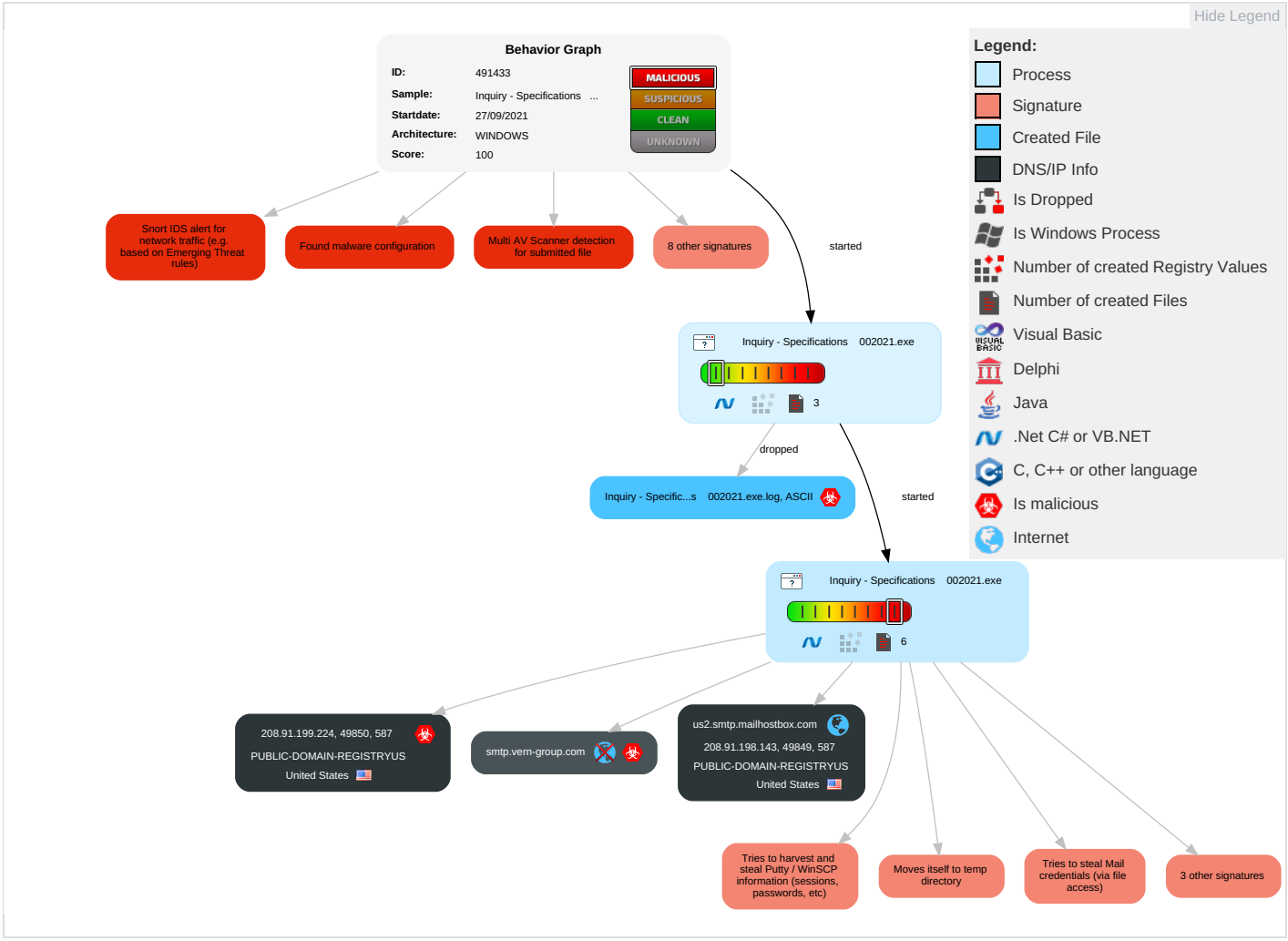
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1 1	OS Credential Dumping 2	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypte Channel
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-Sta Port 1
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 1	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Applicati Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po

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
Inquiry - Specifications 002021.exe	7%	Virustotal		Browse
Inquiry - Specifications 002021.exe	43%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Inquiry - Specifications 002021.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
smtp.vern-group.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.comus0	0%	Avira URL Cloud	safe	
http://www.typography.netI.TTFB5	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fonts.comwN	0%	Avira URL Cloud	safe	
http://https://SAIitQOLdjJT1PWF4ciQ.net(0	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com=	0%	Avira URL Cloud	safe	
http://https://SAIitQOLdjJT1PWF4ciQ.net	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sajatypeworks.comus	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comusJ	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	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://www.typography.net	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	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.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comttvc	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://www.monotype.y	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.typography.nete	0%	Avira URL Cloud	safe	
http://tbdUKh.com	0%	Avira URL Cloud	safe	
http://www.rspb.org.uk/wildlife/birdguide/name/	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://www.monotype.ccN/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com-e	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fonts.comON	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.sajatypeworks.comusW	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.agfamonotype.%AF	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com#	0%	Avira URL Cloud	safe	
http://www.typography.netl	0%	Avira URL Cloud	safe	
http://www.fontbureau.com~	0%	Avira URL Cloud	safe	
http://smtp.vern-group.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high
smtp.vern-group.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.143	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
208.91.199.224	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491433
Start date:	27.09.2021
Start time:	15:29:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Inquiry - Specifications 002021.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:	21
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@3/2@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.7%) • Quality average: 57% • Quality standard deviation: 33.3%
HCA Information:	• Successful, ratio: 97% • 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
15:30:15	API Interceptor	678x Sleep call for process: Inquiry - Specifications 002021.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	#RFQ Medimpex International LLC.exe	Get hash	malicious	Browse	
	New Order.doc	Get hash	malicious	Browse	
	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	
	Solicitud de cotizacion.exe	Get hash	malicious	Browse	
	KLC45E_92421_PI.exe	Get hash	malicious	Browse	
	Products prices request.xlsx	Get hash	malicious	Browse	
	Payment Advice 09-22-2021 SKMBT03783930484080484904003TXT.exe	Get hash	malicious	Browse	
	from-iso_PSC ___ - E41140,PDF.EXE	Get hash	malicious	Browse	
	n267kM6LhuZHjzz.exe	Get hash	malicious	Browse	
	Cv4ms60aUz.exe	Get hash	malicious	Browse	
	iw2crzErP4mvr7r.exe	Get hash	malicious	Browse	
	COMTAC LISTA URGENTE ORDEN 92121,pdf.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	k4QKSYxd03.exe	Get hash	malicious	Browse	
	Po#6672.pdf.exe	Get hash	malicious	Browse	
	Order Confirmation _ Urgent,pdf.exe	Get hash	malicious	Browse	
	Orde Baru #86-55113 ,pdf.exe	Get hash	malicious	Browse	
	RFQ_AP65425652_032421 segera.exe	Get hash	malicious	Browse	
	INTR_ORDER 5676-SEPT1521,pdf.exe	Get hash	malicious	Browse	
208.91.199.224	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	
	#U0916#U0930#U0940#U0926 #U0906#U0926#U0947#U0936-34002174,pdf.exe	Get hash	malicious	Browse	
	#Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe	Get hash	malicious	Browse	
	4f7K9bfgNr.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	KLC45E_92421_PI.exe	Get hash	malicious	Browse	
	MONO Nueva orden - E41140,PDF.exe	Get hash	malicious	Browse	
	SO230921.exe	Get hash	malicious	Browse	
	Products prices request.xlsx	Get hash	malicious	Browse	
	S7v33zELdY.exe	Get hash	malicious	Browse	
	INVOICE AWB 9782166...exe	Get hash	malicious	Browse	
	iJjetWi3z5.exe	Get hash	malicious	Browse	
	COMTAC LISTA URGENTE ORDEN 92121,pdf.exe	Get hash	malicious	Browse	
	Po#6672.pdf.exe	Get hash	malicious	Browse	
	04142021_10RD0207S0N0000,pdf.exe	Get hash	malicious	Browse	
	Order Confirmation _ Urgent,pdf.exe	Get hash	malicious	Browse	
	Orde Baru #86-55113 ,pdf.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	Rvl6j5Uisf.exe	Get hash	malicious	Browse	
	New ORDER.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	#RFQ Medimpex International LLC.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENTS_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	New Order.doc	Get hash	malicious	Browse	• 208.91.198.143
	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	#U0916#U0930#U0940#U0926 #U0906#U0926#U0947#U0936-34002174,pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	#Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	4f7K9bfgNr.exe	Get hash	malicious	Browse	• 208.91.199.224
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.198.143
	Solicitud de cotizacion.exe	Get hash	malicious	Browse	• 208.91.198.143
	New Order.exe	Get hash	malicious	Browse	• 208.91.199.223
	KLC45E_92421_PI.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO-3242.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	MONO Nueva orden - E41140,PDF.exe	Get hash	malicious	Browse	• 208.91.199.223
	SO230921.exe	Get hash	malicious	Browse	• 208.91.199.223
	Products prices request.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	3qyhcUC9um.exe	Get hash	malicious	Browse	• 208.91.198.143

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Advice 09-22-2021 SKMBT03783930484080484904003TXT.exe	Get hash	malicious	Browse	• 208.91.198.143
	from-iso_PSC ___ - E41140,PDF.EXE	Get hash	malicious	Browse	• 208.91.198.143
	n267kM6LhuZHjzz.exe	Get hash	malicious	Browse	• 208.91.198.143
	Payment copy.exe	Get hash	malicious	Browse	• 208.91.199.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	waff.xls	Get hash	malicious	Browse	• 204.11.59.34
	#RFQ Medimpex International LLC.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENTS_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	New Order.doc	Get hash	malicious	Browse	• 208.91.199.225
	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	#U0916#U0930#U0940#U0926 #U0906#U0926#U0947#U0936-34002174,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	#Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	4f7K9bfgNr.exe	Get hash	malicious	Browse	• 208.91.199.224
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.198.143
	Solicitud de cotizacion.exe	Get hash	malicious	Browse	• 208.91.198.143
	New Order.exe	Get hash	malicious	Browse	• 208.91.199.224
	KLC45E_92421_PI.exe	Get hash	malicious	Browse	• 208.91.199.224
	Request_For_Quotation#234242_signed_copy_document_september_rfq.exe	Get hash	malicious	Browse	• 162.215.240.160
	PO-3242.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	MONO Nueva orden - E41140,PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	SO230921.exe	Get hash	malicious	Browse	• 208.91.199.224
	Products prices request.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice 09-22-2021 SKMBT03783930484080484904003TXT.exe	Get hash	malicious	Browse	• 208.91.198.143
	from-iso_PSC ___ - E41140,PDF.EXE	Get hash	malicious	Browse	• 208.91.199.223
	n267kM6LhuZHjzz.exe	Get hash	malicious	Browse	• 208.91.198.143
PUBLIC-DOMAIN-REGISTRYUS	waff.xls	Get hash	malicious	Browse	• 204.11.59.34
	#RFQ Medimpex International LLC.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENTS_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	New Order.doc	Get hash	malicious	Browse	• 208.91.199.225
	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	#U0916#U0930#U0940#U0926 #U0906#U0926#U0947#U0936-34002174,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	#Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	4f7K9bfgNr.exe	Get hash	malicious	Browse	• 208.91.199.224
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.198.143
	Solicitud de cotizacion.exe	Get hash	malicious	Browse	• 208.91.198.143
	New Order.exe	Get hash	malicious	Browse	• 208.91.199.224
	KLC45E_92421_PI.exe	Get hash	malicious	Browse	• 208.91.199.224
	Request_For_Quotation#234242_signed_copy_document_september_rfq.exe	Get hash	malicious	Browse	• 162.215.240.160
	PO-3242.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	MONO Nueva orden - E41140,PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	SO230921.exe	Get hash	malicious	Browse	• 208.91.199.224
	Products prices request.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice 09-22-2021 SKMBT03783930484080484904003TXT.exe	Get hash	malicious	Browse	• 208.91.198.143
	from-iso_PSC ___ - E41140,PDF.EXE	Get hash	malicious	Browse	• 208.91.199.223
	n267kM6LhuZHjzz.exe	Get hash	malicious	Browse	• 208.91.198.143

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Inquiry - Specifications 002021.exe.log	
Process:	C:\Users\user\Desktop\Inquiry - Specifications 002021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1309
Entropy (8bit):	5.3528008810928345
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84aE4Ks:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzg
MD5:	542338C5A30B02E372089FECDC54D607
SHA1:	6FAD29FF14686FC847B160E876C1E078333F6DCB
SHA-256:	6CEA4E70947B962733754346CE49553BE3FB6E1FB3949C29EC22FA9CA4B7E7B6
SHA-512:	FE4431305A8958C4940EB4AC65723A38DA6057C3D30F789C6EDDEBA8962B62E9C0583254E74740855027CF3AE9315E3001A7EEB54168073ED0D2AB9B1F05503A
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..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\w04smpsc.51a\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Inquiry - Specifications 002021.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, 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):	6.817961825290743
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Inquiry - Specifications 002021.exe
File size:	881152
MD5:	768a1127c119149f96a29c0d0c0b56ec
SHA1:	afe86ab8d4a8b5b092e95f1cb2ae563f5ea5867d
SHA256:	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af

General

SHA512:	9288f45ef09172b28a4fa542b2ead2a2026b910eb229859125da6bfb735e0178e7e8dcd7c4eddc590646e409ccb6e180b24813f059e7f5f161983a3b7749c672
SSDEEP:	12288:goSLU8CqriiULSX7yUrMjgY6WDWzjXbdarHOsnoaLOAmQsaypSL+jQHmLDsBhvs8:3bIFJ9F9lPV3X2hM3akNQF+0F+2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...|.Qa.....0..... ....@.. .....@.....

File Icon

Icon Hash:	138e8eccece8cccc

Static PE Info

General

Entrypoint:	0x4bf602
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:	0x61511F7C [Mon Sep 27 01:33:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbd608	0xbd800	False	0.686279941046	data	7.0705910139	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x19424	0x19600	False	0.391692964901	data	4.29511012121	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-15:32:02.040982	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49849	587	192.168.2.3	208.91.198.143
09/27/21-15:32:06.598209	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49850	587	192.168.2.3	208.91.199.224

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 15:32:00.163115025 CEST	192.168.2.3	8.8.8.8	0xd9f2	Standard query (0)	smtp.vern-group.com	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:00.396828890 CEST	192.168.2.3	8.8.8.8	0x69b6	Standard query (0)	smtp.vern-group.com	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:04.844149113 CEST	192.168.2.3	8.8.8.8	0xe910	Standard query (0)	smtp.vern-group.com	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:05.071542978 CEST	192.168.2.3	8.8.8.8	0x574d	Standard query (0)	smtp.vern-group.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 15:32:00.319247007 CEST	8.8.8.8	192.168.2.3	0xd9f2	No error (0)	smtp.vern-group.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 15:32:00.319247007 CEST	8.8.8.8	192.168.2.3	0xd9f2	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:00.319247007 CEST	8.8.8.8	192.168.2.3	0xd9f2	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:00.319247007 CEST	8.8.8.8	192.168.2.3	0xd9f2	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:00.319247007 CEST	8.8.8.8	192.168.2.3	0xd9f2	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:00.585047960 CEST	8.8.8.8	192.168.2.3	0x69b6	No error (0)	smtp.vern-group.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 15:32:00.585047960 CEST	8.8.8.8	192.168.2.3	0x69b6	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:00.585047960 CEST	8.8.8.8	192.168.2.3	0x69b6	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:00.585047960 CEST	8.8.8.8	192.168.2.3	0x69b6	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:00.585047960 CEST	8.8.8.8	192.168.2.3	0x69b6	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:05.005784988 CEST	8.8.8.8	192.168.2.3	0xe910	No error (0)	smtp.vern-group.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 15:32:05.005784988 CEST	8.8.8.8	192.168.2.3	0xe910	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:05.005784988 CEST	8.8.8.8	192.168.2.3	0xe910	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:05.005784988 CEST	8.8.8.8	192.168.2.3	0xe910	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 15:32:05.005784988 CEST	8.8.8.8	192.168.2.3	0xe910	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:05.086332083 CEST	8.8.8.8	192.168.2.3	0x574d	No error (0)	smtp.vern-group.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 15:32:05.086332083 CEST	8.8.8.8	192.168.2.3	0x574d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:05.086332083 CEST	8.8.8.8	192.168.2.3	0x574d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:05.086332083 CEST	8.8.8.8	192.168.2.3	0x574d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Sep 27, 2021 15:32:05.086332083 CEST	8.8.8.8	192.168.2.3	0x574d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

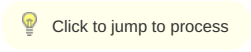
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Sep 27, 2021 15:32:01.146960974 CEST	587	49849	208.91.198.143	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Sep 27, 2021 15:32:01.147341967 CEST	49849	587	192.168.2.3	208.91.198.143	EHLO 364339
Sep 27, 2021 15:32:01.289591074 CEST	587	49849	208.91.198.143	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
Sep 27, 2021 15:32:01.292818069 CEST	49849	587	192.168.2.3	208.91.198.143	AUTH login YW5uZXR0LmphbG93aUB2ZXJuLWdyb3VwLmNvbQ==
Sep 27, 2021 15:32:01.431281090 CEST	587	49849	208.91.198.143	192.168.2.3	334 UGFzc3dvcmQ6
Sep 27, 2021 15:32:01.574882984 CEST	587	49849	208.91.198.143	192.168.2.3	235 2.7.0 Authentication successful
Sep 27, 2021 15:32:01.577059984 CEST	49849	587	192.168.2.3	208.91.198.143	MAIL FROM:<annett.jalowi@vern-group.com>
Sep 27, 2021 15:32:01.719269991 CEST	587	49849	208.91.198.143	192.168.2.3	250 2.1.0 Ok
Sep 27, 2021 15:32:01.719748974 CEST	49849	587	192.168.2.3	208.91.198.143	RCPT TO:<annett.jalowi@vern-group.com>
Sep 27, 2021 15:32:01.898897886 CEST	587	49849	208.91.198.143	192.168.2.3	250 2.1.5 Ok
Sep 27, 2021 15:32:01.899446964 CEST	49849	587	192.168.2.3	208.91.198.143	DATA
Sep 27, 2021 15:32:02.039216042 CEST	587	49849	208.91.198.143	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Sep 27, 2021 15:32:02.044569016 CEST	49849	587	192.168.2.3	208.91.198.143	.
Sep 27, 2021 15:32:02.286237955 CEST	587	49849	208.91.198.143	192.168.2.3	250 2.0.0 Ok: queued as CB0C4192B3B
Sep 27, 2021 15:32:04.643898964 CEST	49849	587	192.168.2.3	208.91.198.143	QUIT
Sep 27, 2021 15:32:04.785418987 CEST	587	49849	208.91.198.143	192.168.2.3	221 2.0.0 Bye
Sep 27, 2021 15:32:05.667896032 CEST	587	49850	208.91.199.224	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Sep 27, 2021 15:32:05.668147087 CEST	49850	587	192.168.2.3	208.91.199.224	EHLO 364339
Sep 27, 2021 15:32:05.817183971 CEST	587	49850	208.91.199.224	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
Sep 27, 2021 15:32:05.819185019 CEST	49850	587	192.168.2.3	208.91.199.224	AUTH login YW5uZXR0LmphbG93aUB2ZXJuLWdyb3VwLmNvbQ==
Sep 27, 2021 15:32:05.966929913 CEST	587	49850	208.91.199.224	192.168.2.3	334 UGFzc3dvcmQ6
Sep 27, 2021 15:32:06.116357088 CEST	587	49850	208.91.199.224	192.168.2.3	235 2.7.0 Authentication successful
Sep 27, 2021 15:32:06.116758108 CEST	49850	587	192.168.2.3	208.91.199.224	MAIL FROM:<annett.jalowi@vern-group.com>
Sep 27, 2021 15:32:06.265615940 CEST	587	49850	208.91.199.224	192.168.2.3	250 2.1.0 Ok
Sep 27, 2021 15:32:06.266062021 CEST	49850	587	192.168.2.3	208.91.199.224	RCPT TO:<annett.jalowi@vern-group.com>
Sep 27, 2021 15:32:06.437005997 CEST	587	49850	208.91.199.224	192.168.2.3	250 2.1.5 Ok
Sep 27, 2021 15:32:06.439989090 CEST	49850	587	192.168.2.3	208.91.199.224	DATA
Sep 27, 2021 15:32:06.586853981 CEST	587	49850	208.91.199.224	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Sep 27, 2021 15:32:06.598243952 CEST	49850	587	192.168.2.3	208.91.199.224	.
Sep 27, 2021 15:32:06.850157976 CEST	587	49850	208.91.199.224	192.168.2.3	250 2.0.0 Ok: queued as 5920E1CACDC

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Inquiry - Specifications 002021.exe PID: 1360 Parent PID: 1664

General

Start time:	15:30:03
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Inquiry - Specifications 002021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Inquiry - Specifications 002021.exe'
Imagebase:	0x70000
File size:	881152 bytes
MD5 hash:	768A1127C119149F96A29C0D0C0B56EC
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: 00000000.00000002.329163786.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.329163786.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.322481518.00000000024D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.322874820.000000000254D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Inquiry - Specifications 002021.exe PID: 6580 Parent PID: 1360

General

Start time:	15:30:16
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Inquiry - Specifications 002021.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Inquiry - Specifications 002021.exe
Imagebase:	0xa10000
File size:	881152 bytes
MD5 hash:	768A1127C119149F96A29C0D0C0B56EC
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: 00000005.00000002.559497777.00000000030EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.553693912.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.553693912.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.558228658.0000000002E01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.558228658.0000000002E01000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis