ID: 452732
Sample Name: Payment $67,765.exe
Cookbook: default.jbs
Time: 19:11:25
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

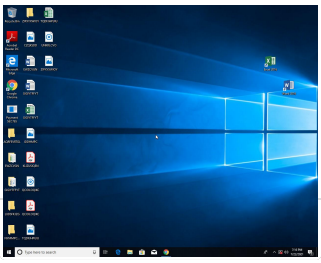
Windows Analysis Report Payment $67,765.exe

Overview

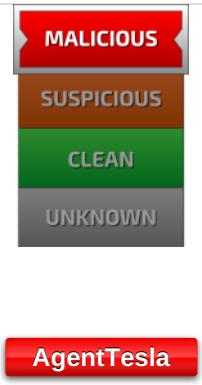
General Information

Sample Name:	Payment $67,765.exe
Analysis ID:	452732
MD5:	eaf39a263bece3c..
SHA1:	6ca9713419a03c..
SHA256:	2bd20bf1f968993..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

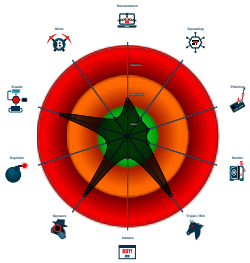


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64**
- Payment $67,765.exe (PID: 5348 cmdline: 'C:\Users\user\Desktop\Payment $67,765.exe' MD5: EAF39A263BECE3CBD0D6B70E22C12D8F)
  - Payment $67,765.exe (PID: 5856 cmdline: C:\Users\user\Desktop\Payment $67,765.exe MD5: EAF39A263BECE3CBD0D6B70E22C12D8F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "billions101@vivaldi.net",
  "Password": "Great#@#$12909()*&^",
  "Host": "smtp.vivaldi.net"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.772368800.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.772368800.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000002.776979004.000000000308000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.776979004.000000000308000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000008.00000002.776594989.0000000002FF1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.Payment $67,765.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.2.Payment $67,765.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

System Summary:

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

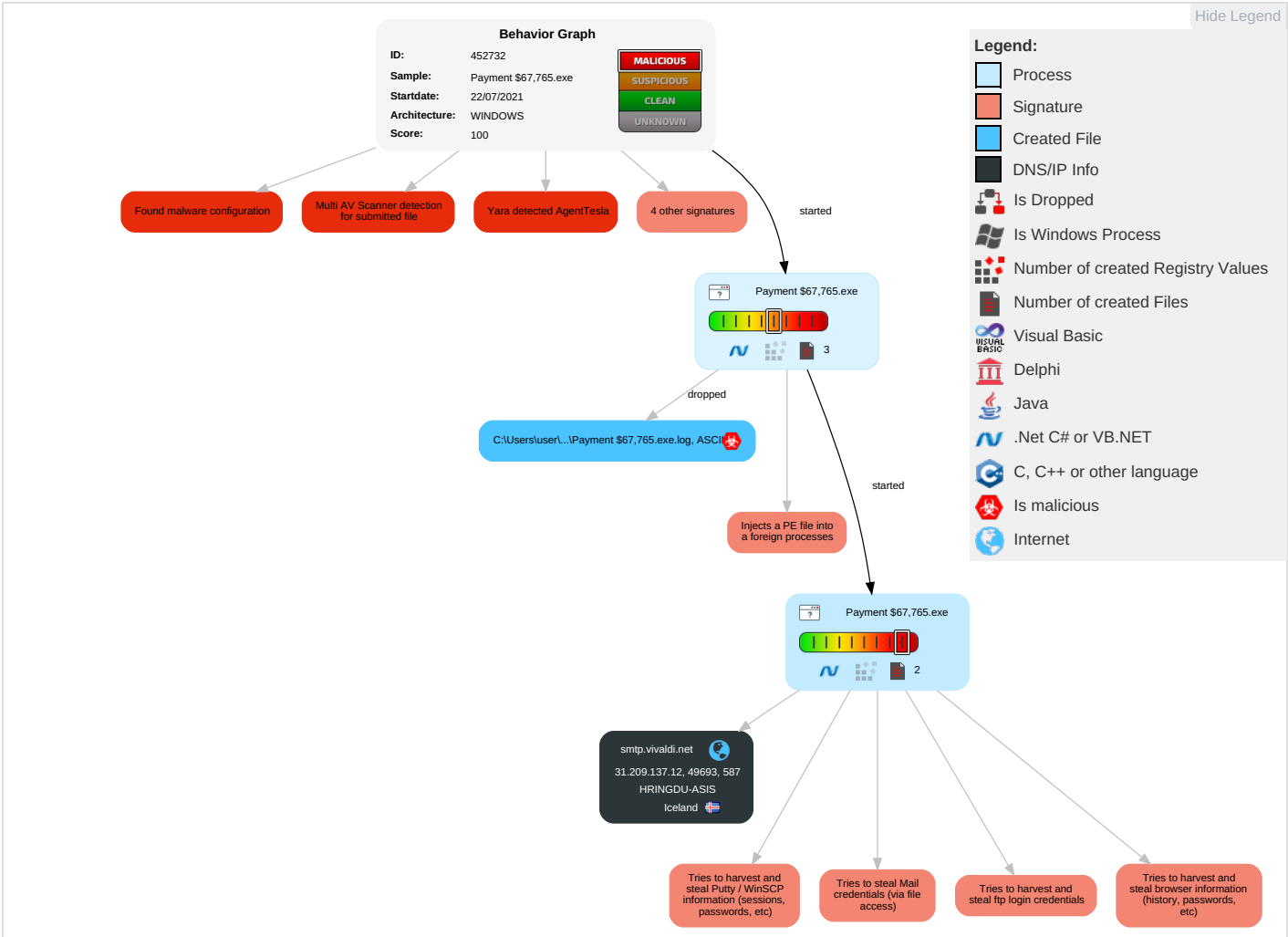
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

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

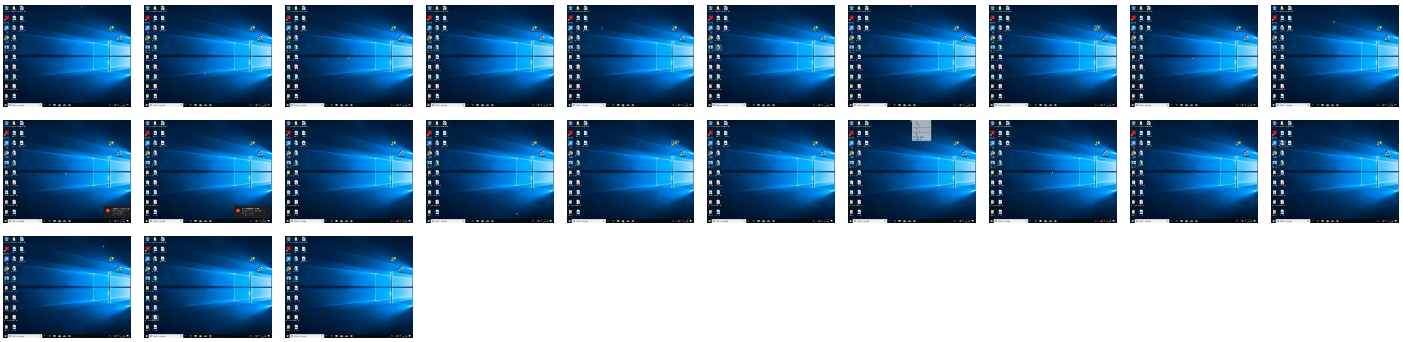
Behavior Graph



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
Payment $67,765.exe	46%	Virustotal		Browse
Payment $67,765.exe	17%	Metadefender		Browse
Payment $67,765.exe	22%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.Payment $67,765.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://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.fontbureau.comceom	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ase	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com4	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://hPAZoH.com	0%	Avira URL Cloud	safe	
http://a8LHbhswx7q.orgL	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/:	0%	Avira URL Cloud	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://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.fontbureau.comk:	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.founder.com.cn/cnv	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma-dS	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	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://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/W	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://www.monotype.ec	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://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.fontbureau.comcomk:	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://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	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://www.tiro.coms	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.sandoll.co.krk	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/E	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/E	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/E	0%	URL Reputation	safe	
http://a8LHbhswx7q.org	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.comts	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.209.137.12	smtp.vivaldi.net	Iceland		51896	HRINGDU-ASIS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452732
Start date:	22.07.2021
Start time:	19:11:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment $67,765.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:	14
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:	• Successful, ratio: 15.1% (good quality ratio 11.6%) • Quality average: 49.9% • Quality standard deviation: 32.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:12:54	API Interceptor	1524x Sleep call for process: Payment $67,765.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
31.209.137.12	SecuriteInfo.com.W32.MSIL_Agent.CAC.genEldorado.5417.exe	Get hash	malicious	Browse	
	DHL SHIPPING INVOICE.pdf.exe	Get hash	malicious	Browse	
	URGENT REQUEST FOR QUOTATION.pdf.exe	Get hash	malicious	Browse	
	RE Outstanding SOA Settled.exe	Get hash	malicious	Browse	
	Swift Copy.exe	Get hash	malicious	Browse	
	Swift Copy.exe	Get hash	malicious	Browse	
	9872362-1926.exe	Get hash	malicious	Browse	
	invoice.exe	Get hash	malicious	Browse	
	Order.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis960D9DB7F7C9.7109.exe	Get hash	malicious	Browse	
	PREPAYMENT.exe	Get hash	malicious	Browse	
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	
	quo 4542.exe	Get hash	malicious	Browse	
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	
	Swift TT copy.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.ArtemisA47F39CCDFEA.14562.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.495766.21629.exe	Get hash	malicious	Browse	
	COMMERCIAL INVOICE.exe	Get hash	malicious	Browse	
	Scan 07.07.2021# 99147.exe	Get hash	malicious	Browse	
	Quotes 04.06.2021.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.vivaldi.net	SecuriteInfo.com.W32.MSIL_Agent.CAC.genEldorado.5417.exe	Get hash	malicious	Browse	• 31.209.137.12
	DHL SHIPPING INVOICE.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	URGENT REQUEST FOR QUOTATION.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	RE Outstanding SOA Settled.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift Copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift Copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	9872362-1926.exe	Get hash	malicious	Browse	• 31.209.137.12
	invoice.exe	Get hash	malicious	Browse	• 31.209.137.12
	Order.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.Artemis960D9DB7F7C9.7109.exe	Get hash	malicious	Browse	• 31.209.137.12
	PREPAYMENT.exe	Get hash	malicious	Browse	• 31.209.137.12
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 31.209.137.12
	quo 4542.exe	Get hash	malicious	Browse	• 31.209.137.12
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift TT copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.ArtemisA47F39CCDFEA.14562.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.Variant.Bulz.495766.21629.exe	Get hash	malicious	Browse	• 31.209.137.12
	COMMERCIAL INVOICE.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 07.07.2021# 99147.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quotes 04.06.2021.exe	Get hash	malicious	Browse	• 31.209.137.12

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HRINGDU-ASIS	SecuriteInfo.com.W32.MSIL_Agent.CAC.genEldorado.5417.exe	Get hash	malicious	Browse	• 31.209.137.12
	DHL SHIPPING INVOICE.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	URGENT REQUEST FOR QUOTATION.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	RE Outstanding SOA Settled.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift Copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	Swift Copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	9872362-1926.exe	Get hash	malicious	Browse	• 31.209.137.12
	invoice.exe	Get hash	malicious	Browse	• 31.209.137.12
	Order.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.Artemis960D9DB7F7C9.7109.exe	Get hash	malicious	Browse	• 31.209.137.12
	PREPAYMENT.exe	Get hash	malicious	Browse	• 31.209.137.12
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 31.209.137.12
	quo 4542.exe	Get hash	malicious	Browse	• 31.209.137.12
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 31.209.137.12

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Swift TT copy.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.ArtemisA47F39CCDFEA.14562.exe	Get hash	malicious	Browse	• 31.209.137.12
	SecuriteInfo.com.Variant.Bulz.495766.21629.exe	Get hash	malicious	Browse	• 31.209.137.12
	COMMERCIAL INVOICE.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 07.07.2021# 99147.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quotes 04.06.2021.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\Payment $67,765.exe.log	
Process:	C:\Users\user\Desktop\Payment $67,765.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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):	7.779950459380049
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Payment $67,765.exe
File size:	784896
MD5:	eaf39a263bece3cbd0d6b70e22c12d8f
SHA1:	6ca9713419a03c0d1ab3e7a17dc3256bae2acb59
SHA256:	2bd20bf1f968993cf9f212761a86b1745abf4990ddcd5d5c553f456dcff3535f
SHA512:	3d9802404d26a7033a10e319d4bf99c8b63b931d5980c5176d4f0fbe35904b506e14f4b3b4d6f0b71560429389a28f70788cb83f7da01da5ac0938f90cc96d99

General

SSDEEP:	12288:CYtMBhsEtFHuGMaaEowPYqafsjTa2lQQqgum9HRPNk36p8MJTcdB2QnUfxEVO7/W:HMBztMa1ow8fsjTVxjP/EnMo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..... ... ....@.. ..... `.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c0c0e
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:	0x60F88385 [Wed Jul 21 20:28:53 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbec14	0xbee00	False	0.870332709152	SysEx File - Voyce	7.78926933063	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc2000	0x640	0x800	False	0.34521484375	data	3.51813378508	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	0xc	0x200	False	0.041015625	data	0.0776331623432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 19:14:33.924093008 CEST	192.168.2.5	8.8.8.8	0x7d30	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
Jul 22, 2021 19:14:33.983745098 CEST	8.8.8.8	192.168.2.5	0x7d30	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
Jul 22, 2021 19:14:34.713717937 CEST	587	49693	31.209.137.12	192.168.2.5	220 smtp.vivaldi.net ESMTP Postfix (Ubuntu)
Jul 22, 2021 19:14:34.714492083 CEST	49693	587	192.168.2.5	31.209.137.12	EHLO 928100
Jul 22, 2021 19:14:34.805233955 CEST	587	49693	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
Jul 22, 2021 19:14:34.805751085 CEST	49693	587	192.168.2.5	31.209.137.12	STARTTLS
Jul 22, 2021 19:14:34.893631935 CEST	587	49693	31.209.137.12	192.168.2.5	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Payment $67,765.exe PID: 5348 Parent PID: 5512

General

Start time:	19:12:27
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Payment $67,765.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment $67,765.exe'
Imagebase:	0x650000
File size:	784896 bytes
MD5 hash:	EAF39A263BECE3CBD0D6B70E22C12D8F

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: Payment $67,765.exe PID: 5856 Parent PID: 5348

General

Start time:	19:12:55
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Payment $67,765.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment $67,765.exe
Imagebase:	0x7ff797770000
File size:	784896 bytes
MD5 hash:	EAF39A263BECE3CBD0D6B70E22C12D8F
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: 00000008.00000002.772368800.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.772368800.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.776979004.0000000003098000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.776979004.0000000003098000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.776594989.0000000002FF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.776594989.0000000002FF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis