ID: 452459
Sample Name: RFQ_
21072021.exe
Cookbook: default.jbs
Time: 12:00:04
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

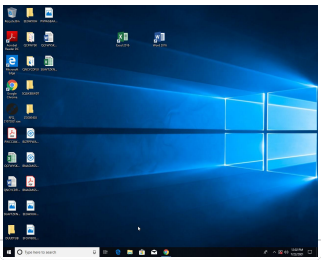
Windows Analysis Report RFQ_ 21072021.exe

Overview

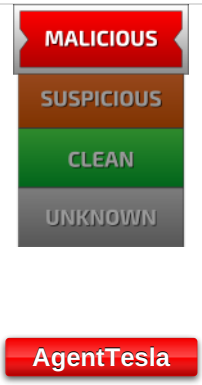
General Information

Sample Name:	RFQ_ 21072021.exe
Analysis ID:	452459
MD5:	0a74cbd4246a6e..
SHA1:	0a4f341f4e9b399..
SHA256:	4856e75e63f0c5c..
Infos:	

Most interesting Screenshot:



Detection



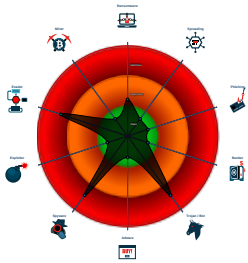
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- RFQ_ 21072021.exe (PID: 4792 cmdline: 'C:\Users\user\Desktop\RFQ_ 21072021.exe' MD5: 0A74CBD4246A6E11077876C572A3D507)
  - RFQ_ 21072021.exe (PID: 2408 cmdline: C:\Users\user\Desktop\RFQ_ 21072021.exe MD5: 0A74CBD4246A6E11077876C572A3D507)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "webmaster@tccinfaes.com",
  "Password": "transportes",
  "Host": "mail.tccinfaes.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.467647680.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.467647680.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.471299072.00000000031E1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RFQ_ 21072021.exe PID: 2408	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RFQ_ 21072021.exe PID: 2408	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RFQ_ 21072021.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.RFQ_ 21072021.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

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:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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:

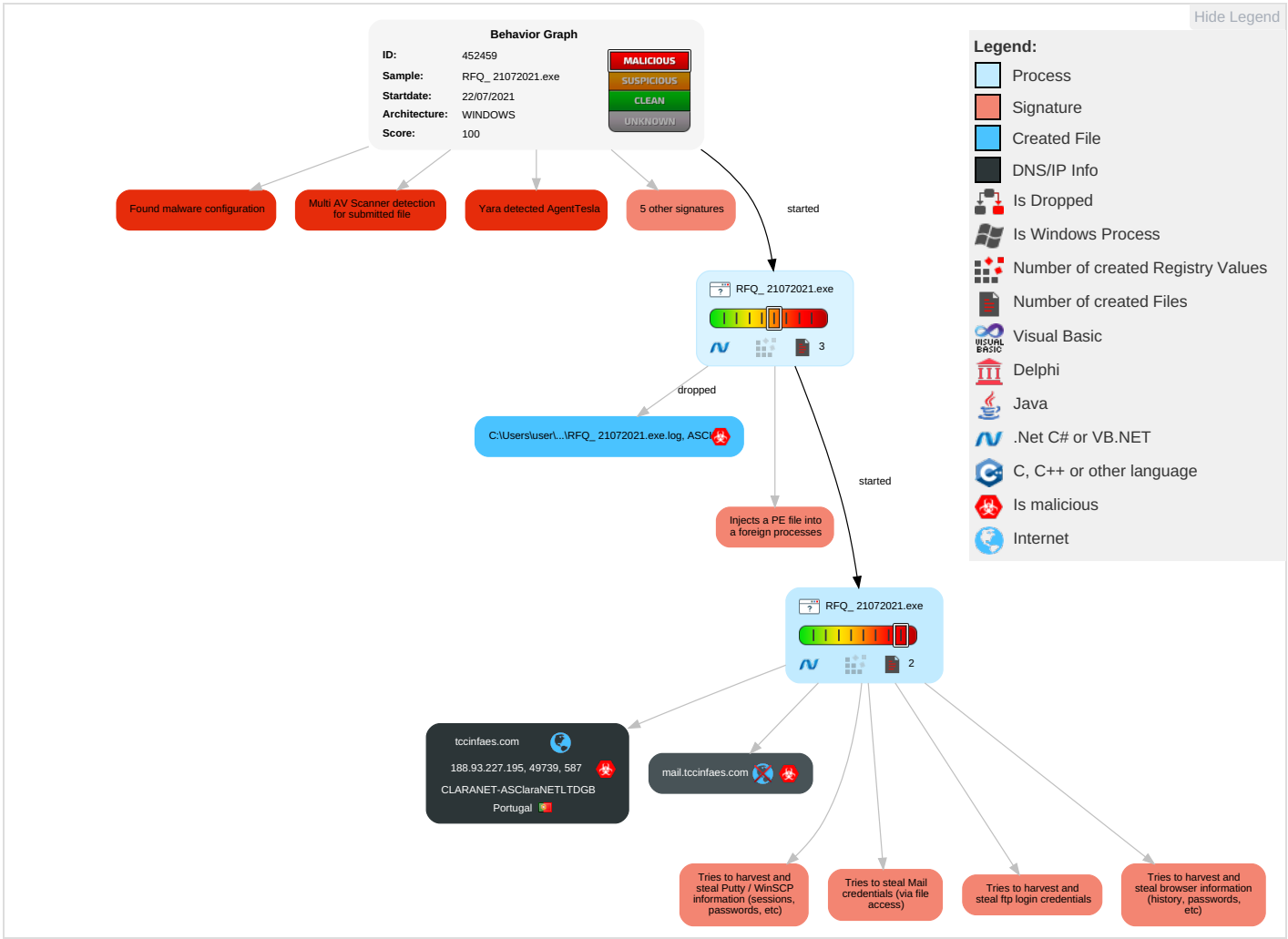
Yara detected AgentTesla

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	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RFQ_ 21072021.exe	30%	Virustotal		Browse
RFQ_ 21072021.exe	15%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
RFQ_ 21072021.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RFQ_ 21072021.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
tccinfaes.com	1%	Virustotal		Browse
mail.tccinfaes.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://mail.tccinfaes.com	2%	Virustotal		Browse
http://mail.tccinfaes.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://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://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://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://tccinfaes.com	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://TryUj9XyxT6LakY.org	0%	Avira URL Cloud	safe	
http://xmALXm.com	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0)	0%	URL Reputation	safe	
http://r3.i.lencr.org/0)	0%	URL Reputation	safe	
http://r3.i.lencr.org/0)	0%	URL Reputation	safe	
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://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tccinfaes.com	188.93.227.195	true	true	• 1%, Virustotal, Browse	unknown
mail.tccinfaes.com	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.93.227.195	tccinfaes.com	Portugal		8426	CLARANET-ASClaraNETLTDGB	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452459
Start date:	22.07.2021
Start time:	12:00:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ_ 21072021.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@2/1
EGA Information:	• Successful, ratio: 50%
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
12:01:14	API Interceptor	663x Sleep call for process: RFQ_ 21072021.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
188.93.227.195	NRPwo7uSCaLmXtV.exe	Get hash	malicious	Browse	
	zam#U00f3w 1536625_pdf.exe	Get hash	malicious	Browse	
	SHIPPING DOCUMENT.exe	Get hash	malicious	Browse	
	5evmU6c7Nx.exe	Get hash	malicious	Browse	
	Zam#U00f3wienie-017.2021.exe	Get hash	malicious	Browse	
	PO HDT01-07.xlsx	Get hash	malicious	Browse	
	184285013-044310-sanlccjavap0003-7069.exe	Get hash	malicious	Browse	
	PO DOCS 30-06.xlsx	Get hash	malicious	Browse	
	qiKDsbFyzQ.exe	Get hash	malicious	Browse	
	PO DHS312445.xlsx	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.MSIL_Kryptik.DVA.genEldorado.15172.exe	Get hash	malicious	Browse	
	TRANSFER SLIP00020212405_pdf.exe	Get hash	malicious	Browse	
	RFQ-284683839.001.exe	Get hash	malicious	Browse	
	Dane bankowe.exe	Get hash	malicious	Browse	
	33aee36c_by_Libranalysis.exe	Get hash	malicious	Browse	
	Dane bankowe.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLARANET-ASClaraNETLTDGB	5qpsqg7U0G	Get hash	malicious	Browse	• 185.77.75.98
	8wzyljMmmn	Get hash	malicious	Browse	• 138.248.76.96
	AT9n7Bk0yE	Get hash	malicious	Browse	• 195.8.76.231
	0aC0TBcdxb	Get hash	malicious	Browse	• 195.170.117.46
	NRPwo7uSCaLmXtV.exe	Get hash	malicious	Browse	• 188.93.227.195
	zam#U00f3w 1536625_pdf.exe	Get hash	malicious	Browse	• 188.93.227.195
	SHIPPING DOCUMENT.exe	Get hash	malicious	Browse	• 188.93.227.195
	5evmU6c7Nx.exe	Get hash	malicious	Browse	• 188.93.227.195
	Zam#U00f3wienie-017.2021.exe	Get hash	malicious	Browse	• 188.93.227.195
	PO HDT01-07.xlsx	Get hash	malicious	Browse	• 188.93.227.195
	184285013-044310-sanlccjavap0003-7069.exe	Get hash	malicious	Browse	• 188.93.227.195
	PO DOCS 30-06.xlsx	Get hash	malicious	Browse	• 188.93.227.195
	qiKDsbFyzQ.exe	Get hash	malicious	Browse	• 188.93.227.195
	PO DHS312445.xlsx	Get hash	malicious	Browse	• 188.93.227.195
	SecuriteInfo.com.W32.MSIL_Kryptik.DVA.genEldorado.15172.exe	Get hash	malicious	Browse	• 188.93.227.195
	TRANSFER SLIP00020212405_pdf.exe	Get hash	malicious	Browse	• 188.93.227.195
	RFQ-284683839.001.exe	Get hash	malicious	Browse	• 188.93.227.195
	Dane bankowe.exe	Get hash	malicious	Browse	• 188.93.227.195
	33aee36c_by_Libranalysis.exe	Get hash	malicious	Browse	• 188.93.227.195
	Dane bankowe.exe	Get hash	malicious	Browse	• 188.93.227.195

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ_ 21072021.exe.log	
Process:	C:\Users\user\Desktop\RFQ_ 21072021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.450390704563295
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	RFQ_ 21072021.exe
File size:	934400
MD5:	0a74cbd4246a6e11077876c572a3d507
SHA1:	0a4f341f4e9b399fa37a42e041bb3bb3b6f455ff
SHA256:	4856e75e63f0c5c14255001eefbea1d88c99fa8b7279dd0703a407a90b222b93
SHA512:	b04188c94acf13c205697681f273f370bb259ac782735b25854e412e7290a32214c00a2b0e5bf9e0d49888df2c6cc0a487ee88c320d9b440c0205b48895d1d59
SSDEEP:	12288:YSIt+/xerrmsnUsFIYHqCZnjKFBce/9ghkR6jDzjSbfeXnhLPu2syaUVKnpa:YZD/7nZ7H9njKFBcli67O6XhLjzahpa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Y..`.....X.....w... .....@.. .....@.....

File Icon

Icon Hash:	1749c81a994c2d93

Static PE Info

General

Entrypoint:	0x4c771e

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F91259 [Thu Jul 22 06:38:17 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	0xc5724	0xc5800	False	0.777621884889	data	7.56840197347	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xc8000	0x18	0x200	False	0.060546875	data	0.456640975135	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xca000	0x1e06c	0x1e200	False	0.304201244813	data	5.12107540034	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	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
Jul 22, 2021 12:02:55.214694023 CEST	192.168.2.3	8.8.8.8	0x9451	Standard query (0)	mail.tccinfaes.com	A (IP address)	IN (0x0001)
Jul 22, 2021 12:02:55.304380894 CEST	192.168.2.3	8.8.8.8	0x348c	Standard query (0)	mail.tccinfaes.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 12:02:55.289421082 CEST	8.8.8.8	192.168.2.3	0x9451	No error (0)	mail.tccinfaes.com	tccinfaes.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 12:02:55.289421082 CEST	8.8.8.8	192.168.2.3	0x9451	No error (0)	tccinfaes.com		188.93.227.195	A (IP address)	IN (0x0001)
Jul 22, 2021 12:02:55.362222910 CEST	8.8.8.8	192.168.2.3	0x348c	No error (0)	mail.tccinfaes.com	tccinfaes.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 12:02:55.362222910 CEST	8.8.8.8	192.168.2.3	0x348c	No error (0)	tccinfaes.com		188.93.227.195	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 22, 2021 12:02:55.718158007 CEST	587	49739	188.93.227.195	192.168.2.3	220-iberweb-11a.ibername.com ESMTP Exim 4.94.2 #2 Thu, 22 Jul 2021 11:02:54 +0100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jul 22, 2021 12:02:55.720782995 CEST	49739	587	192.168.2.3	188.93.227.195	EHLO 936905
Jul 22, 2021 12:02:55.804296017 CEST	587	49739	188.93.227.195	192.168.2.3	250-iberweb-11a.ibername.com Hello 936905 [84.17.52.8] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jul 22, 2021 12:02:55.804797888 CEST	49739	587	192.168.2.3	188.93.227.195	STARTTLS
Jul 22, 2021 12:02:55.890711069 CEST	587	49739	188.93.227.195	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RFQ_ 21072021.exe PID: 4792 Parent PID: 5668

General

Start time:	12:00:50
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\RFQ_ 21072021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ_ 21072021.exe'
Imagebase:	0x510000
File size:	934400 bytes
MD5 hash:	0A74CBD4246A6E11077876C572A3D507
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: RFQ_ 21072021.exe PID: 2408 Parent PID: 4792

General

Start time:	12:01:15
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\RFQ_ 21072021.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RFQ_ 21072021.exe
Imagebase:	0xd90000
File size:	934400 bytes
MD5 hash:	0A74CBD4246A6E11077876C572A3D507
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: 00000005.00000002.467647680.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.467647680.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.471299072.00000000031E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis