ID: 339258
Sample Name: file
Cookbook: default.jbs
Time: 18:55:21
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

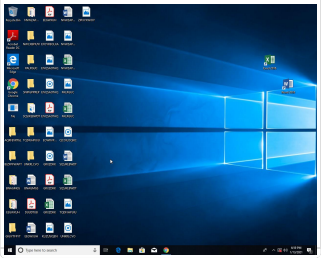
Analysis Report file

Overview

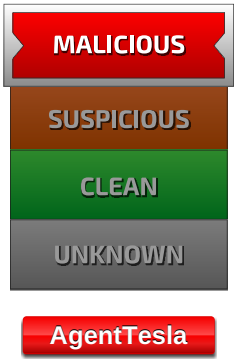
General Information

Sample Name:	file (renamed file extension from none to exe)
Analysis ID:	339258
MD5:	4014c919c4f26d8..
SHA1:	88a96eca367759..
SHA256:	7b2e9f16b557d19.
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

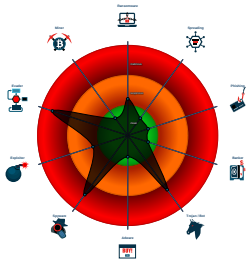


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- Binary contains a suspicious time st…
- 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…
- Tries to harvest and steal ftp login c…

Classification



Startup

- **System is w10x64**
- file.exe (PID: 1748 cmdline: 'C:\Users\user\Desktop\file.exe' MD5: 4014C919C4F26D8B5E72B255CFFEE0AB)
  - file.exe (PID: 4388 cmdline: {path} MD5: 4014C919C4F26D8B5E72B255CFFEE0AB)
  - file.exe (PID: 3336 cmdline: {path} MD5: 4014C919C4F26D8B5E72B255CFFEE0AB)
  - file.exe (PID: 2964 cmdline: {path} MD5: 4014C919C4F26D8B5E72B255CFFEE0AB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

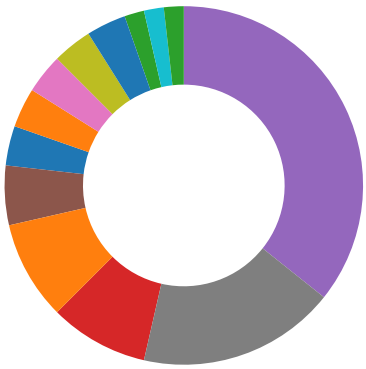
Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.239658084.000000000425 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.238874071.000000000325 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: file.exe PID: 1748	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: file.exe PID: 1748	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	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:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Data Obfuscation:

.NET source code contains potential unpacker

Binary contains a suspicious time stamp

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)

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)

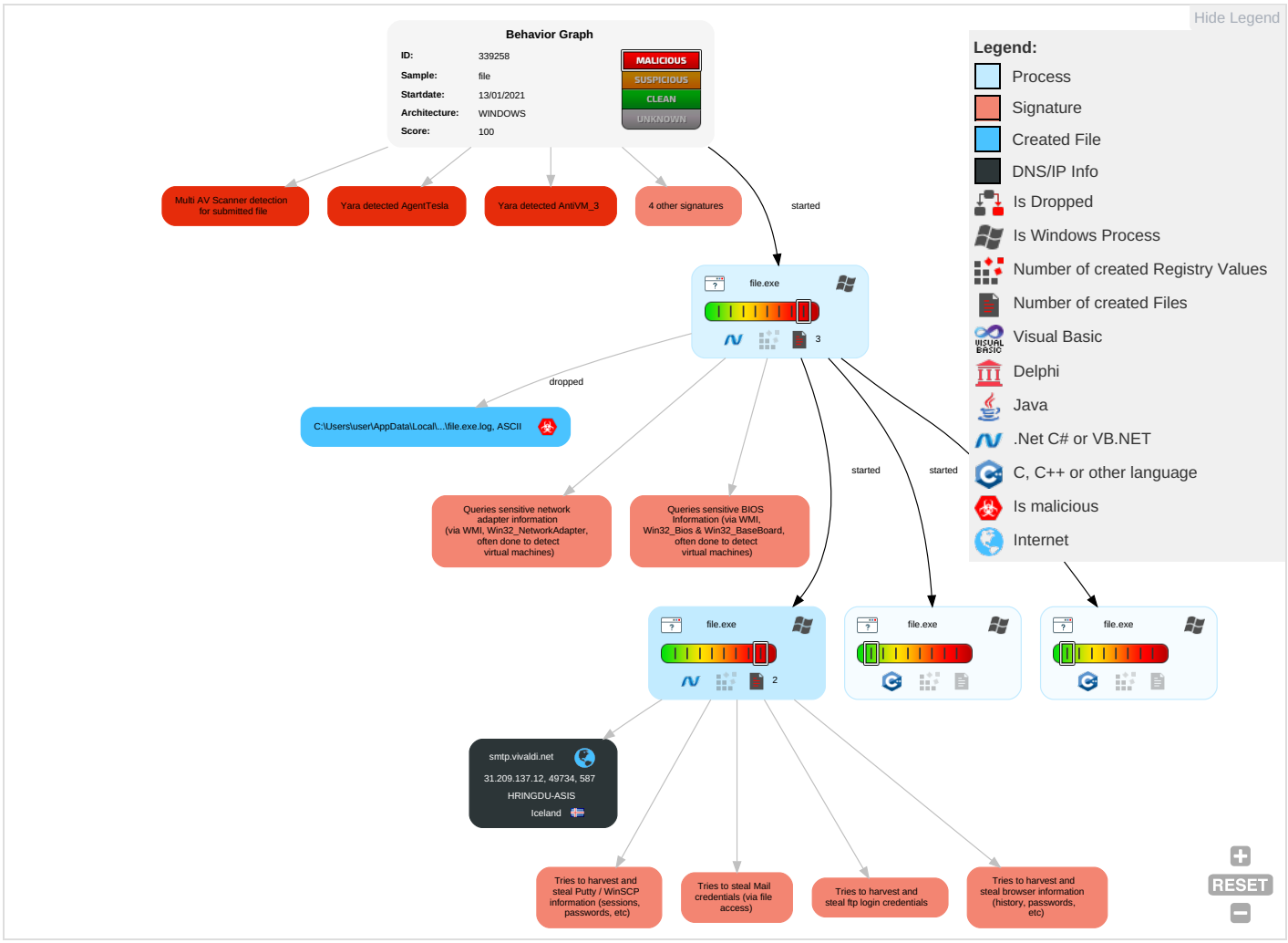
Remote Access Functionality:

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	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E Ir N C
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	Exfiltration Over Bluetooth	Non-Standard Port 1	E R C
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-Application Layer Protocol 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 1	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A

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
file.exe	48%	ReversingLabs	Win32.Trojan.Woreflint	
file.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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://TNxeq3XdBc59HHjc.org1-5-21-3853321935-2125563209-4053062332-1002_Classes	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	file.exe, 00000001.00000002.239658084.0000000004259000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://TNxeq3XdBc59HHjc.org1-5-21-3853321935-2125563209-4053062332-1002_Classes	file.exe, 00000004.00000003.442698435.0000000000EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

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 Red Diamond
Analysis ID:	339258
Start date:	13.01.2021
Start time:	18:55:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/1@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.1% (good quality ratio 0.8%) • Quality average: 62.5% • Quality standard deviation: 41%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 23.210.248.85, 51.104.139.180, 92.122.213.194, 92.122.213.247, 20.54.26.129, 51.103.5.159, 51.104.144.132, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.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, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, 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 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/339258/sample/file.exe

Simulations

Behavior and APIs

Time	Type	Description
18:56:12	API Interceptor	1141x Sleep call for process: file.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
31.209.137.12	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	
	image001.exe	Get hash	malicious	Browse	
	Quote-20201203-0076.exe	Get hash	malicious	Browse	
	Project quotation list.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	L4z6CoqR4E.exe	Get hash	malicious	Browse	
	Scan 0027511202054.xlsx	Get hash	malicious	Browse	
	Scan002519332020.exe	Get hash	malicious	Browse	
	PI-08351.xlsx	Get hash	malicious	Browse	
	Benz.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	
	Swift298321.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.vivaldi.net	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
	image001.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quote-20201203-0076.exe	Get hash	malicious	Browse	• 31.209.137.12
	Project quotation list.exe	Get hash	malicious	Browse	• 31.209.137.12
	L4z6CoqR4E.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 0027511202054.xlsx	Get hash	malicious	Browse	• 31.209.137.12
	Scan002519332020.exe	Get hash	malicious	Browse	• 31.209.137.12
	PI-08351.xlsx	Get hash	malicious	Browse	• 31.209.137.12
	Benz.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift298321.exe	Get hash	malicious	Browse	• 31.209.137.12

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HRINGDU-ASIS	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
	image001.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quote-20201203-0076.exe	Get hash	malicious	Browse	• 31.209.137.12
	Project quotation list.exe	Get hash	malicious	Browse	• 31.209.137.12
	L4z6CoqR4E.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 0027511202054.xlsx	Get hash	malicious	Browse	• 31.209.137.12
	Scan002519332020.exe	Get hash	malicious	Browse	• 31.209.137.12
	PI-08351.xlsx	Get hash	malicious	Browse	• 31.209.137.12
	Benz.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift298321.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\file.exe.log	
Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.883442204183753
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:	file.exe
File size:	636928
MD5:	4014c919c4f26d8b5e72b255cffee0ab
SHA1:	88a96eca36775921b5244f206ad461e761bc7a4a
SHA256:	7b2e9f16b557d194f079e970dac923105073eb2aed4b639 60c05d5c4bb816184
SHA512:	48b1961ff9a2aaf68c37a2c4c72b20a51e0bb12f202a185 d4cc8ddf0c175637e4e5c693daca8417af6d2c93860d46a 83997774ae2e6318057ec9cd29f7b447b7
SSDEEP:	12288:rKYV9NiqZSVZN0wi/LTz8q/JoulRXYmT0TYLE:ZV9AqZ2ywivI0JoUhYmTE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....|.....0.....^.... .....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49cc5e

General

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:	0xC0B97CD9 [Fri Jun 17 09:33:13 2072 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9cc0c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9e000	0x5d4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa0000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x9cbf0	0x1c	.text
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	0x9ac64	0x9ae00	False	0.918406981437	data	7.8915177109	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9e000	0x5d4	0x600	False	0.427734375	data	4.15163496674	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa0000	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	0x9e090	0x344	data		
RT_MANIFEST	0x9e3e4	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 2019
Assembly Version	1.0.0.0
InternalName	n.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	MultiUserParentalControl
ProductVersion	1.0.0.0
FileDescription	MultiUserParentalControl
OriginalFilename	n.exe

Network Behavior

Network Port Distribution

Total Packets: 48

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 18:57:56.224176884 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:56.310677052 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:56.311003923 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:56.805943966 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:56.807125092 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:56.893294096 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:56.893366098 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:56.893961906 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:56.980767965 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.021300077 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:57.055424929 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:57.144740105 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.144901037 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.144962072 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.145082951 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:57.154726028 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:57.241655111 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.286962032 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:57.507659912 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:57.594647884 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.596720934 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:57.685456991 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.686661005 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:57.814996958 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.860768080 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.861700058 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:57.947978020 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.949260950 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:57.949758053 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:58.068697929 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:58.069173098 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:58.160855055 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:58.163665056 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:58.163866997 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:58.164338112 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:58.164449930 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:57:58.252366066 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:58.252397060 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:58.252404928 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:58.270442963 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:57:58.318633080 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:59:35.816016912 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:59:35.903565884 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:59:35.908802032 CET	49734	587	192.168.2.5	31.209.137.12

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 18:59:35.995928049 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:59:35.996154070 CET	587	49734	31.209.137.12	192.168.2.5
Jan 13, 2021 18:59:35.996279001 CET	49734	587	192.168.2.5	31.209.137.12
Jan 13, 2021 18:59:35.997035980 CET	49734	587	192.168.2.5	31.209.137.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 18:56:06.375739098 CET	60151	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:06.432495117 CET	53	60151	8.8.8.8	192.168.2.5
Jan 13, 2021 18:56:07.186747074 CET	56969	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:07.235227108 CET	53	56969	8.8.8.8	192.168.2.5
Jan 13, 2021 18:56:08.063805103 CET	55161	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:08.115190029 CET	53	55161	8.8.8.8	192.168.2.5
Jan 13, 2021 18:56:08.952631950 CET	54757	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:09.000559092 CET	53	54757	8.8.8.8	192.168.2.5
Jan 13, 2021 18:56:29.261269093 CET	49992	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:29.321979046 CET	53	49992	8.8.8.8	192.168.2.5
Jan 13, 2021 18:56:34.638742924 CET	60075	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:34.689512968 CET	53	60075	8.8.8.8	192.168.2.5
Jan 13, 2021 18:56:39.920598030 CET	55016	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:39.980798960 CET	53	55016	8.8.8.8	192.168.2.5
Jan 13, 2021 18:56:52.762825012 CET	64345	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:52.827168941 CET	53	64345	8.8.8.8	192.168.2.5
Jan 13, 2021 18:56:55.365467072 CET	57128	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:55.446609974 CET	53	57128	8.8.8.8	192.168.2.5
Jan 13, 2021 18:56:58.713556051 CET	54791	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:56:58.771142960 CET	53	54791	8.8.8.8	192.168.2.5
Jan 13, 2021 18:57:33.131481886 CET	50463	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:57:33.182451010 CET	53	50463	8.8.8.8	192.168.2.5
Jan 13, 2021 18:57:56.037352085 CET	50394	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:57:56.111146927 CET	53	50394	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:00.513489962 CET	58530	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:00.564424992 CET	53	58530	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:00.979659081 CET	53813	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:01.048316002 CET	53	53813	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:45.417656898 CET	63732	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:45.513396978 CET	53	63732	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:46.186269045 CET	57344	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:46.247777939 CET	53	57344	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:46.998650074 CET	54450	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:47.059990883 CET	53	54450	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:47.666222095 CET	59261	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:47.725531101 CET	53	59261	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:48.302527905 CET	57151	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:48.359021902 CET	53	57151	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:49.499062061 CET	59413	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:49.555541992 CET	53	59413	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:50.700992107 CET	60516	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:50.757522106 CET	53	60516	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:52.413744926 CET	51649	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:52.461869955 CET	53	51649	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:53.522161007 CET	65086	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:53.578886032 CET	53	65086	8.8.8.8	192.168.2.5
Jan 13, 2021 18:58:54.084847927 CET	56432	53	192.168.2.5	8.8.8.8
Jan 13, 2021 18:58:54.141771078 CET	53	56432	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 18:57:56.037352085 CET	192.168.2.5	8.8.8.8	0x738a	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 13, 2021 18:57:56.111146927 CET	8.8.8.8	192.168.2.5	0x738a	No error (0)	smtp.vivaldi.net		31.209.137.12	A (IP address)	IN (0x0001)

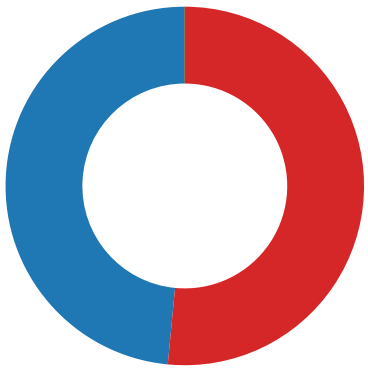
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 18:57:56.805943966 CET	587	49734	31.209.137.12	192.168.2.5	220 smtp.vivaldi.net ESMTP Postfix (Ubuntu)
Jan 13, 2021 18:57:56.807125092 CET	49734	587	192.168.2.5	31.209.137.12	EHLO 960781
Jan 13, 2021 18:57:56.893366098 CET	587	49734	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 13, 2021 18:57:56.893961906 CET	49734	587	192.168.2.5	31.209.137.12	STARTTLS
Jan 13, 2021 18:57:56.980767965 CET	587	49734	31.209.137.12	192.168.2.5	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 1748 Parent PID: 5632

General

Start time:	18:56:11
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\file.exe'
Imagebase:	0xed0000

File size:	636928 bytes
MD5 hash:	4014C919C4F26D8B5E72B255CFFEE0AB
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: 00000001.00000002.239658084.0000000004259000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.238874071.0000000003251000.00000004.00000001.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	6DABCF06	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	6DABCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDCC78D	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\file.exe.log	unknown	1216	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 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 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 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 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6DDCC907	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Analysis Process: file.exe PID: 4388 Parent PID: 1748

General

Start time:	18:56:14
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1d0000
File size:	636928 bytes
MD5 hash:	4014C919C4F26D8B5E72B255CFFEE0AB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: file.exe PID: 3336 Parent PID: 1748

General

Start time:	18:56:14
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x190000
File size:	636928 bytes
MD5 hash:	4014C919C4F26D8B5E72B255CFFEE0AB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: file.exe PID: 2964 Parent PID: 1748

General

Start time:	18:56:15
Start date:	13/01/2021

Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x890000
File size:	636928 bytes
MD5 hash:	4014C919C4F26D8B5E72B255CFFEE0AB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6DABCF06	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	6DABCF06	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C901B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C901B4F	ReadFile

Disassembly

Code Analysis