ID: 344833
Sample Name: Invoice-3990993.exe
Cookbook: default.jbs
Time: 08:29:13
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

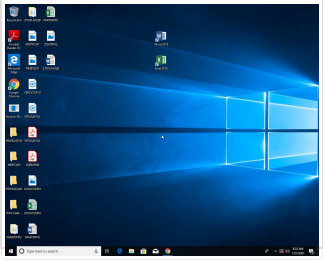
Analysis Report Invoice-3990993.exe

Overview

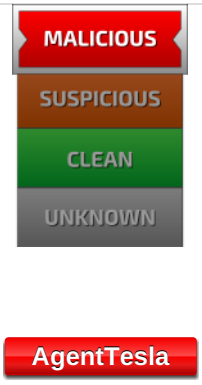
General Information

Sample Name:	Invoice-3990993.exe
Analysis ID:	344833
MD5:	c240ecb4d6da45..
SHA1:	de229f907f93f89…
SHA256:	4730211b41726d..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



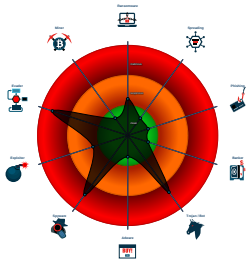
AgentTesla

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…
- Initial sample is a PE file and has a …
- 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…

Classification



Startup

- **System is w10x64**
- Invoice-3990993.exe (PID: 4556 cmdline: 'C:\Users\user\Desktop\Invoice-3990993.exe' MD5: C240ECB4D6DA455111DCA9256DCD3604)
  - Invoice-3990993.exe (PID: 6228 cmdline: C:\Users\user\Desktop\Invoice-3990993.exe MD5: C240ECB4D6DA455111DCA9256DCD3604)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "2hoa0Zb0I7ot",
  "URL: ": "https://K2J5CnzUCIra4sFQC.org",
  "To: ": "chuksanderson@hybridgroupco.com",
  "ByHost: ": "mail.hybridgroupco.com:587",
  "Password: ": "7ynpV9cGEL",
  "From: ": "chuksanderson@hybridgroupco.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.588090737.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.230286237.000000000452000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.230847336.000000000429000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.591701413.00000000032C1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.230261930.000000000421000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

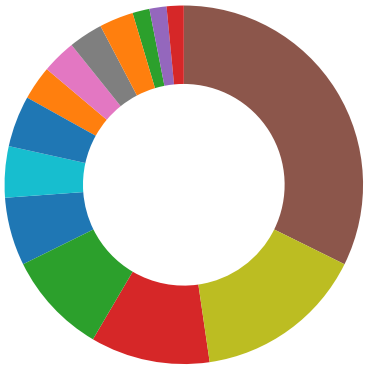
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Invoice-3990993.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
- 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:

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

Initial sample is a PE file and has a suspicious name

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)

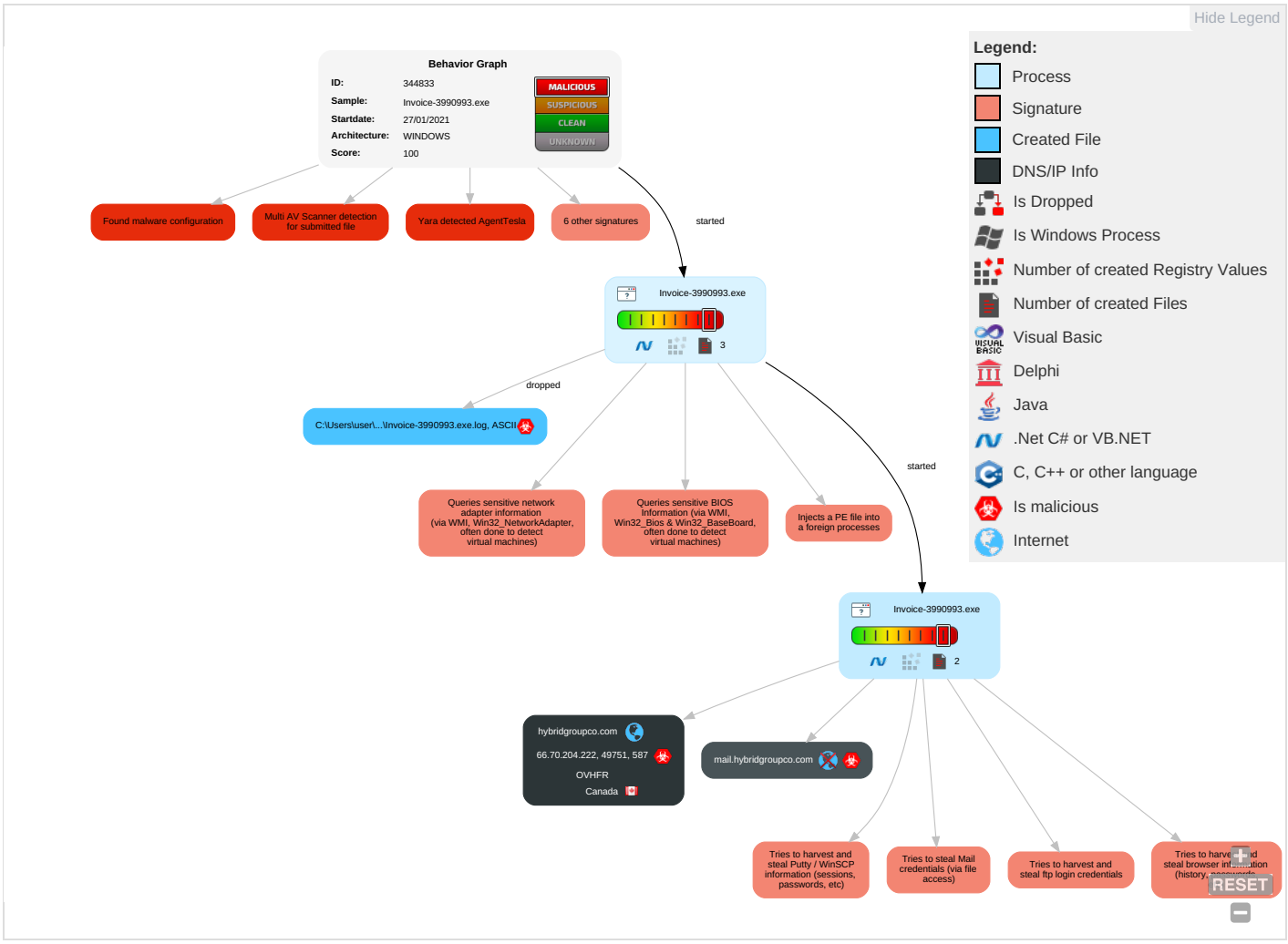
Remote Access Functionality:

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	Input Capture 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Archive Collected Data 1 1	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	Data from Local System 2	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
Invoice-3990993.exe	53%	Virustotal		Browse
Invoice-3990993.exe	50%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Invoice-3990993.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.Invoice-3990993.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
hybridgroupco.com	0%	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://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://hybridgroupco.com	0%	Avira URL Cloud	safe	
http://mail.hybridgroupco.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://https://K2J5CnzUCIra4sFQC.org	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://NvVyeo.com	0%	Avira URL Cloud	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://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	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
hybridgroupco.com	66.70.204.222	true	true	• 0%, Virustotal, Browse	unknown
mail.hybridgroupco.com	unknown	unknown	true		unknown

Contacted URLs

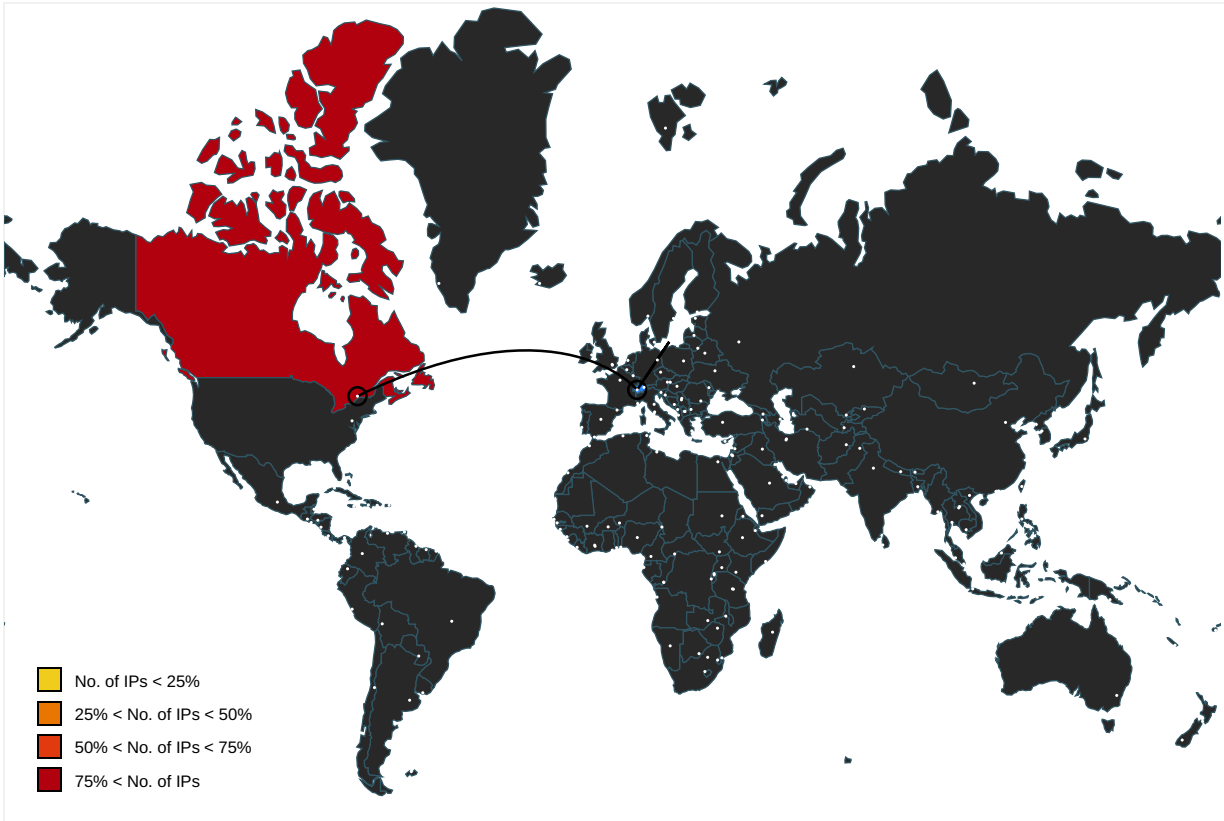
Name	Malicious	Antivirus Detection	Reputation
http://https://K2J5CnzUCIra4sFQC.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Invoice-3990993.exe, 00000002.00000002.591701413.00000000032C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	Invoice-3990993.exe, 00000002.00000002.591701413.00000000032C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	Invoice-3990993.exe, 00000002.00000002.594011651.00000000356F000.00000004.00000001.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%tordir%%ha	Invoice-3990993.exe, 00000002.00000002.591701413.00000000032C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot%telegramapi%/	Invoice-3990993.exe, 00000000.00000002.230847336.0000000003429000.00000004.00000001.sdmp, Invoice-3990993.exe, 00000002.00000002.588090737.0000000000402000.00000040.00000001.sdmp	false		high
http://hybridgroupco.com	Invoice-3990993.exe, 00000002.00000002.594011651.000000000356F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.hybridgroupco.com	Invoice-3990993.exe, 00000002.00000002.594011651.000000000356F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	Invoice-3990993.exe, 00000002.00000002.594011651.000000000356F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Invoice-3990993.exe, 00000000.00000002.230261930.0000000002421000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	Invoice-3990993.exe, 00000002.00000002.591701413.000000000032C1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Invoice-3990993.exe, 00000000.00000002.230847336.0000000003429000.00000004.00000001.sdmp, Invoice-3990993.exe, 00000002.00000002.588090737.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://NvVyeo.com	Invoice-3990993.exe, 00000002.00000002.591701413.000000000032C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	Invoice-3990993.exe, 00000002.00000002.594011651.000000000356F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	Invoice-3990993.exe, 00000002.00000002.591701413.000000000032C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0	Invoice-3990993.exe, 00000002.00000002.594011651.000000000356F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.70.204.222	unknown	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344833
Start date:	27.01.2021
Start time:	08:29:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice-3990993.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@2/1
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, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 13.64.90.137, 52.255.188.83, 92.122.144.200, 168.61.161.212, 51.104.139.180, 52.155.217.156, 20.54.26.129, 51.103.5.159, 67.26.81.254, 8.248.131.254, 8.241.121.254, 67.26.73.254, 67.27.159.126, 95.101.22.224, 95.101.22.216 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.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, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus15.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
08:30:02	API Interceptor	1057x Sleep call for process: Invoice-3990993.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.70.204.222	PARTS REQUEST SO_30005141.exe	Get hash	malicious	Browse	
	Yu2iMnAJBdOGPyv.exe	Get hash	malicious	Browse	
	CONTRACT AGREEMENT.exe	Get hash	malicious	Browse	
	PARTS REQUEST SO_30005141.exe	Get hash	malicious	Browse	
	PARTS REQUEST SO_30005141.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	SWIFT_6979034.exe	Get hash	malicious	Browse	
	P-O.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PAYMENT COPY.exe	Get hash	malicious	Browse	
	INV # 16809 & 16769.exe	Get hash	malicious	Browse	
	S.O.A.exe	Get hash	malicious	Browse	
	PROFORMAR INVOICE DETAILS.exe	Get hash	malicious	Browse	
	U-8913.exe	Get hash	malicious	Browse	
	ORDB2002765.exe	Get hash	malicious	Browse	
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	
	Proforma Invoice with Bank Details_pdf.exe	Get hash	malicious	Browse	
	Image001.exe	Get hash	malicious	Browse	
	4nfg3g3nwg.exe	Get hash	malicious	Browse	
	DOC04121993.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	ra8tqy1c.rar.dll	Get hash	malicious	Browse	• 158.69.118.130
	ARCH_25_012021.doc	Get hash	malicious	Browse	• 51.255.203.164
	WUHU95Apq3	Get hash	malicious	Browse	• 46.105.5.118
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.Generic.mg.59d4c719403b7938.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.Generic.mg.9d9c1d19818e75cc.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 158.69.118.130
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 158.69.118.130
	roboforex4multisetup.exe	Get hash	malicious	Browse	• 139.99.148.202
	xDKOaCQQTQ.dll	Get hash	malicious	Browse	• 158.69.118.130
	4bEUfowOcg.dll	Get hash	malicious	Browse	• 158.69.118.130
	P_O INV 01262021.exe	Get hash	malicious	Browse	• 51.195.53.221
	DHL doc.exe	Get hash	malicious	Browse	• 51.195.53.221
	PL5CS6pwNitND2n.exe	Get hash	malicious	Browse	• 51.75.130.83
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 51.255.203.164
	PARTS REQUEST SO_30005141.exe	Get hash	malicious	Browse	• 66.70.204.222
	Document_PDF.exe	Get hash	malicious	Browse	• 51.195.53.221
	SecuriteInfo.com.Variant.Zusy.363976.21086.exe	Get hash	malicious	Browse	• 54.39.198.228
	ARCH 05 2_80074.doc	Get hash	malicious	Browse	• 144.217.19 0.240
	PO NO 214000070.doc	Get hash	malicious	Browse	• 94.23.169.237

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice-3990993.exe.log

Process:	C:\Users\user\Desktop\Invoice-3990993.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice-3990993.exe.log	
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):	7.680106020831519
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:	Invoice-3990993.exe
File size:	595968
MD5:	c240ecb4d6da455111dca9256dcd3604
SHA1:	de229f907f93f89d5fe10828fa7e8034e70cda55
SHA256:	4730211b41726d261fe9f81bbbacd224b2659f9f05909395f8492adf187d8666
SHA512:	28ff87cdbc0d40702122818592a197e92d637947b7591c785d34c7b37175061206683dc3ff57918a50de021841bf33d1aba13275f2fc4337b6c19e4c19adaacf
SSDEEP:	12288:2VKLNoOoLnxjNmtpca8JFn/BThD/2hAcz2UPmnRST0:2VKKOonxjYpY5/2hAU2lRS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-..`.....P.....N-... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x492d4e
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:	0x6010092D [Tue Jan 26 12:21:01 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

General

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x92cfc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x94000	0x5f4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x96000	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	0x90d54	0x90e00	False	0.810157598145	data	7.69028247011	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x94000	0x5f4	0x600	False	0.431640625	data	4.18640822203	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x96000	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	0x94090	0x364	data		
RT_MANIFEST	0x94404	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

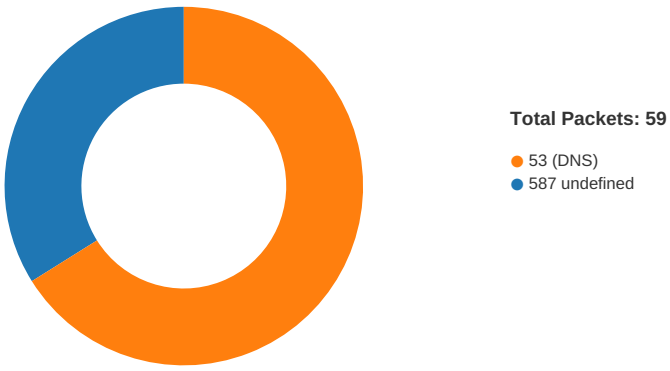
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	EncoderReplacementFallback.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HaploTree
ProductVersion	1.0.0.0
FileDescription	HaploTree
OriginalFilename	EncoderReplacementFallback.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 08:31:42.935362101 CET	49751	587	192.168.2.7	66.70.204.222

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 08:31:43.074661970 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:43.076642990 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:43.383580923 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:43.385039091 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:43.521696091 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:43.522202969 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:43.661992073 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:43.707190990 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:43.745526075 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:43.892276049 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:43.892304897 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:43.892313957 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:43.892549038 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:43.901139975 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:44.040610075 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:44.082218885 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:44.309752941 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:44.447779894 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:44.450066090 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:44.586184978 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:44.587112904 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:44.744554043 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:44.745982885 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:44.881819010 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:44.882464886 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:45.018640041 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:45.019244909 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:45.155807972 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:45.161557913 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:45.161890030 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:45.162748098 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:45.162998915 CET	49751	587	192.168.2.7	66.70.204.222
Jan 27, 2021 08:31:45.297488928 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:45.297532082 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:45.298389912 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:45.298584938 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:45.300465107 CET	587	49751	66.70.204.222	192.168.2.7
Jan 27, 2021 08:31:45.347937107 CET	49751	587	192.168.2.7	66.70.204.222

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 08:29:55.805435896 CET	58739	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:29:55.861742973 CET	53	58739	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:02.127450943 CET	60338	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:02.178242922 CET	53	60338	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:03.940587997 CET	58717	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:03.991457939 CET	53	58717	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:05.149806023 CET	59762	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:05.207145929 CET	53	59762	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:06.313421011 CET	54329	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:06.363697052 CET	53	54329	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:07.549200058 CET	58052	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:07.597451925 CET	53	58052	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:09.713658094 CET	54008	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:09.769964933 CET	53	54008	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:11.100361109 CET	59451	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:11.148260117 CET	53	59451	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:12.276639938 CET	52914	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:12.324451923 CET	53	52914	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:13.598438025 CET	64569	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:13.657857895 CET	53	64569	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:14.861053944 CET	52816	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:14.922621012 CET	53	52816	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 08:30:16.125519991 CET	50781	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:17.155932903 CET	50781	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:18.170857906 CET	53	50781	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:18.180001974 CET	53	50781	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:19.237205029 CET	54230	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:19.285069942 CET	53	54230	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:20.034487009 CET	54911	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:20.085191011 CET	53	54911	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:20.710486889 CET	49958	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:20.768939972 CET	53	49958	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:20.830303907 CET	50860	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:20.878164053 CET	53	50860	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:22.113315105 CET	50452	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:22.163888931 CET	53	50452	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:22.965773106 CET	59730	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:23.024951935 CET	53	59730	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:23.763603926 CET	59310	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:23.811451912 CET	53	59310	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:26.595953941 CET	51919	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:26.646748066 CET	53	51919	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:44.151503086 CET	64296	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:44.212990046 CET	53	64296	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:44.751173019 CET	56680	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:44.807472944 CET	53	56680	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:45.356668949 CET	58820	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:45.415868044 CET	53	58820	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:45.470717907 CET	60983	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:45.541775942 CET	53	60983	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:45.546591997 CET	49247	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:45.594413996 CET	53	49247	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:45.771631956 CET	52286	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:45.819367886 CET	53	52286	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:45.852531910 CET	56064	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:45.912009001 CET	53	56064	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:45.927172899 CET	63744	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:45.979773045 CET	53	63744	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:46.404088020 CET	61457	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:46.455960035 CET	53	61457	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:47.034354925 CET	58367	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:47.083096027 CET	53	58367	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:47.717230082 CET	60599	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:47.765117884 CET	53	60599	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:49.035284996 CET	59571	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:49.083312035 CET	53	59571	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:50.325737953 CET	52689	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:50.375698090 CET	53	52689	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:51.019479036 CET	50290	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:51.067539930 CET	53	50290	8.8.8.8	192.168.2.7
Jan 27, 2021 08:30:52.373521090 CET	60427	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:30:52.431407928 CET	53	60427	8.8.8.8	192.168.2.7
Jan 27, 2021 08:31:30.405361891 CET	56209	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:31:30.456808090 CET	53	56209	8.8.8.8	192.168.2.7
Jan 27, 2021 08:31:42.674546957 CET	59582	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:31:42.744016886 CET	53	59582	8.8.8.8	192.168.2.7
Jan 27, 2021 08:31:42.764156103 CET	60949	53	192.168.2.7	8.8.8.8
Jan 27, 2021 08:31:42.820476055 CET	53	60949	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 08:31:42.674546957 CET	192.168.2.7	8.8.8.8	0x9fdd	Standard query (0)	mail.hybridgroupco.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:31:42.764156103 CET	192.168.2.7	8.8.8.8	0x98fc	Standard query (0)	mail.hybridgroupco.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 08:31:42.744016886 CET	8.8.8.8	192.168.2.7	0x9fdd	No error (0)	mail.hybridgroupco.com	hybridgroupco.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 08:31:42.744016886 CET	8.8.8.8	192.168.2.7	0x9fdd	No error (0)	hybridgroupco.com		66.70.204.222	A (IP address)	IN (0x0001)
Jan 27, 2021 08:31:42.820476055 CET	8.8.8.8	192.168.2.7	0x98fc	No error (0)	mail.hybridgroupco.com	hybridgroupco.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 08:31:42.820476055 CET	8.8.8.8	192.168.2.7	0x98fc	No error (0)	hybridgroupco.com		66.70.204.222	A (IP address)	IN (0x0001)

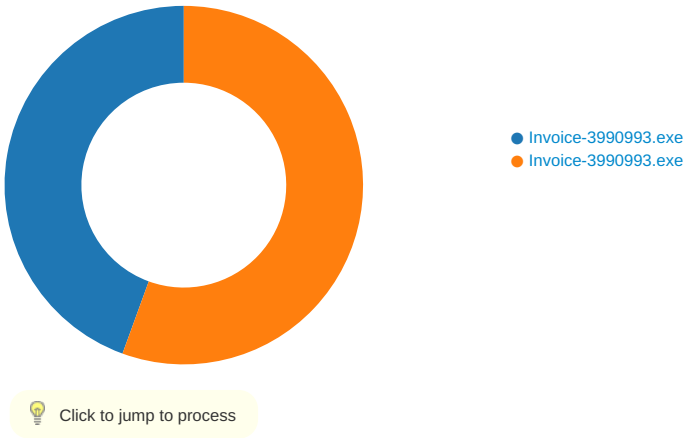
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 08:31:43.383580923 CET	587	49751	66.70.204.222	192.168.2.7	220-server.wlcserver.com ESMTP Exim 4.93 #2 Wed, 27 Jan 2021 11:31:43 +0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 27, 2021 08:31:43.385039091 CET	49751	587	192.168.2.7	66.70.204.222	EHLO 128757
Jan 27, 2021 08:31:43.521696091 CET	587	49751	66.70.204.222	192.168.2.7	250-server.wlcserver.com Hello 128757 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Jan 27, 2021 08:31:43.522202969 CET	49751	587	192.168.2.7	66.70.204.222	STARTTLS
Jan 27, 2021 08:31:43.661992073 CET	587	49751	66.70.204.222	192.168.2.7	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Invoice-3990993.exe PID: 4556 Parent PID: 5724

General

Start time:	08:30:00
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\Invoice-3990993.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Invoice-3990993.exe'
Imagebase:	0x50000
File size:	595968 bytes
MD5 hash:	C240ECB4D6DA455111DCA9256DCD3604
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: 00000000.00000002.230286237.0000000002452000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.230847336.0000000003429000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.230261930.0000000002421000.00000004.00000001.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	6D3FCF06	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	6D3FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice-3990993.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D70C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice-3990993.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	6D70C907	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	6D3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C241B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C241B4F	ReadFile

Analysis Process: Invoice-3990993.exe PID: 6228 Parent PID: 4556

General

Start time:	08:30:02
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\Invoice-3990993.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Invoice-3990993.exe
Imagebase:	0xe10000
File size:	595968 bytes
MD5 hash:	C240ECB4D6DA455111DCA9256DCD3604
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: 00000002.00000002.588090737.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.591701413.00000000032C1000.00000004.00000001.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	6D3FCF06	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	6D3FCF06	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	6D3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C241B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C241B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C241B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C241B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C241B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\1441a476-0993-4f6d-922a-35d6166eaba8	unknown	4096	success or wait	1	6C241B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C241B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C241B4F	ReadFile

Disassembly

Code Analysis