ID: 358219
Sample Name: malware.exe
Cookbook: default.jbs
Time: 08:57:15
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

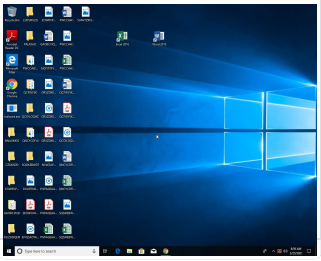
Analysis Report malware.exe

Overview

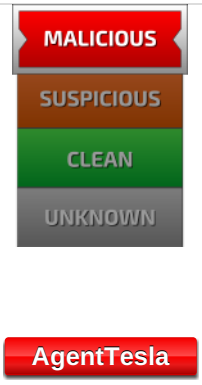
General Information

Sample Name:	malware.exe
Analysis ID:	358219
MD5:	2ee5a68ee37af14.
SHA1:	c27220c28c6119..
SHA256:	7e2a3464cd57a8..
Infos:	

Most interesting Screenshot:



Detection



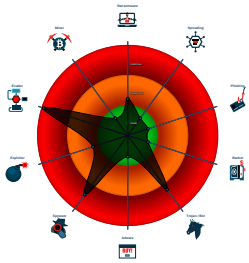
AgentTesla

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

Signatures

- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- Binary contains a suspicious time st…
- Found evasive API chain (trying to d…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- PE file contains section with special…

Classification



Startup

- **System is w10x64**
- malware.exe (PID: 6380 cmdline: 'C:\Users\user\Desktop\malware.exe' MD5: 2EE5A68EE37AF14C612FC4C8A589858A)
  - malware.exe (PID: 6536 cmdline: C:\Users\user\Desktop\malware.exe MD5: 2EE5A68EE37AF14C612FC4C8A589858A)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "info@nijos.esJose170458@smtp.ionos.es"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.459799944.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.201606646.000000000335E000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.201927296.00000000040B5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.465412261.00000000039D8000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.464476473.000000000353000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 5 entries

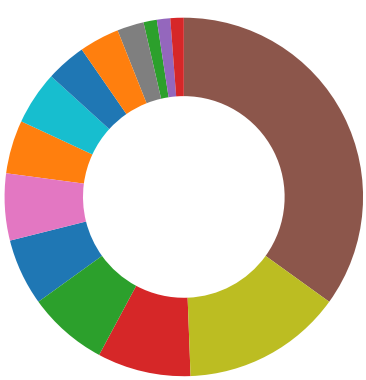
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.malware.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.malware.exe.4374cd0.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.malware.exe.4374cd0.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.malware.exe.421ba00.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.malware.exe.4277620.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

System Summary:

.NET source code contains very large array initializations

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Binary contains a suspicious time stamp

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Found evasive API chain (trying to detect sleep duration tampering with parallel thread)
- 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

Stealing of Sensitive Information:

- 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:

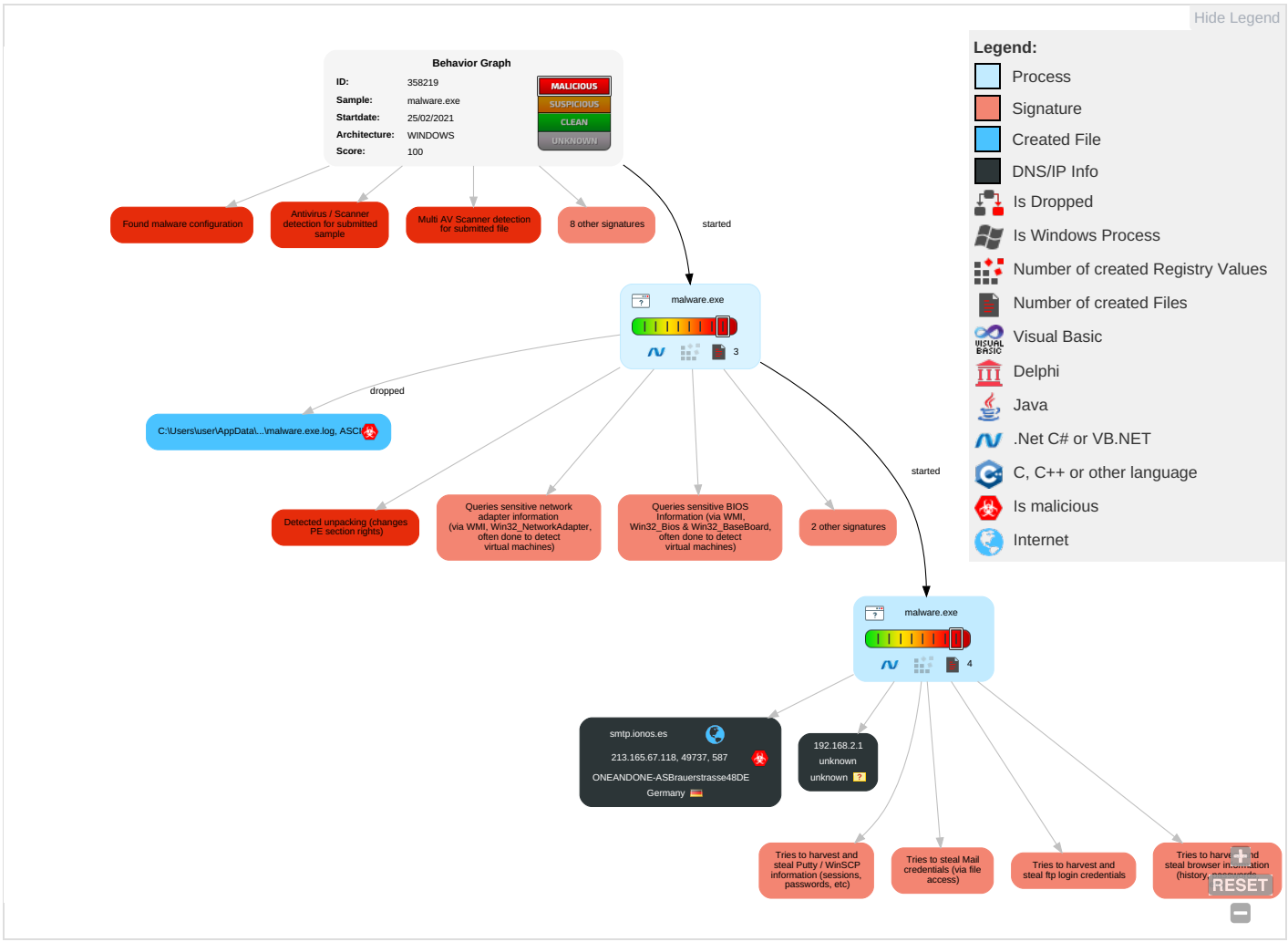
- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Obfuscated Files or Information 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 4	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 4	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 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
malware.exe	45%	Virustotal		Browse
malware.exe	30%	Metadefender		Browse
malware.exe	69%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
malware.exe	100%	Avira	HEUR/AGEN.1138558	
malware.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.malware.exe.930000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
3.2.malware.exe.ef0000.1.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
3.2.malware.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.malware.exe.930000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
3.0.malware.exe.ef0000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File

Domains

Source	Detection	Scanner	Label	Link
smtp.ionos.es	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://QDDeRKxxql47yvGyut1.com4	0%	Avira URL Cloud	safe	
http://https://QDDeRKxxql47yvGyut1.com	0%	Avira URL Cloud	safe	
http://eYrjmd.com	0%	Avira URL Cloud	safe	
http://https://QDDeRKxxql47yvGyut1.co	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://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
smtp.ionos.es	213.165.67.118	true	true	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	malware.exe, 00000003.00000002.464476473.0000000003531000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	malware.exe, 00000003.00000002.464476473.0000000003531000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://QDDeRKxxql47yvGyut1.com4	malware.exe, 00000003.00000002.465412261.00000000039D8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://QDDeRKxxql47yvGyut1.com	malware.exe, 00000003.00000002.465412261.00000000039D8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://eYrjmd.com	malware.exe, 00000003.00000002.464476473.0000000003531000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://QDDeRKxxql47yvGyut1.co	malware.exe, 00000003.00000002.465505838.0000000003A2D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	malware.exe, 00000003.00000002.464476473.0000000003531000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	malware.exe, 00000000.00000002.201927296.00000000040B5000.00000004.00000001.sdmp, malware.exe, 00000003.00000002.459799944.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	malware.exe, 00000000.00000002.201606646.000000000335E000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.165.67.118	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358219
Start date:	25.02.2021
Start time:	08:57:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	malware.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:	28
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@1/2
EGA Information:	Failed
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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 92.122.145.220, 131.253.33.200, 13.107.22.200, 104.43.193.48, 13.64.90.137, 52.255.188.83, 51.11.168.160, 184.30.20.56, 92.122.213.247, 92.122.213.194, 20.54.26.129, 51.104.139.180 • Excluded domains from analysis (whitelisted): www.bing.com, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:58:01	API Interceptor	980x Sleep call for process: malware.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
213.165.67.118	JUSTF11.exe	Get hash	malicious	Browse	
	FAC20.exe	Get hash	malicious	Browse	
	TRANFl.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JUSTF2.tar	Get hash	malicious	Browse	
	Oroder no 3.exe	Get hash	malicious	Browse	
	ORDER0984653.exe	Get hash	malicious	Browse	
	34433453-WONDN5-FTBO-9766464.exe	Get hash	malicious	Browse	
	Catalogs.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.ionos.es	JUSTF11.exe	Get hash	malicious	Browse	• 213.165.67.118
	FAC20.exe	Get hash	malicious	Browse	• 213.165.67.118
	TRANFI.exe	Get hash	malicious	Browse	• 213.165.67.118
	JUSTF2.tar	Get hash	malicious	Browse	• 213.165.67.118
	JUST1F1CA.exe	Get hash	malicious	Browse	• 213.165.67.102
	orders.exe	Get hash	malicious	Browse	• 213.165.67.102
	Oroder no 3.exe	Get hash	malicious	Browse	• 213.165.67.102
	ORDER0984653.exe	Get hash	malicious	Browse	• 213.165.67.118
	ORDER8162020.exe	Get hash	malicious	Browse	• 213.165.67.102
	4642WOT-T7864-66OBO.exe	Get hash	malicious	Browse	• 213.165.67.102
	34433453-WONDN5-FTBO-9766464.exe	Get hash	malicious	Browse	• 213.165.67.118
	Catalogs.exe	Get hash	malicious	Browse	• 213.165.67.118
	86597599579.exe	Get hash	malicious	Browse	• 213.165.67.102
	troystealer.exe	Get hash	malicious	Browse	• 213.165.67.102

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	Betalingsadvies Opmerking.exe	Get hash	malicious	Browse	• 212.227.15.142
	42#U0438.exe	Get hash	malicious	Browse	• 212.227.15.142
	WYX-09901.exe	Get hash	malicious	Browse	• 212.227.15.142
	530000.exe	Get hash	malicious	Browse	• 82.165.103.72
	raLXirFBY1.exe	Get hash	malicious	Browse	• 66.175.232.221
	Tyre Order 24th February.xlsx	Get hash	malicious	Browse	• 217.160.0.201
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 212.227.17.174
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 212.227.17.184
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 74.208.173.91
	ohLCullPse.exe	Get hash	malicious	Browse	• 66.175.232.221
	e-profile.exe	Get hash	malicious	Browse	• 74.208.88.51
	SecuriteInfo.com.Trojan.Packed2.42850.9624.exe	Get hash	malicious	Browse	• 198.251.65.112
	JUSTF11.exe	Get hash	malicious	Browse	• 213.165.67.118
	Nota de aviso de pago.exe	Get hash	malicious	Browse	• 212.227.15.142
	Drawings.xlsm	Get hash	malicious	Browse	• 74.208.236.5
	SWIFT COMMERCIAL DUTY 0818J.exe	Get hash	malicious	Browse	• 74.208.5.2
	Proforma invoice.xlsx	Get hash	malicious	Browse	• 198.71.50.125
	Purchase Order.exe	Get hash	malicious	Browse	• 198.71.50.125
	Proforma invoice.exe	Get hash	malicious	Browse	• 198.71.50.125
	5i8sLcQqHI.dll	Get hash	malicious	Browse	• 217.160.10 7.189

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\malware.exe.log	
Process:	C:\Users\user\Desktop\malware.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	782
Entropy (8bit):	5.273573871875595
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3AN0U22v:MLF20NaL3z2p29hJ5g522rW2xAi3AP2l
MD5:	F15C9C88F7D7A8FD8C28FD33A19EEDC1
SHA1:	F703E7360D4958CE7BC5362E8AAC8EA150DACE7C
SHA-256:	C32A5354F545CCE575E77A171272F0A9CBD6CD4501AAB657C893A663D3F0E00E
SHA-512:	B3DE9EE4E585FF1C48AE3DFC19A60039D461FCB551F2BF4E22C59A634270E95EFEC240FB1C420DB6F189354B1AAA90D4DC3F85FFD690D70CC4E5CD595FE10 94
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Data\27ab8d047396db374abb803b 446b76f0\System.Data.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.856223289308941
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	malware.exe
File size:	543232
MD5:	2ee5a68ee37af14c612fc4c8a589858a
SHA1:	c27220c28c611908f7cf4e727619aef99decb00b
SHA256:	7e2a3464cd57a807ba4fa1bc0cc9b61fd7ace25fae45a7227bc2184587c9945b
SHA512:	e58676f9df7185bea043d07910fae75bf9ec82a80e2f6f09227c621ed46b3676bb5535c64368ec81ed229f9b7e37f448e8847a24d2b0be8ef88724849a968082
SSDEEP:	12288:RFq90ghy2fQTVHv0jAJEnz4VUIZLO98cx:RSy2foHv0jCEYbjcx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....#.....P..`..... ....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48a00a
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xDA072381 [Thu Nov 29 19:35:29 2085 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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

Instruction
jmp dword ptr [0048A000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x103c4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x640	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8a000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x10000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
7wjw!	0x2000	0xdb84	0xdc00	False	1.00046164773	data	7.99674140744	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x10000	0x75d30	0x75e00	False	0.888632522534	data	7.85224276661	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x640	0x800	False	0.33984375	data	3.51419264617	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x8a000	0x10	0x200	False	0.044921875	data	0.122275881259	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x860a0	0x3b0	data		
RT_MANIFEST	0x86450	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

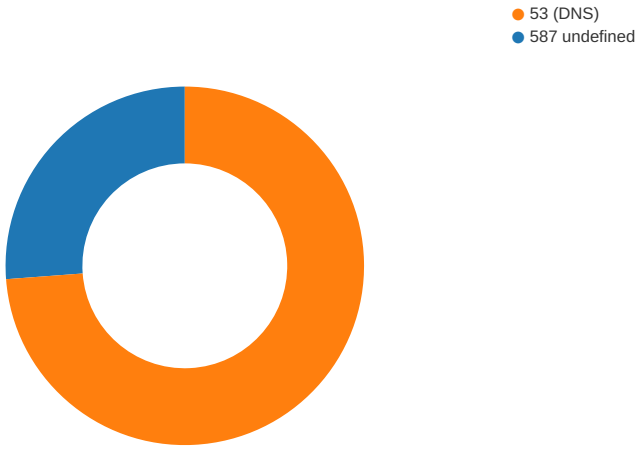
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hotplates 2020-2021
Assembly Version	2.0.9.0
InternalName	NonVersionableAttribute.exe
FileVersion	2.0.9.0
CompanyName	Hotplates
LegalTrademarks	
Comments	MLT
ProductName	Medical Laboratory
ProductVersion	2.0.9.0
FileDescription	Medical Laboratory
OriginalFilename	NonVersionableAttribute.exe

Network Behavior

Network Port Distribution

Total Packets: 42



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 08:59:30.885272026 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:30.930377960 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:30.930645943 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:30.980669022 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:30.981647015 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:31.026617050 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:31.026638985 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:31.026930094 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:31.072876930 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:31.117345095 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:31.168613911 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:31.168642998 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:31.168652058 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:31.168895960 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:31.179493904 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:31.224597931 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:31.264990091 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:31.291666985 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:31.336853981 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:31.336878061 CET	587	49737	213.165.67.118	192.168.2.3
Feb 25, 2021 08:59:31.336990118 CET	49737	587	192.168.2.3	213.165.67.118
Feb 25, 2021 08:59:31.337100983 CET	49737	587	192.168.2.3	213.165.67.118

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 08:57:54.432770967 CET	50200	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:57:54.482414007 CET	53	50200	8.8.8.8	192.168.2.3
Feb 25, 2021 08:57:54.956418991 CET	51281	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:57:55.024233103 CET	53	51281	8.8.8.8	192.168.2.3
Feb 25, 2021 08:57:55.177892923 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:57:55.226635933 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 08:57:55.392517090 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:57:55.444052935 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 08:57:57.056886911 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:57:57.105473042 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 08:57:58.407277107 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:57:58.467240095 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 08:57:59.686897993 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:57:59.735665083 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:02.530145884 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:02.579716921 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:03.326384068 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:03.376665115 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:24.511018038 CET	65110	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 08:58:25.509896994 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:25.562223911 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:26.551956892 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:26.602132082 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:29.230931997 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:29.288131952 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:29.408329010 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:29.461874008 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:30.104022026 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:30.155157089 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:31.018234015 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:31.067037106 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:31.747823000 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:31.809592009 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:31.922199965 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:31.971175909 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:33.155597925 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:33.204462051 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:35.681423903 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:35.734956980 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:36.691859961 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:36.743544102 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:37.720766068 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:37.769865036 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:39.077197075 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:39.125957966 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:39.949260950 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:39.998086929 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:43.294401884 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:43.363955975 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 08:58:51.368130922 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:58:51.438606024 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 08:59:05.859128952 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:59:05.908250093 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 08:59:08.623389959 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:59:08.681668043 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 08:59:30.794899940 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:59:30.857991934 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 08:59:41.252029896 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:59:41.305337906 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 08:59:42.680293083 CET	56132	53	192.168.2.3	8.8.8.8
Feb 25, 2021 08:59:42.754112959 CET	53	56132	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 08:59:30.794899940 CET	192.168.2.3	8.8.8.8	0x4cc6	Standard query (0)	smtp.ionos.es	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 08:59:30.857991934 CET	8.8.8.8	192.168.2.3	0x4cc6	No error (0)	smtp.ionos.es		213.165.67.118	A (IP address)	IN (0x0001)
Feb 25, 2021 08:59:30.857991934 CET	8.8.8.8	192.168.2.3	0x4cc6	No error (0)	smtp.ionos.es		213.165.67.102	A (IP address)	IN (0x0001)

SMTP Packets

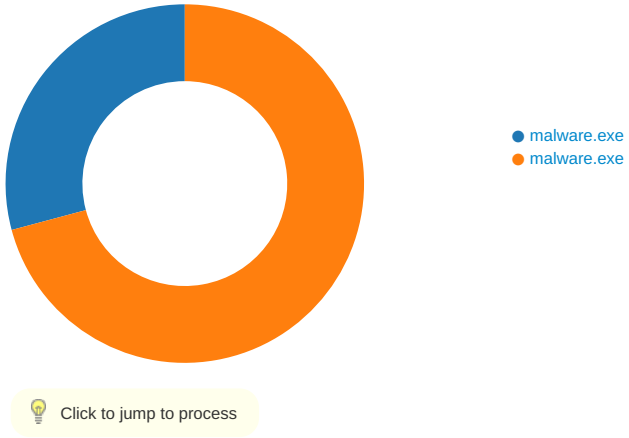
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 08:59:30.980669022 CET	587	49737	213.165.67.118	192.168.2.3	220 kundenserver.de (mreue107) Nemesis ESMTP Service ready
Feb 25, 2021 08:59:30.981647015 CET	49737	587	192.168.2.3	213.165.67.118	EHLO 506407

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 08:59:31.026638985 CET	587	49737	213.165.67.118	192.168.2.3	250-kundenserver.de Hello 506407 [84.17.52.78] 250-8BITMIME 250-AUTH LOGIN PLAIN 250-SIZE 140000000 250 STARTTLS
Feb 25, 2021 08:59:31.026930094 CET	49737	587	192.168.2.3	213.165.67.118	STARTTLS
Feb 25, 2021 08:59:31.072876930 CET	587	49737	213.165.67.118	192.168.2.3	220 OK

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: malware.exe PID: 6380 Parent PID: 5844

General

Start time:	08:57:59
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\malware.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\malware.exe'
Imagebase:	0x930000
File size:	543232 bytes
MD5 hash:	2EE5A68EE37AF14C612FC4C8A589858A
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: 00000000.00000002.201606646.000000000335E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.201927296.00000000040B5000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\malware.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\malware.exe.log	unknown	782	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: malware.exe PID: 6536 Parent PID: 6380

General

Start time:	08:58:01
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\malware.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\malware.exe
Imagebase:	0xef0000
File size:	543232 bytes
MD5 hash:	2EE5A68EE37AF14C612FC4C8A589858A
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: 00000003.00000002.459799944.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.465412261.00000000039D8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.464476473.0000000003531000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.464476473.0000000003531000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6011277	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\523b9955-f3b1-46fe-8a5a-9403c849bf6e	unknown	4096	success or wait	1	6011277	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6011277	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6011277	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6011277	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6011277	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	6011277	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	6011277	ReadFile

Disassembly

Code Analysis