ID: 345017
Sample Name: MT 103.exe
Cookbook: default.jbs
Time: 15:55:34
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

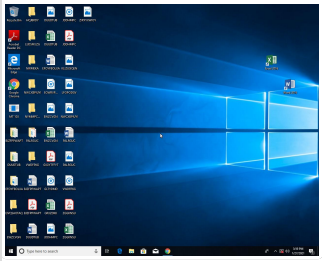
Analysis Report MT 103.exe

Overview

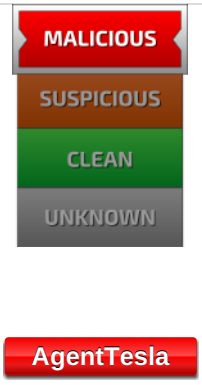
General Information

Sample Name:	MT 103.exe
Analysis ID:	345017
MD5:	4672f4c82e362f8..
SHA1:	870e7f55eeb4caf..
SHA256:	c964743f18f4703..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

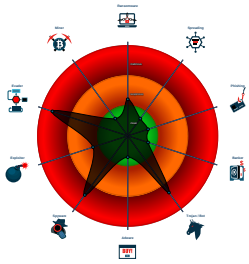


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- MT 103.exe (PID: 6452 cmdline: 'C:\Users\user\Desktop\MT 103.exe' MD5: 4672F4C82E362F8FA602A273B82B2D2C)
  - MT 103.exe (PID: 6524 cmdline: C:\Users\user\Desktop\MT 103.exe MD5: 4672F4C82E362F8FA602A273B82B2D2C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "FDyIk99O",
  "URL: ": "https://RUj6sv9z4cuyCVePS.org",
  "To: ": "shakazoro@vivaldi.net",
  "ByHost: ": "smtp.vivaldi.net:587",
  "Password: ": "1CFmnRUIaFbHY",
  "From: ": "shakazoro@vivaldi.net"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.618421104.0000000002BB1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.618421104.0000000002BB1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.248576551.0000000002F22000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.618540994.0000000002C12000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.616043319.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 7 entries				

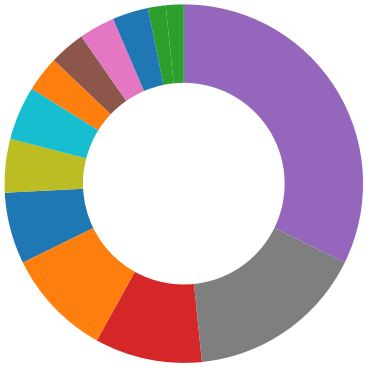
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.MT 103.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM_3

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)

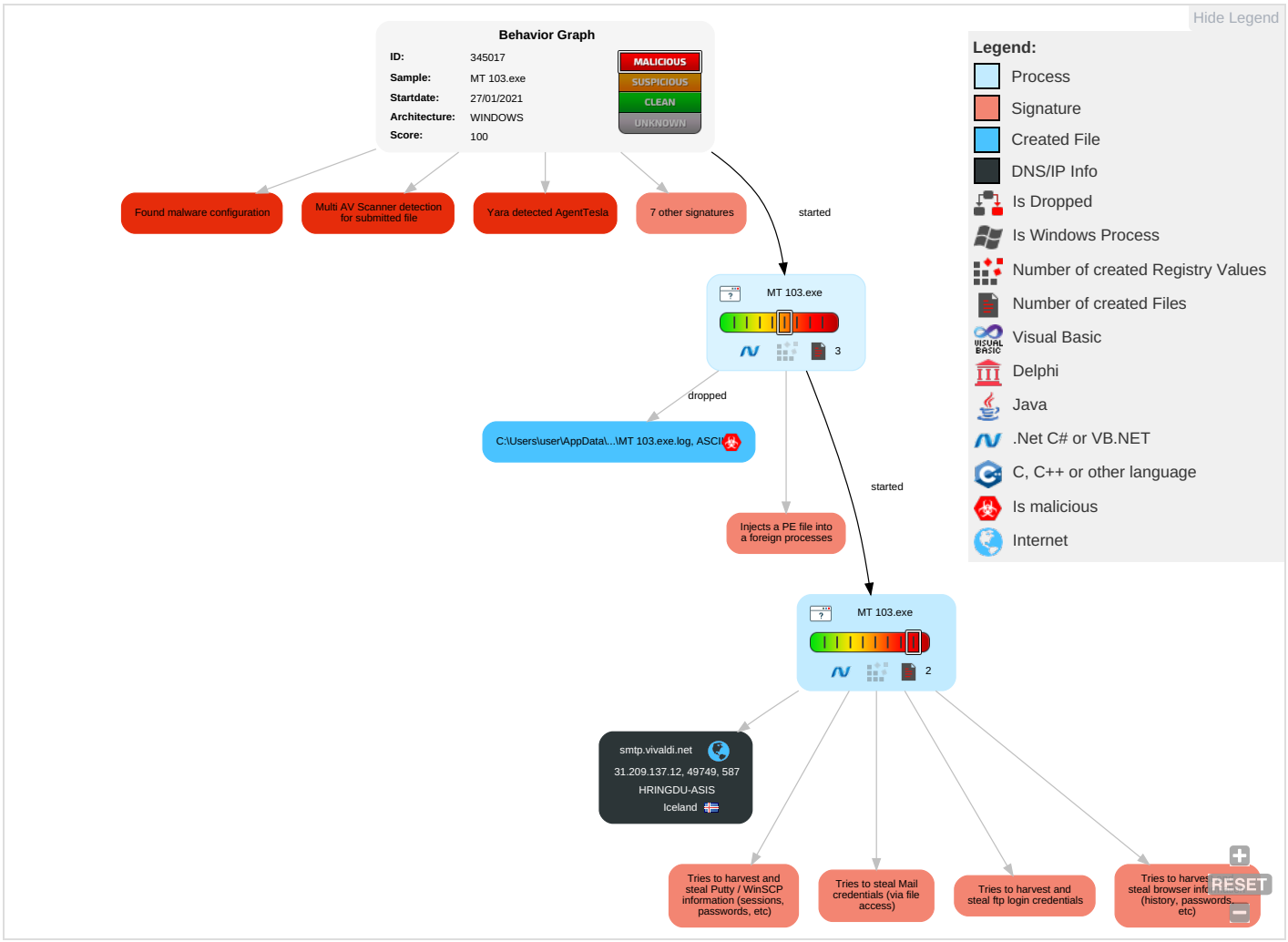
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

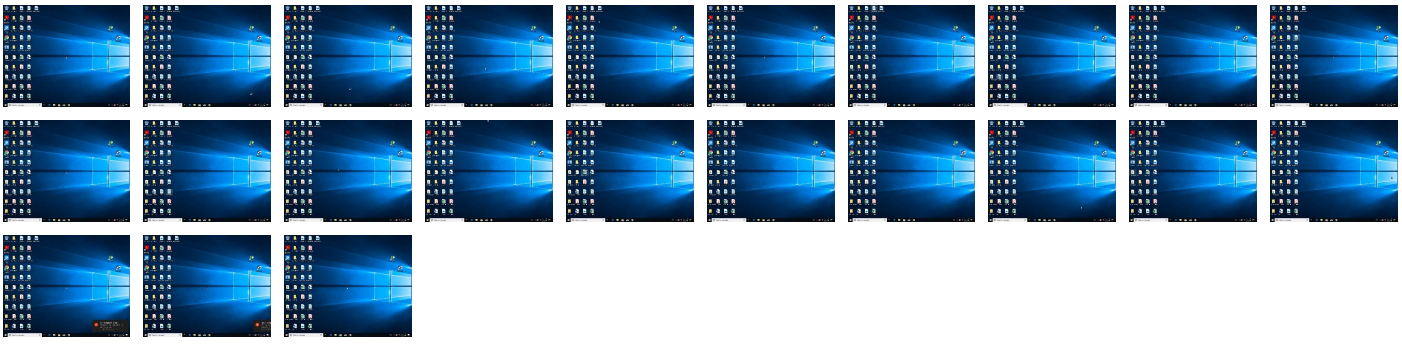
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
MT 103.exe	15%	ReversingLabs	Win32.Trojan.Generic	
MT 103.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.MT 103.exe.400000.0.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	
http://DynDns.comDynDNS	0%	URL Reputation	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://https://RUj6sv9z4cuyCVePS.org	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://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://HGYsjc.com	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://thesnake.herokuapp.com/snakes	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://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://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	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.vivaldi.net	31.209.137.12	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://RUj6sv9z4cuyCVePS.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	MT 103.exe, 00000001.00000002.618421104.0000000002BB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	MT 103.exe, 00000001.00000002.618421104.0000000002BB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	MT 103.exe, 00000001.00000002.617564319.0000000000F87000.00000004.00000020.sdmp	false	• URL Reputation: safe • 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%tordir%%ha	MT 103.exe, 00000001.00000002.618421104.0000000002BB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://HGYsjc.com	MT 103.exe, 00000001.00000002.618421104.0000000002BB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	MT 103.exe, 00000001.00000002.617564319.0000000000F87000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.vivaldi.net	MT 103.exe, 00000001.00000002.618858084.0000000002C72000.00000004.00000001.sdmp	false		high
http://thesnake.herokuapp.com/snakes	MT 103.exe	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	MT 103.exe, 00000000.00000002.248507355.0000000002EF1000.00000004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	MT 103.exe, 00000000.00000002.249712252.0000000003EF9000.00000004.00000001.sdmp, MT 103.exe, 00000001.00000002.616043319.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.root-x1.letsencrypt.org0	MT 103.exe, 00000001.00000002.617564319.0000000000F87000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0	MT 103.exe, 00000001.00000002.617564319.0000000000F87000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.209.137.12	unknown	Iceland		51896	HRINGDU-ASIS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345017
Start date:	27.01.2021
Start time:	15:55:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MT 103.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:	34
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@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • 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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.255.188.83, 104.42.151.234, 23.210.248.85, 51.104.144.132, 95.101.22.216, 95.101.22.224, 95.101.27.142, 95.101.27.163, 8.241.9.254, 8.248.133.254, 8.253.204.249, 8.241.9.126, 67.27.159.126, 51.103.5.159, 52.155.217.156, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • 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
15:56:33	API Interceptor	1131x Sleep call for process: MT 103.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
31.209.137.12	_____.exe	Get hash	malicious	Browse	
	PO-KMML17-01-2021-ATV-image.png.zip.exe	Get hash	malicious	Browse	
	PO-KMML-17-01-2021-ATV-image.png.zip.exe	Get hash	malicious	Browse	
	PO-JAN16-2021.ASW.image.jpeg.eml.png.exe	Get hash	malicious	Browse	
	SwiftRef_INV0880021122020.exe	Get hash	malicious	Browse	
	_____.exe	Get hash	malicious	Browse	
	DINTEC order list.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	30714756.PDF.exe	Get hash	malicious	Browse	
	30714756.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	jK49h2Aa3n.exe	Get hash	malicious	Browse	
	RFQ.01-12-2021.eml.exe	Get hash	malicious	Browse	
	Scan003.pdf.exe	Get hash	malicious	Browse	
	21122020_001.exe	Get hash	malicious	Browse	
	Invoice 277.exe	Get hash	malicious	Browse	
	Shipment Details.Pdf.exe	Get hash	malicious	Browse	
	CIYH2001.pdf.exe	Get hash	malicious	Browse	
	Order Inquiry.Jpeg.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.vivaldi.net	_____.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO-KMML17-01-2021-ATV-image.png.zip.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO-KMML-17-01-2021-ATV-image.png.zip.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO-JAN16-2021.ASW.image.jpeg.eml.png.exe	Get hash	malicious	Browse	• 31.209.137.12
	SwiftRef_INV0880021122020.exe	Get hash	malicious	Browse	• 31.209.137.12
	_____.exe	Get hash	malicious	Browse	• 31.209.137.12
	DINTEC order list.exe	Get hash	malicious	Browse	• 31.209.137.12
	30714756.PDF.exe	Get hash	malicious	Browse	• 31.209.137.12
	30714756.exe	Get hash	malicious	Browse	• 31.209.137.12
	file.exe	Get hash	malicious	Browse	• 31.209.137.12
	file.exe	Get hash	malicious	Browse	• 31.209.137.12
	file.exe	Get hash	malicious	Browse	• 31.209.137.12
	jK49h2Aa3n.exe	Get hash	malicious	Browse	• 31.209.137.12
	RFQ.01-12-2021.eml.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan003.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	21122020_001.exe	Get hash	malicious	Browse	• 31.209.137.12
	Invoice 277.exe	Get hash	malicious	Browse	• 31.209.137.12
	Shipment Details.Pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	CIYH2001.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	Order Inquiry.Jpeg.exe	Get hash	malicious	Browse	• 31.209.137.12

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HRINGDU-ASIS	Vivaldi.3.5.2115.87.x64.exe	Get hash	malicious	Browse	• 31.209.137.5
	_____.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO-KMML17-01-2021-ATV-image.png.zip.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO-KMML-17-01-2021-ATV-image.png.zip.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO-JAN16-2021.ASW.image.jpeg.eml.png.exe	Get hash	malicious	Browse	• 31.209.137.12
	SwiftRef_INV0880021122020.exe	Get hash	malicious	Browse	• 31.209.137.12
	_____.exe	Get hash	malicious	Browse	• 31.209.137.12
	DINTEC order list.exe	Get hash	malicious	Browse	• 31.209.137.12
	30714756.PDF.exe	Get hash	malicious	Browse	• 31.209.137.12
	30714756.exe	Get hash	malicious	Browse	• 31.209.137.12
	file.exe	Get hash	malicious	Browse	• 31.209.137.12
	file.exe	Get hash	malicious	Browse	• 31.209.137.12
	file.exe	Get hash	malicious	Browse	• 31.209.137.12
	jK49h2Aa3n.exe	Get hash	malicious	Browse	• 31.209.137.12
	RFQ.01-12-2021.eml.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan003.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	21122020_001.exe	Get hash	malicious	Browse	• 31.209.137.12
	Invoice 277.exe	Get hash	malicious	Browse	• 31.209.137.12
	Shipment Details.Pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	CIYH2001.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MT 103.exe.log	
Process:	C:\Users\user\Desktop\MT 103.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.569888038395144
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • 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% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	MT 103.exe
File size:	630272
MD5:	4672f4c82e362f8fa602a273b82b2d2c
SHA1:	870e7f55eeb4caf63422e8260e25bbda34cbb4d5
SHA256:	c964743f18f47032f7b0cbfa7467b310927bb44813bd7861d4c85d55d6f34590
SHA512:	14444e0a52543742f683b0f139d6a1fbbafdbc301275383ffe8b2976e16a0ecf6be25db58e331fac20685de991e40b8dca59eb04ca859b6fbdfc3b6fcb8e0f18
SSDEEP:	12288:UlrkyMXW2j4eRtpfQC2fvNvHjJGa1UlxzEXIG9DRYn:UlwjAvFH8xbQXLYn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Lq.`.....P.....V.... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x49b356
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:	0x6011714C [Wed Jan 27 13:57:32 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

Instruction
jmp dword ptr [00402000h]
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
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	0x9b304	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9c000	0x5dc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9e000	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	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9935c	0x99400	False	0.790695414458	data	7.5797406422	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x5dc	0x600	False	0.427734375	data	4.15501859449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x9c090	0x34c	data		
RT_MANIFEST	0x9c3ec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

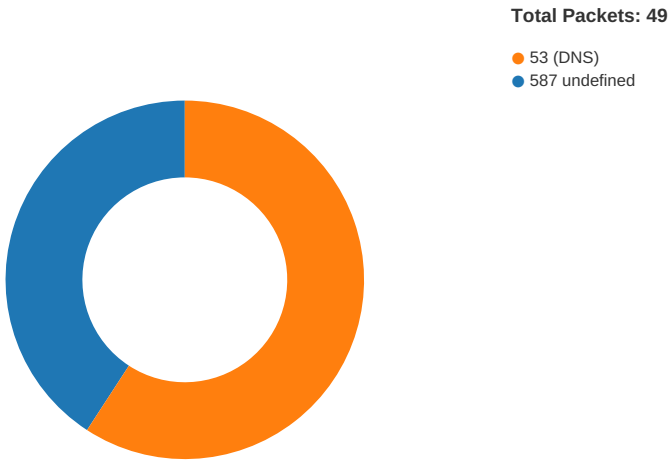
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	RestrictedErrorObject.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Revision
ProductVersion	1.0.0.0
FileDescription	Revision
OriginalFilename	RestrictedErrorObject.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:58:07.079046965 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:07.161716938 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:07.161848068 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:07.642831087 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:07.643309116 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:07.727960110 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:07.728022099 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:07.728478909 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:07.814469099 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:07.861269951 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:07.870682955 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:07.955635071 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:07.955660105 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:07.955668926 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:07.955841064 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:07.962594032 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.047523022 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.095602036 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.132920980 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.215461016 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.217914104 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.303095102 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.304089069 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.428047895 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.489077091 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.490253925 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.577325106 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.580863953 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.581585884 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.701534986 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.702164888 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.786614895 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.792118073 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.792442083 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.793147087 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.793267965 CET	49749	587	192.168.2.5	31.209.137.12
Jan 27, 2021 15:58:08.875999928 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.876442909 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.876451969 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.892770052 CET	587	49749	31.209.137.12	192.168.2.5
Jan 27, 2021 15:58:08.939368963 CET	49749	587	192.168.2.5	31.209.137.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:56:26.373944998 CET	65296	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:56:26.424725056 CET	53	65296	8.8.8.8	192.168.2.5
Jan 27, 2021 15:56:27.420595884 CET	63183	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:56:27.468648911 CET	53	63183	8.8.8.8	192.168.2.5
Jan 27, 2021 15:56:29.202940941 CET	60151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:56:29.250948906 CET	53	60151	8.8.8.8	192.168.2.5
Jan 27, 2021 15:56:31.049668074 CET	56969	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:56:31.097757101 CET	53	56969	8.8.8.8	192.168.2.5
Jan 27, 2021 15:56:31.867089987 CET	55161	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:56:31.920504093 CET	53	55161	8.8.8.8	192.168.2.5
Jan 27, 2021 15:56:33.100469112 CET	54757	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:56:33.156724930 CET	53	54757	8.8.8.8	192.168.2.5
Jan 27, 2021 15:56:42.751538992 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:56:42.812489033 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2021 15:56:55.667288065 CET	60075	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:56:55.717937946 CET	53	60075	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:00.229284048 CET	55016	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:00.287761927 CET	53	55016	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:14.984648943 CET	64345	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:15.042973042 CET	53	64345	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:15.141880035 CET	57128	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:15.189727068 CET	53	57128	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:15.434649944 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:15.516995907 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:17.759613037 CET	50463	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:17.810312986 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:20.427763939 CET	50394	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:20.485363960 CET	53	50394	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:28.116421938 CET	58530	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:28.175647974 CET	53	58530	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:43.850028038 CET	53813	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:43.912199974 CET	53	53813	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:45.455710888 CET	63732	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:45.513135910 CET	53	63732	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:46.172065973 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:46.231161118 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:46.699399948 CET	54450	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:46.767466068 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:46.896500111 CET	59261	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:46.957297087 CET	53	59261	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:47.245702028 CET	57151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:47.346760988 CET	53	57151	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:48.303390980 CET	59413	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:48.361988068 CET	53	59413	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:49.355200052 CET	60516	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:49.411828995 CET	53	60516	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:51.138535023 CET	51649	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:51.196787119 CET	53	51649	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:52.242624998 CET	65086	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:52.299139023 CET	53	65086	8.8.8.8	192.168.2.5
Jan 27, 2021 15:57:54.782999992 CET	56432	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:57:54.830873966 CET	53	56432	8.8.8.8	192.168.2.5
Jan 27, 2021 15:58:01.879125118 CET	52929	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:58:01.929246902 CET	53	52929	8.8.8.8	192.168.2.5
Jan 27, 2021 15:58:03.784403086 CET	64317	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:58:03.864379883 CET	53	64317	8.8.8.8	192.168.2.5
Jan 27, 2021 15:58:07.000411987 CET	61004	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:58:07.060689926 CET	53	61004	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:58:07.000411987 CET	192.168.2.5	8.8.8.8	0xde90	Standard query (0)	smtp.vivaldi.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:58:07.060689926 CET	8.8.8.8	192.168.2.5	0xde90	No error (0)	smtp.vivaldi.net		31.209.137.12	A (IP address)	IN (0x0001)

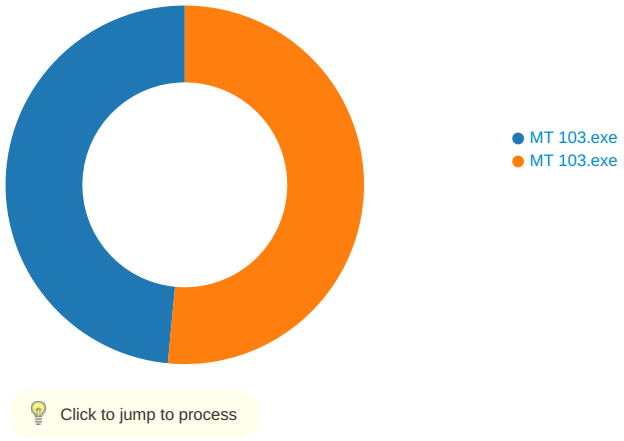
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:58:07.642831087 CET	587	49749	31.209.137.12	192.168.2.5	220 smtp.vivaldi.net ESMTP Postfix (Ubuntu)
Jan 27, 2021 15:58:07.643309116 CET	49749	587	192.168.2.5	31.209.137.12	EHLO 992547
Jan 27, 2021 15:58:07.728022099 CET	587	49749	31.209.137.12	192.168.2.5	250-smtp.vivaldi.net 250-PIPELINING 250-SIZE 36700160 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 SMTPUTF8
Jan 27, 2021 15:58:07.728478909 CET	49749	587	192.168.2.5	31.209.137.12	STARTTLS
Jan 27, 2021 15:58:07.814469099 CET	587	49749	31.209.137.12	192.168.2.5	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: MT 103.exe PID: 6452 Parent PID: 5672

General

Start time:	15:56:31
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\MT 103.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\MT 103.exe'
Imagebase:	0xa70000
File size:	630272 bytes
MD5 hash:	4672F4C82E362F8FA602A273B82B2D2C
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: 00000000.00000002.248576551.0000000002F22000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.248507355.0000000002EF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.249712252.0000000003EF9000.00000004.00000001.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	6DA5CF06	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	6DA5CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MT 103.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD6C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MT 103.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	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.	success or wait	1	6DD6C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8A1B4F	ReadFile

Analysis Process: MT 103.exe PID: 6524 Parent PID: 6452

General

Start time:	15:56:33
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\MT 103.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\MT 103.exe
Imagebase:	0x8e0000
File size:	630272 bytes
MD5 hash:	4672F4C82E362F8FA602A273B82B2D2C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.618421104.0000000002BB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.618421104.0000000002BB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.618540994.0000000002C12000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.616043319.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.618470302.0000000002BE5000.00000004.00000001.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	6DA5CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DA5CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8A1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C8A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C8A1B4F	ReadFile

Disassembly

Code Analysis