ID: 432673
Sample Name: supply us this product.exe
Cookbook: default.jbs
Time: 16:42:14
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

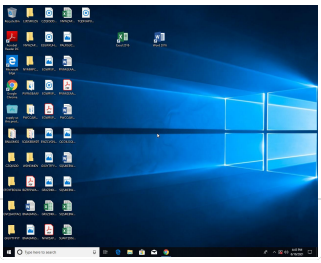
Analysis Report supply us this product.exe

Overview

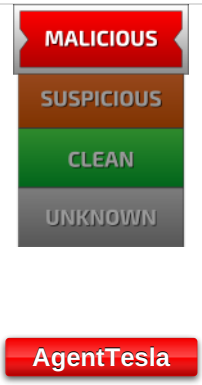
General Information

Sample Name:	supply us this product.exe
Analysis ID:	432673
MD5:	958f243581dc2ed.
SHA1:	cd163dd563fa0cd..
SHA256:	ae44346a0297d8..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

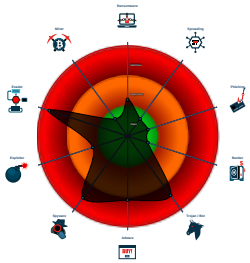


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Modifies the hosts file
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Process Tree

- **System is w10x64**
- supply us this product.exe (PID: 5764 cmdline: 'C:\Users\user\Desktop\supply us this product.exe' MD5: 958F243581DC2EDA4E763086875E9A0B)
  - supply us this product.exe (PID: 4800 cmdline: C:\Users\user\Desktop\supply us this product.exe MD5: 958F243581DC2EDA4E763086875E9A0B)
  - supply us this product.exe (PID: 4772 cmdline: C:\Users\user\Desktop\supply us this product.exe MD5: 958F243581DC2EDA4E763086875E9A0B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "ideshow@eflownutrition.com",
  "Password": "ngozi8989",
  "Host": "mail.scottbyscott.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.216164536.000000000252E000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000000.212702747.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.212702747.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.216940516.00000000034F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.216940516.00000000034F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 7 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.supply us this product.exe.3770470.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.supply us this product.exe.3770470.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.supply us this product.exe.3770470.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.supply us this product.exe.3770470.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.2.supply us this product.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

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:

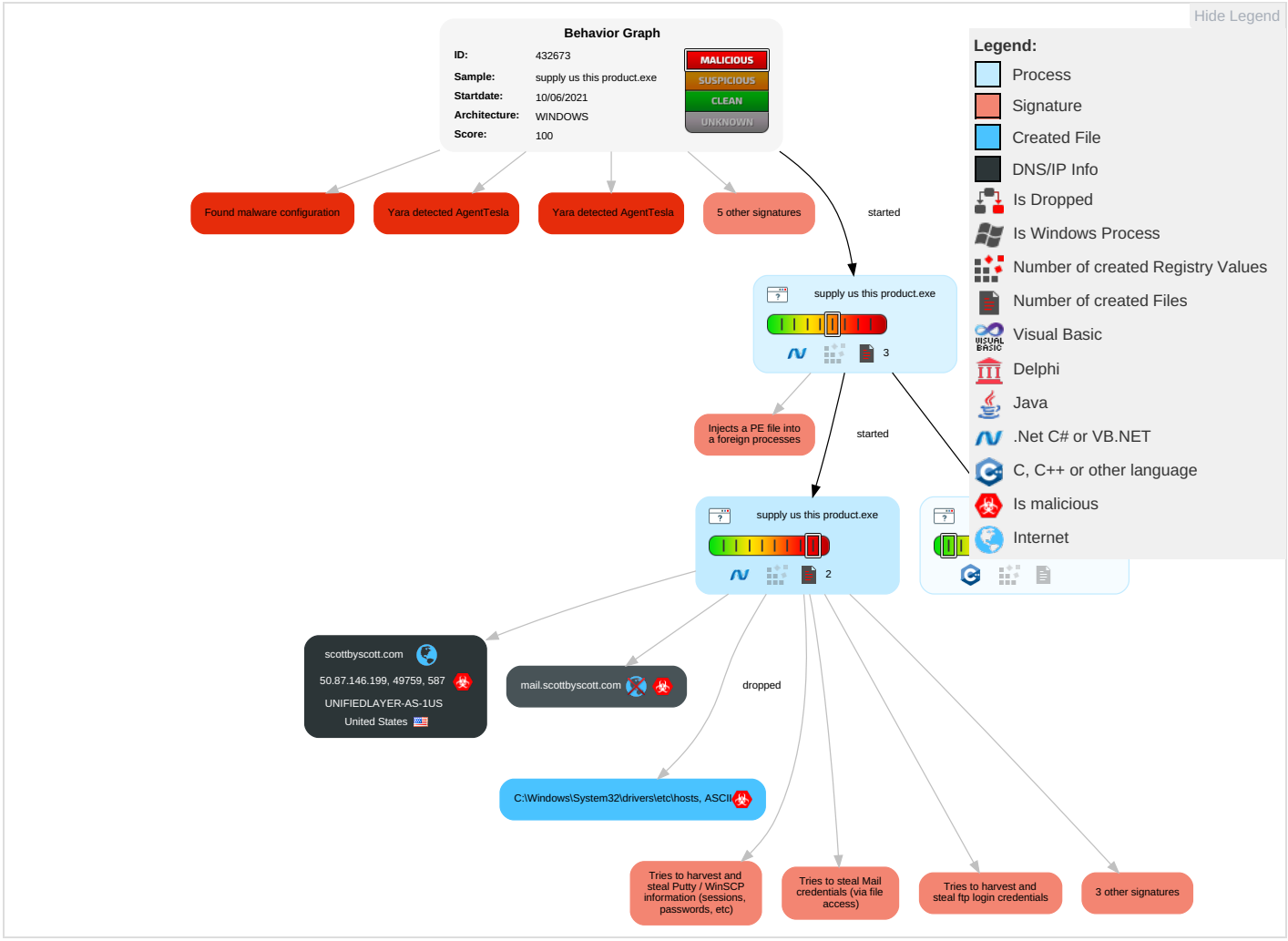
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 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	Input Capture 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applicatio Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Applicatio Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 3	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Prot

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
supply us this product.exe	9%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.supply us this product.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.supply us this product.exe.400000.1.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	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://scottbyscott.com	0%	Avira URL Cloud	safe	
http://htwqxRSsZE4FT.org	0%	Avira URL Cloud	safe	
http://mail.scottbyscott.com	0%	Avira URL Cloud	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://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://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://vmyBzt.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://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	
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scottbyscott.com	50.87.146.199	true	true		unknown
mail.scottbyscott.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.87.146.199	scottbyscott.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432673
Start date:	10.06.2021

Start time:	16:42:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	supply us this product.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.adwa.spyw.evad.winEXE@5/2@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.1% (good quality ratio 1%) • Quality average: 47.9% • Quality standard deviation: 25.7%
HCA Information:	• Successful, ratio: 98% • 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
16:43:04	API Interceptor	740x Sleep call for process: supply us this product.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 192.185.74.169
	3arZKnr21W.exe	Get hash	malicious	Browse	• 192.254.235.195
	6b6zVfqxbk.xlsb	Get hash	malicious	Browse	• 216.172.184.23

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HM-20210428 HBL.exe	Get hash	malicious	Browse	• 192.254.180.165
	INQUIRY. ZIP.exe	Get hash	malicious	Browse	• 50.87.190.227
	audit-78958169.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	research-1315978726.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	ExHNIXd73f.exe	Get hash	malicious	Browse	• 108.167.142.232
	research-2012220787.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	research-2012220787.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	viVrtGR9Wg.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	DEMLwnv0Nt.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	audit-367497006.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	analysis-31947858.xlsb	Get hash	malicious	Browse	• 108.167.156.223
	analysis-1593377733.xlsb	Get hash	malicious	Browse	• 108.167.156.223
	research-531942606.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	OM PHOENIX TRADERS.exe	Get hash	malicious	Browse	• 192.254.185.244
	research-121105165.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	research-76934760.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	research-1960540844.xlsx	Get hash	malicious	Browse	• 192.185.33.8

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\supply us this product.exe.log	
Process:	C:\Users\user\Desktop\supply us this product.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:	false
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

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\supply us this product.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11

C:\Windows\System32\drivers\etc\hosts	
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.607581520365733
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:	supply us this product.exe
File size:	907264
MD5:	958f243581dc2eda4e763086875e9a0b
SHA1:	cd163dd563fa0cda762ab9c5df8743f053fed612
SHA256:	ae44346a0297d8a9deab5419ff2b4679b83646abbed05b835c90fc33eb3ce2d5
SHA512:	da0face65969d9ec3626eae938111a7bd863a842b19fbd8ecefc8df6dd011652a157ab476d857d8af7e7a8506bf6e4a4de205958242ddbf059c9a6791fcd78c3
SSDEEP:	12288:bUV7Cwg8mnQigQl1j/Bi31o8BAAmx9HvBI0RA43AGDhZM4e/ZUdtb:bmC4mjgQzj/BiFFafx9F9AchNeBUdt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...M..`.....P..0.....fO... ...`....@.. .....@.....@.....

File Icon

Icon Hash:	8c8caa8e9692aa00

Static PE Info

General

Entrypoint:	0x4b4f66
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:	0x60C2164D [Thu Jun 10 13:40:29 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General

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	0xb2f6c	0xb3000	False	0.946567300978	data	7.95544670392	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x2a3d4	0x2a400	False	0.12447993713	data	4.17411605052	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 16:45:00.238121986 CEST	192.168.2.3	8.8.8.8	0xbed1	Standard query (0)	mail.scott byscott.com	A (IP address)	IN (0x0001)
Jun 10, 2021 16:45:00.766784906 CEST	192.168.2.3	8.8.8.8	0xa072	Standard query (0)	mail.scott byscott.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 16:45:00.436954975 CEST	8.8.8.8	192.168.2.3	0xbed1	No error (0)	mail.scott byscott.com	scottbyscott.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 16:45:00.436954975 CEST	8.8.8.8	192.168.2.3	0xbed1	No error (0)	scottbyscott.com		50.87.146.199	A (IP address)	IN (0x0001)
Jun 10, 2021 16:45:00.826528072 CEST	8.8.8.8	192.168.2.3	0xa072	No error (0)	mail.scott byscott.com	scottbyscott.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 16:45:00.826528072 CEST	8.8.8.8	192.168.2.3	0xa072	No error (0)	scottbyscott.com		50.87.146.199	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 10, 2021 16:45:03.956713915 CEST	587	49759	50.87.146.199	192.168.2.3	220-gator3013.hostgator.com ESMTP Exim 4.94.2 #2 Thu, 10 Jun 2021 09:45:03 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 10, 2021 16:45:03.957417011 CEST	49759	587	192.168.2.3	50.87.146.199	EHLO 045012
Jun 10, 2021 16:45:04.145348072 CEST	587	49759	50.87.146.199	192.168.2.3	250-gator3013.hostgator.com Hello 045012 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 10, 2021 16:45:04.145904064 CEST	49759	587	192.168.2.3	50.87.146.199	STARTTLS
Jun 10, 2021 16:45:04.340920925 CEST	587	49759	50.87.146.199	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: supply us this product.exe PID: 5764 Parent PID: 5780

General

Start time:	16:43:03
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\supply us this product.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\supply us this product.exe'
Imagebase:	0xc0000
File size:	907264 bytes
MD5 hash:	958F243581DC2EDA4E763086875E9A0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.216164536.000000000252E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.216940516.00000000034F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.216940516.00000000034F9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: supply us this product.exe PID: 4800 Parent PID: 5764

General

Start time:	16:43:06
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\supply us this product.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\supply us this product.exe
Imagebase:	0x420000
File size:	907264 bytes
MD5 hash:	958F243581DC2EDA4E763086875E9A0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: supply us this product.exe PID: 4772 Parent PID: 5764

General

Start time:	16:43:06
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\supply us this product.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\supply us this product.exe
Imagebase:	0x4c0000
File size:	907264 bytes
MD5 hash:	958F243581DC2EDA4E763086875E9A0B
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: 00000005.00000000.212702747.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.212702747.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.476764881.0000000002881000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.471383380.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.471383380.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis