ID: 432660
Sample Name: i6xFULh8J5.exe
Cookbook: default.jbs
Time: 16:30:27
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

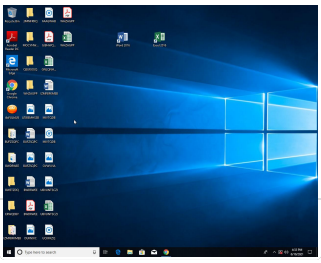
Analysis Report i6xFULh8J5.exe

Overview

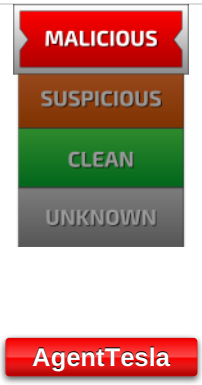
General Information

Sample Name:	i6xFULh8J5.exe
Analysis ID:	432660
MD5:	6c425cf25da766d..
SHA1:	874344555856dc..
SHA256:	0b72882fbad7f82..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

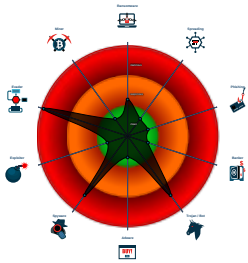


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- 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



Process Tree

- **System is w10x64**
- i6xFULh8J5.exe (PID: 6920 cmdline: 'C:\Users\user\Desktop\i6xFULh8J5.exe' MD5: 6C425CF25DA766D3D98597A9BE4E7300)
  - i6xFULh8J5.exe (PID: 6956 cmdline: 'C:\Users\user\Desktop\i6xFULh8J5.exe' MD5: 6C425CF25DA766D3D98597A9BE4E7300)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "no-reply@mytravelws.com",
  "Password": "hbhf@--8hyhb#E6g",
  "Host": "mail.mytravelws.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.915053341.000000000231 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.915053341.000000000231 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.913772727.000000000040 0000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.913772727.000000000040 0000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.916734898.000000000486 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.i6xFULh8J5.exe.400000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.i6xFULh8J5.exe.400000.1.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.i6xFULh8J5.exe.2310000.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.i6xFULh8J5.exe.2310000.4.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.i6xFULh8J5.exe.415058.0.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 31 entries				

Sigma Overview

No Sigma rule has matched

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

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

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

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:

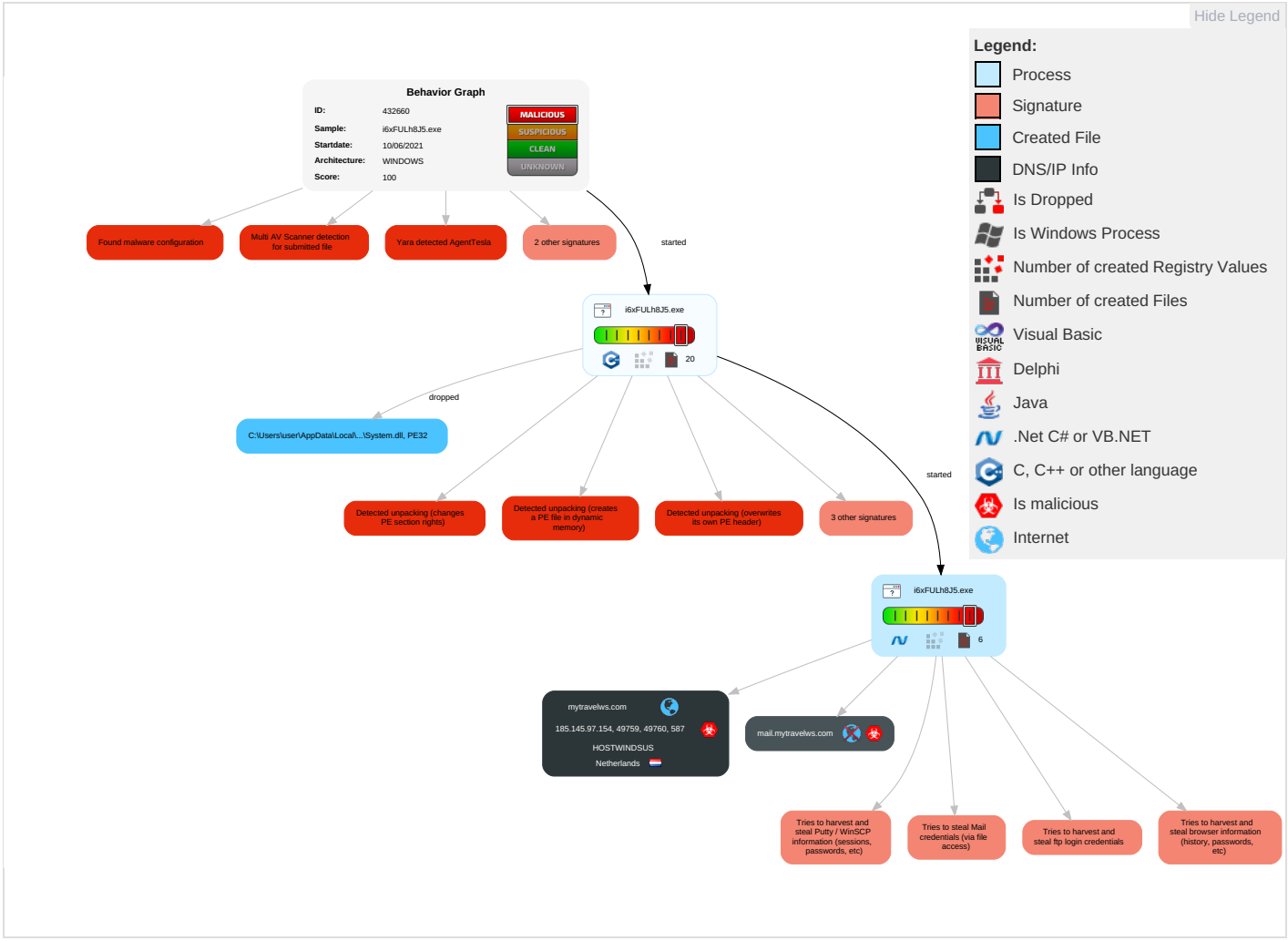
Yara detected AgentTesla

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	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 6	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 3 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Security Software Discovery 1 2 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 4 1	LSA Secrets	Process Discovery 2	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 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

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
i6xFULh8J5.exe	13%	Virustotal		Browse
i6xFULh8J5.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsm5CFC.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsm5CFC.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.i6xFULh8J5.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.2.i6xFULh8J5.exe.4860000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.i6xFULh8J5.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
1.0.i6xFULh8J5.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.0.i6xFULh8J5.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
1.1.i6xFULh8J5.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	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://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationScZ	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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://DZUhkq.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://Aloa82nGvgBCiZ.org	0%	Avira URL Cloud	safe	
http://mytravelws.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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://mail.mytravelws.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mytravelws.com	185.145.97.154	true	true		unknown
mail.mytravelws.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.145.97.154	mytravelws.com	Netherlands		54290	HOSTWINDSUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432660
Start date:	10.06.2021
Start time:	16:30:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	i6xFULh8J5.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:	16
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@3/5@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64.6% (good quality ratio 63.4%) • Quality average: 88.5% • Quality standard deviation: 21.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:31:28	API Interceptor	742x Sleep call for process: i6xFULh8J5.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.145.97.154	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	
	bnpQ6kcuVR.exe	Get hash	malicious	Browse	
	vbc (2).exe	Get hash	malicious	Browse	
	ST7Ado3UF0.exe	Get hash	malicious	Browse	
	P6Jz2vkfxM.exe	Get hash	malicious	Browse	
	report payment.xlsx	Get hash	malicious	Browse	
	sUBjOPCltO.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO-May-2021.xlsx	Get hash	malicious	Browse	
	0WkusO1rOi.exe	Get hash	malicious	Browse	
	H2alwW0WIT.exe	Get hash	malicious	Browse	
	YOWLnt9Yre.exe	Get hash	malicious	Browse	
	38 X 38 X 2.5 MM.xlsx	Get hash	malicious	Browse	
	Jj8w5yRkRd.exe	Get hash	malicious	Browse	
	9c1ed25a_by_Libranalysis.exe	Get hash	malicious	Browse	
	bNU0rOHXQb.exe	Get hash	malicious	Browse	
	0b8e201e_by_Libranalysis.exe	Get hash	malicious	Browse	
	AWSC-##YU.xlsx	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
HOSTWINDSUS	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	• 185.145.97.154
	PO.exe	Get hash	malicious	Browse	• 104.168.175.179
	___(__)10115_____210609.exe	Get hash	malicious	Browse	• 192.119.111.43
	#Ubc1c#Uc8fc#Ubd84(#Uc2e0#Uaddc)_10115_#Uc9c0#Uc544#Uc774#Ud14c#Ud06c_210608.exe	Get hash	malicious	Browse	• 192.119.111.43
	#Ubc1c#Uc8fc#Ubd84(#Uc2e0#Uaddc)_10115_#Uc9c0#Uc544#Uc774#Ud14c#Ud06c_210607.exe	Get hash	malicious	Browse	• 192.119.111.43
	Quote20210607.exe	Get hash	malicious	Browse	• 192.119.111.43
	bnpQ6kcuVR.exe	Get hash	malicious	Browse	• 185.145.97.154
	vbc (2).exe	Get hash	malicious	Browse	• 185.145.97.154
	20200237 Item List -#U00bb#U00e7#U00be#U00e7 #U00c0#U00fb#U00bf#U00eb.xlsx.exe	Get hash	malicious	Browse	• 192.119.111.43
	_.html	Get hash	malicious	Browse	• 192.236.192.242
	ST7Ado3UF0.exe	Get hash	malicious	Browse	• 185.145.97.154
	P6Jz2vkfxM.exe	Get hash	malicious	Browse	• 185.145.97.154
	report payment.xlsx	Get hash	malicious	Browse	• 185.145.97.154
	20210531 Item List (114578PZ) - #U00bb#U00e7#U00be #U00e7 #U00c0#U00fb#U00bf#U00eb.exe	Get hash	malicious	Browse	• 104.168.166.188
	PO-20210601.exe	Get hash	malicious	Browse	• 104.168.166.188
	Quote-20210601.exe	Get hash	malicious	Browse	• 104.168.166.188
	20200237 Item List (84EA) - #Uc0ac#Uc591 #Uc801#Uc6a9.exe	Get hash	malicious	Browse	• 104.168.166.188
	Quote-210601.exe	Get hash	malicious	Browse	• 104.168.166.188
	QUOTATION-FORM.exe	Get hash	malicious	Browse	• 104.168.166.188
	sUBjOPCltO.exe	Get hash	malicious	Browse	• 185.145.97.154

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsm5CFC.tmp\System.dll	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	
	090049000009000.exe	Get hash	malicious	Browse	
	dYy3yfSkwY.exe	Get hash	malicious	Browse	
	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	UGGJ4NnzFz.exe	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	3arZKnr21W.exe	Get hash	malicious	Browse	
	Shipping receipt.exe	Get hash	malicious	Browse	
	New Order TL273723734533.pdf.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	YZ8OvkljWm.exe	Get hash	malicious	Browse	
	U03c2doc.exe	Get hash	malicious	Browse	
	QUOTE061021.exe	Get hash	malicious	Browse	
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	
	PO187439.exe	Get hash	malicious	Browse	
	090009000000090.exe	Get hash	malicious	Browse	
	NEWORDERLIST.exe	Get hash	malicious	Browse	
	00404000004.exe	Get hash	malicious	Browse	
	40900900090000.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\cngupzj2oe	
Process:	C:\Users\user\Desktop\i6xFULh8J5.exe
File Type:	data
Category:	dropped
Size (bytes):	292864
Entropy (8bit):	**7.999431096026405**
Encrypted:	**true**
SSDEEP:	6144:Fl0wrd3yw6dDxCbwJQ2BYabuiDeD7rSphe5Tx/J81Y454:/rNyzCbwGebpheTx/Ju4
MD5:	50C707C4A6C86D7DEEA6AB366421D287
SHA1:	D8C267A75759ACFA4C41440FA114F1537C1C6DEB
SHA-256:	D318B7EA53EA3BAEA3077BDF6A509F5795F50347BCED88553B49224322115CBF
SHA-512:	B0E7AD4DB0358D8598E97EC9D3766115520CEA7586B1E1145DDB08D94DE4C39CE541CB5E11BDD45054B222778708A30A98B4044809110D76825F52DE8B20DDE
Malicious:	false
Reputation:	low
Preview:	....#.Z...Z..r..n...V.....'.]....(.....c[..&C.[.zP_..~..z.^.8.....1|.Y...../....4...Z.f.hX.<...P......\..z._c6....._.g..Q...wm....`.Q...\...@...~...d...#..-..mY....M:.....C5<E....S..}.?K@YG+..1.....1. >@5.$...Fs.....2.P.....v...J.P.{.R..E>a..e....(=l.@R|.....^.K.1../..n..2..yh..\../.eq.l...74~..K..o..CM.<.Z..AP...#.....ye./p..F....>"*...a.aT.8..5X.....-t..*...Mi.b...x....j.`|?.....".(.. ...cA..k.A}..T..E.u (...5..'.M...D.3.c.w.L.&.t..P.wb[V...S._....8.....#f."...o'.~....d.....^Q.L.4.n.E....g..M..R..S....b_[.0+..iT....X`...hQ...h..l4..d.O...X.....>.L.Xn....D.|.Q.{.0]/.S..>.Ry. .=.@w....xKu.w..U.....Z.8<...v..>_9L....y."..*..A2...A..QW.=.....,G..4.O.\M.s.Lig....> .....^..H.`lb$.....2._7.c....|!n.O4%?>O.*.'.5|..fl.....i.N]".8....1...b.L.Ev.....$._..O@..j$.... (.pW....._.O...U..j3....(ag].3v..[...E..>..U.kh..M...;..~R+.3.f.....0.V.T+AC.Z.J..F..W~11.YD....|i.c.a.W{.....P..R{S.] x..c.x3....J.f...._...+

C:\Users\user\AppData\Local\Temp\imrixuzycldld	
Process:	C:\Users\user\Desktop\i6xFULh8J5.exe
File Type:	data
Category:	dropped
Size (bytes):	56353
Entropy (8bit):	4.960718014510871
Encrypted:	false
SSDEEP:	768:PtBIk3+DDvjQSgCsBn/7sUA+J2/yBjJi+X7eqJpVxdk2q8xlB9mPiM8+xlMg8VS:1y/DCdBDsd+JQelnVxdkB8/B9mPi2yVS
MD5:	9C22DFC73C577BE53A2D0216ED1D846F
SHA1:	B6C3D777BFD8D4EA20AF30D77D413B50B558CB88
SHA-256:	CC6D0EC0C062FBB1934B0CDE671CD19F10130B7773F707F3CEBFC48841268DE3
SHA-512:	ED4A93461E65AD09228481AA973082F4319453ED77D62273E8535C8DD25FD7C92CA4BB1CF4A5D467E1D1B04593B9CEE3E30079CC682F32D8242E84BDD0C0DF
Malicious:	false
Reputation:	low
Preview:	U.....p...).q.....r.....s.....t.....u.....v...k.w.....x.....y...d.z.....{.....|.....}...k.~.....f.....O.....6..... .....k.....k.....k.....Z.....K.....N.....2.....m.....'....'....'..... .....2.....k.....k.....k.....2....Z.....2....K....N.....m.....'....'....'.....f... .....k.....f.....k.....f

C:\Users\user\AppData\Local\Temp\nsm5CFB.tmp	
Process:	C:\Users\user\Desktop\i6xFULh8J5.exe
File Type:	data
Category:	dropped
Size (bytes):	388931
Entropy (8bit):	7.644285707033539
Encrypted:	false
SSDEEP:	6144:ph4l0wrd3yw6dDxCbwJQ2BYabuiDeD7rSphe5Tx/J81Y45s/ZQjkIuPut:KrNyzCbwGebpheTx/JusCjkI8m
MD5:	779592F0B8F98EBF3E724421735E1876
SHA1:	97C3E60CF03CBF2F57F78A172E09A53DB520F9E5

C:\Users\user\AppData\Local\Temp\nsm5CFB.tmp	
SHA-256:	9066D1B11F2B6FB122A37F20AA9DFD2FFFC99230A3328844E5BFBB79857FCE9A
SHA-512:	3F97F51DCA3A32825DB0806304137B16DDDBED911FBFAFEF70ACDA34D8093AC3C90B6EADA45FF32A190D1B8E0A279915E82AF5BE5EE5AEBCDCB69E12C3D18D53
Malicious:	false
Reputation:	low
Preview:	.m.....LP.....I.....I.....#..... .....J.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\nsm5CFC.tmp\System.dll	
Process:	C:\Users\user\Desktop\i6xFULh8J5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: AWB00028487364 -000487449287.doc, Detection: malicious, Browse • Filename: 090049000009000.exe, Detection: malicious, Browse • Filename: dYy3yfSkwY.exe, Detection: malicious, Browse • Filename: PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx, Detection: malicious, Browse • Filename: Purchase Order Price List 061021.xlsx, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: UGGJ4NnzFz.exe, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: 3arZKnr21W.exe, Detection: malicious, Browse • Filename: Shipping receipt.exe, Detection: malicious, Browse • Filename: New Order TL273723734533.pdf.exe, Detection: malicious, Browse • Filename: YZ8OvkljWm.exe, Detection: malicious, Browse • Filename: U03c2doc.exe, Detection: malicious, Browse • Filename: QUOTE061021.exe, Detection: malicious, Browse • Filename: PAYMENT CONFIRMATION.exe, Detection: malicious, Browse • Filename: PO187439.exe, Detection: malicious, Browse • Filename: 090090000000090.exe, Detection: malicious, Browse • Filename: NEWORDERLIST.exe, Detection: malicious, Browse • Filename: 00404000004.exe, Detection: malicious, Browse • Filename: 40900900090000.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Roaming\xnpbd3fr.5ju\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\i6xFULh8J5.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
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, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.080951210547221
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	i6xFULh8J5.exe
File size:	540995
MD5:	6c425cf25da766d3d98597a9be4e7300
SHA1:	874344555856dca223730f32ac81b8a743db4cfd
SHA256:	0b72882fbad7f826525003747565e03257ad2e9f60b70d5 3fe11686dfff1705c
SHA512:	6a43093a9eb59d68c6fc7347eab380bd9dd35d4b8badc5 8eb744643e6a7b97425b6b5f21078c46bd9ef988c4ec4b8 13a14cf2a92f8e2e557c0dda5d82a6a87a9
SSDEEP:	6144:6sS4XfaAuVCZHen8rTxSLMsM30U2ckP0v5AhLx r0sQfjF9fc5+L+k6uzVXvC2f/N:skNfxxvxe0RAz4eo4cVR f/pJdNoSAg
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....1..:u..iu.. iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE. .L.....K.....\.....

File Icon

Icon Hash:	31f8d4f0e8f47080

Static PE Info

General

Entrypoint:	0x40323c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x2ea88	0x2ec00	False	0.348648479278	data	4.44560190393	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 16:33:07.010297060 CEST	192.168.2.4	8.8.8.8	0x32a0	Standard query (0)	mail.mytravelws.com	A (IP address)	IN (0x0001)
Jun 10, 2021 16:33:07.089621067 CEST	192.168.2.4	8.8.8.8	0x3c7a	Standard query (0)	mail.mytravelws.com	A (IP address)	IN (0x0001)
Jun 10, 2021 16:33:11.307936907 CEST	192.168.2.4	8.8.8.8	0x10e9	Standard query (0)	mail.mytravelws.com	A (IP address)	IN (0x0001)
Jun 10, 2021 16:33:11.389303923 CEST	192.168.2.4	8.8.8.8	0xca35	Standard query (0)	mail.mytravelws.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 16:33:07.077755928 CEST	8.8.8.8	192.168.2.4	0x32a0	No error (0)	mail.mytravelws.com	mytravelws.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 16:33:07.077755928 CEST	8.8.8.8	192.168.2.4	0x32a0	No error (0)	mytravelws.com		185.145.97.154	A (IP address)	IN (0x0001)
Jun 10, 2021 16:33:07.151684999 CEST	8.8.8.8	192.168.2.4	0x3c7a	No error (0)	mail.mytravelws.com	mytravelws.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 16:33:07.151684999 CEST	8.8.8.8	192.168.2.4	0x3c7a	No error (0)	mytravelws.com		185.145.97.154	A (IP address)	IN (0x0001)
Jun 10, 2021 16:33:11.366795063 CEST	8.8.8.8	192.168.2.4	0x10e9	No error (0)	mail.mytravelws.com	mytravelws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 16:33:11.366795063 CEST	8.8.8.8	192.168.2.4	0x10e9	No error (0)	mytravelws.com		185.145.97.154	A (IP address)	IN (0x0001)
Jun 10, 2021 16:33:11.458507061 CEST	8.8.8.8	192.168.2.4	0xca35	No error (0)	mail.mytravelws.com	mytravelws.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 16:33:11.458507061 CEST	8.8.8.8	192.168.2.4	0xca35	No error (0)	mytravelws.com		185.145.97.154	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 10, 2021 16:33:07.407892942 CEST	587	49759	185.145.97.154	192.168.2.4	220-servertrv.mytravelws.com ESMTP Exim 4.94.2 #2 Thu, 10 Jun 2021 14:33:07 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 10, 2021 16:33:07.408173084 CEST	49759	587	192.168.2.4	185.145.97.154	EHLO 301389
Jun 10, 2021 16:33:07.461004972 CEST	587	49759	185.145.97.154	192.168.2.4	250-servertrv.mytravelws.com Hello 301389 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Jun 10, 2021 16:33:07.461407900 CEST	49759	587	192.168.2.4	185.145.97.154	STARTTLS
Jun 10, 2021 16:33:07.515892029 CEST	587	49759	185.145.97.154	192.168.2.4	220 TLS go ahead
Jun 10, 2021 16:33:11.592566013 CEST	587	49760	185.145.97.154	192.168.2.4	220-servertrv.mytravelws.com ESMTP Exim 4.94.2 #2 Thu, 10 Jun 2021 14:33:11 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 10, 2021 16:33:11.593064070 CEST	49760	587	192.168.2.4	185.145.97.154	EHLO 301389
Jun 10, 2021 16:33:11.645109892 CEST	587	49760	185.145.97.154	192.168.2.4	250-servertrv.mytravelws.com Hello 301389 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Jun 10, 2021 16:33:11.647048950 CEST	49760	587	192.168.2.4	185.145.97.154	STARTTLS
Jun 10, 2021 16:33:11.701004028 CEST	587	49760	185.145.97.154	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: i6xFULh8J5.exe PID: 6920 Parent PID: 5940

General

Start time:	16:31:16
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\i6xFULh8J5.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\i6xFULh8J5.exe'
Imagebase:	0x400000
File size:	540995 bytes
MD5 hash:	6C425CF25DA766D3D98597A9BE4E7300
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: 00000000.00000002.657892904.00000000022C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.657892904.00000000022C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: i6xFULh8J5.exe PID: 6956 Parent PID: 6920

General

Start time:	16:31:17
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\i6xFULh8J5.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\i6xFULh8J5.exe'
Imagebase:	0x400000
File size:	540995 bytes
MD5 hash:	6C425CF25DA766D3D98597A9BE4E7300
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: 00000001.00000002.915053341.0000000002310000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.915053341.0000000002310000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.913772727.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.913772727.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.916734898.0000000004862000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.916734898.0000000004862000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.915137007.0000000002381000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.915996454.0000000003381000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.915996454.0000000003381000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000001.654864588.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000001.654864588.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.914093005.0000000000549000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.914093005.0000000000549000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis