

JOeSandbox Cloud BASIC



ID: 532918

Sample Name:

Waybilldoc_220950655.pdf.exe

Cookbook: default.jbs

Time: 20:16:14

Date: 02/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Waybilldoc_220950655.pdf.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Jbx Signature Overview	5
AV Detection:	5
System Summary:	5
Data Obfuscation:	5
Hooking and other Techniques for Hiding and Protection:	5
Malware Analysis System Evasion:	5
Stealing of Sensitive Information:	5
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
Contacted IPs	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	10
General	11
File Icon	11
Static PE Info	11
General	11
Entrypoint Preview	11
Data Directories	11
Sections	11
Resources	12
Imports	12
Version Infos	12
Network Behavior	12
Code Manipulations	12
Statistics	12
Behavior	12
System Behavior	12
Analysis Process: Waybilldoc_220950655.pdf.exe PID: 7004 Parent PID: 2244	12
General	12
File Activities	12
File Created	13
File Written	13
File Read	13
Analysis Process: Waybilldoc_220950655.pdf.exe PID: 7124 Parent PID: 7004	13
General	13
File Activities	13
File Created	13
File Read	13
Disassembly	13

Windows Analysis Report Waybilldoc_220950655.pdf.exe

Overview

General Information

Sample Name:

Waybilldoc_220950655.pdf.exe

Analysis ID:

532918

MD5:

717a4adeef2cc5..

SHA1:

834b3549011ac5..

SHA256:

52ffc0a75a42165..

Tags:

exe

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

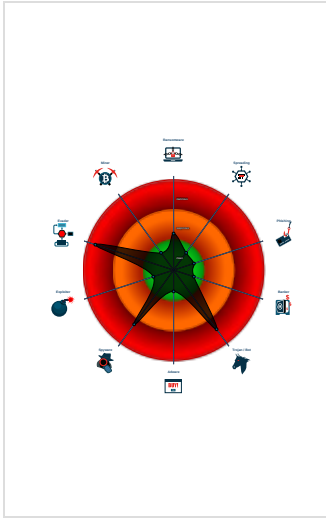
AgentTesla

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

Signatures

- Found malware configuration
- Sigma detected: Suspicious Double ...
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fil...
- Initial sample is a PE file and has a ...
- Tries to detect sandboxes and other...
- .NET source code contains potentia...
- .NET source code contains very larg...
- Uses an obfuscated file name to hid...
- Queries sensitive network adapter in...
- Tries to harvest and steal browser in...

Classification



Process Tree

- System is w10x64
- Waybilldoc_220950655.pdf.exe (PID: 7004 cmdline: "C:\Users\user\Desktop\Waybilldoc_220950655.pdf.exe" MD5: 717A4ADEEAF2CC5CCCCC944ACCB3B2FD)
 - Waybilldoc_220950655.pdf.exe (PID: 7124 cmdline: C:\Users\user\Desktop\Waybilldoc_220950655.pdf.exe MD5: 717A4ADEEAF2CC5CCCCC944ACCB3B2FD)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "ugo@bhgautopartes.com",
  "Password": "icui4cu2@@",
  "Host": "mail.bhgautopartes.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.285254478.0000000002871000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000000.282755212.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.282755212.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.547694451.0000000003091000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.547694451.0000000003091000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 15 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Waybilldoc_220950655.pdf.exe.2891bac.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
1.2.Waybilldoc_220950655.pdf.exe.38d3790.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Waybilldoc_220950655.pdf.exe.38d3790.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.Waybilldoc_220950655.pdf.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.Waybilldoc_220950655.pdf.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 16 entries

Sigma Overview

System Summary:



Sigma detected: Suspicious Double Extension

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

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:



Uses an obfuscated file name to hide its real file extension (double extension)

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)

Stealing of Sensitive Information:



Yara detected AgentTesla

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

Remote Access Functionality:

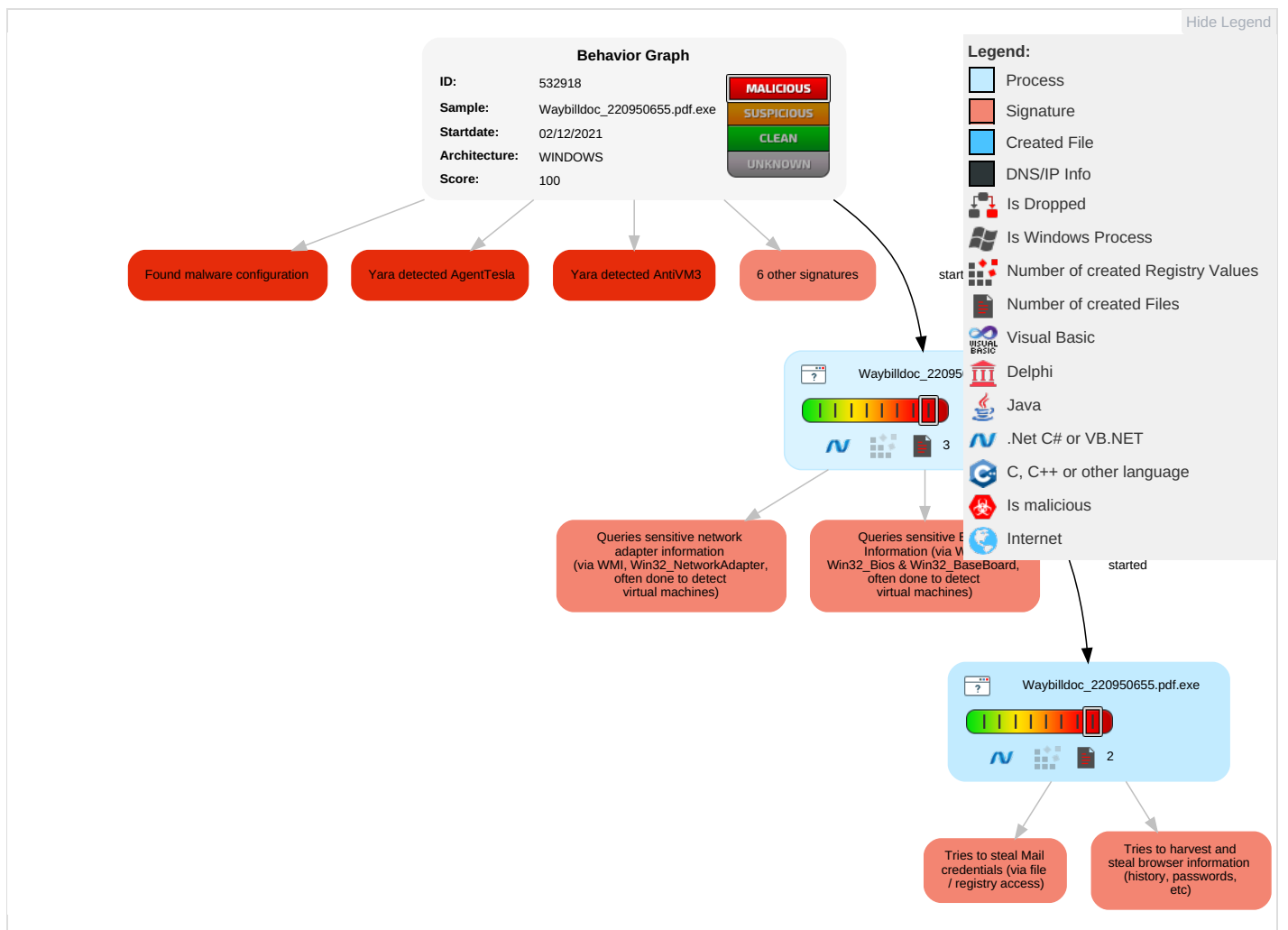


Yara detected AgentTesla

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 2	Masquerading 1 1	OS Credential Dumping 1	Security Software Discovery 2 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	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

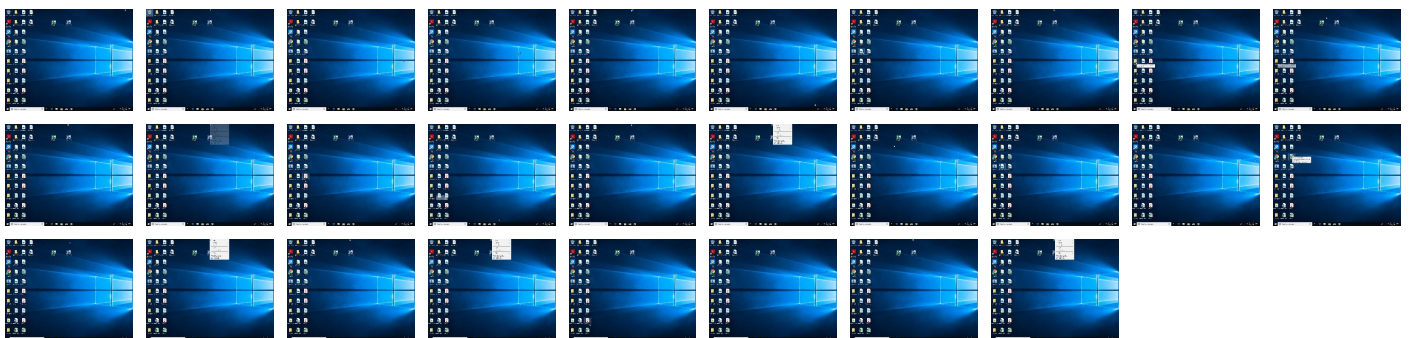
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.Waybilldoc_220950655.pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Waybilldoc_220950655.pdf.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Waybilldoc_220950655.pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Waybilldoc_220950655.pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Waybilldoc_220950655.pdf.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Waybilldoc_220950655.pdf.exe.400000.6.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://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	0%	URL Reputation	safe	
http://uArhJl.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532918
Start date:	02.12.2021
Start time:	20:16:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Waybilldoc_220950655.pdf.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:	26
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@0/0
EGA Information:	Failed
HDC Information:	- Successful, ratio: 0.8% (good quality ratio 0.6%) - Quality average: 61.1% - Quality standard deviation: 36.7%
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
20:17:04	API Interceptor	815x Sleep call for process: Waybilldoc_220950655.pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\luser\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Waybilldoc_220950655.pdf.exe.log	
Process:	C:\Users\luser\Desktop\Waybilldoc_220950655.pdf.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\1d8480152e0da9a60ad49c6d16a3b6d\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\1b219d4630d26b88041b59c21

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.77736834777064
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:	Waybilldoc_220950655.pdf.exe
File size:	476672
MD5:	717a4adeeaf2cc5ccccc944accb3b2fd
SHA1:	834b3549011ac52fa34c2299b8194087f6a695e8
SHA256:	52ffc0a75a42165e68bc35efc7b9bdd4069c7f5d4054c040737cfc87ae158da8
SHA512:	a6f52d450d198458a85f01a9b6a0a14aa8356cb68bec713474efd1935f686b9c4fc68eb0dd43fd978bbee17650ef8688e46759d30c11f50ec2c15dd5584b40ea
SSDEEP:	12288:xFQp3eY/+Rwfc2doD8SjUWNO/s4kFK+Rx/L17G:NmEAaNO/s4g1p7
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.PE..L.....<.....^Z...`....@..@.....

File Icon	
	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x475a5e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x91B4DF98 [Wed Jun 19 09:40:40 2047 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	0x73a64	0x73c00	False	0.887488610286	data	7.78942430376	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x4e0	0x600	False	0.373697916667	data	3.73482907125	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x78000	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

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Waybilldoc_220950655.pdf.exe PID: 7004 Parent PID: 2244

General

Start time:	20:17:03
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Waybilldoc_220950655.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Waybilldoc_220950655.pdf.exe"
Imagebase:	0x400000
File size:	476672 bytes
MD5 hash:	717A4ADEEAF2CC5CCCCC944ACCB3B2FD
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: 00000001.00000002.285254478.0000000002871000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.285322085.00000000028AD000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.286150173.0000000003879000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.286150173.0000000003879000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Waybilldoc_220950655.pdf.exe PID: 7124 Parent PID: 7004

General

Start time:	20:17:05
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Waybilldoc_220950655.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Waybilldoc_220950655.pdf.exe
Imagebase:	0xcd0000
File size:	476672 bytes
MD5 hash:	717A4ADEEAF2CC5CCCCC944ACCB3B2FD
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: 00000003.00000000.282755212.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.282755212.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.547694451.0000000003091000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.547694451.0000000003091000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.281746367.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.281746367.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.282312678.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.282312678.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.544593892.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.544593892.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.283323027.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.283323027.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

