ID: 764045
Sample Name: ADOC RFQ-WCMS-18097255.exe
Cookbook: default.jbs
Time: 11:04:13
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

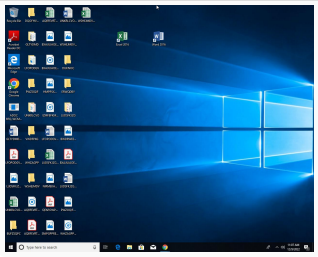
Windows Analysis Report

ADOC RFQ-WCMS-18097255.exe

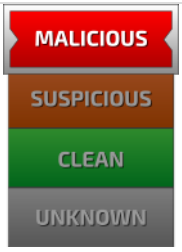
Overview

General Information

Sample Name:	ADOC RFQ-WCMS-18097255.exe
Analysis ID:	764045
MD5:	856317033475c7..
SHA1:	6b24fa54a99047..
SHA256:	15700616b67e3a..
Tags:	exe
Infos:	



Detection



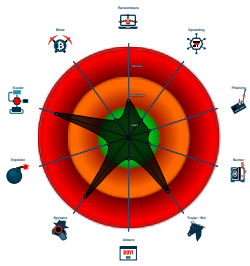
AgentTesla

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- ADOC RFQ-WCMS-18097255.exe (PID: 5788 cmdline: C:\Users\user\Desktop\ADOC RFQ-WCMS-18097255.exe MD5: 856317033475C7932F8CBF88EC2B7EF8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Host": "us2.smtp.mailhostbox.com",
  "Username": "gamzy@freesteelmyst.xyz",
  "Password": "  JIRUmBO0        "
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.508080417.0000000002B8E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.513606305.0000000003C61000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x23760:$a20: get_LastAccessed • 0x25885:$a30: set_GuidMasterKey • 0x23814:$a33: get_Clipboard • 0x23822:$a34: get_Keyboard • 0x249cd:$a35: get_ShiftKeyDown • 0x249de:$a36: get_AltKeyDown • 0x2382f:$a37: get_Password • 0x24253:$a38: get_PasswordHash • 0x250d6:$a39: get_DefaultCredentials
00000000.00000002.519041329.0000000007040000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2619e:$s10: logins • 0x25cd7:$s11: credential • 0x22b94:$g1: get_Clipboard • 0x22ba2:$g2: get_Keyboard • 0x22baf:$g3: get_Password • 0x23d3d:$g4: get_CtrlKeyDown • 0x23d4d:$g5: get_ShiftKeyDown • 0x23d5e:$g6: get_AltKeyDown
00000000.00000002.519041329.0000000007040000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x22ae0:$a20: get_LastAccessed • 0x24c05:$a30: set_GuidMasterKey • 0x22b94:$a33: get_Clipboard • 0x22ba2:$a34: get_Keyboard • 0x23d4d:$a35: get_ShiftKeyDown • 0x23d5e:$a36: get_AltKeyDown • 0x22baf:$a37: get_Password • 0x235d3:$a38: get_PasswordHash • 0x24456:$a39: get_DefaultCredentials
00000000.00000002.510469030.0000000003881000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x53430:$a20: get_LastAccessed • 0x55555:$a30: set_GuidMasterKey • 0x534e4:$a33: get_Clipboard • 0x534f2:$a34: get_Keyboard • 0x5469d:$a35: get_ShiftKeyDown • 0x546ae:$a36: get_AltKeyDown • 0x534ff:$a37: get_Password • 0x53f23:$a38: get_PasswordHash • 0x54da6:$a39: get_DefaultCredentials
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ADOC RFQ-WCMS-18097255.exe.7040000.12.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2439e:$s10: logins • 0x23ed7:$s11: credential • 0x20d94:$g1: get_Clipboard • 0x20da2:$g2: get_Keyboard • 0x20daf:$g3: get_Password • 0x21f3d:$g4: get_CtrlKeyDown • 0x21f4d:$g5: get_ShiftKeyDown • 0x21f5e:$g6: get_AltKeyDown
0.2.ADOC RFQ-WCMS-18097255.exe.7040000.12.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x20ce0:$a20: get_LastAccessed • 0x22e05:$a30: set_GuidMasterKey • 0x20d94:$a33: get_Clipboard • 0x20da2:$a34: get_Keyboard • 0x21f4d:$a35: get_ShiftKeyDown • 0x21f5e:$a36: get_AltKeyDown • 0x20daf:$a37: get_Password • 0x217d3:$a38: get_PasswordHash • 0x22656:$a39: get_DefaultCredentials
0.2.ADOC RFQ-WCMS-18097255.exe.3c61c80.6.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2619e:$s10: logins • 0x25cd7:$s11: credential • 0x22b94:$g1: get_Clipboard • 0x22ba2:$g2: get_Keyboard • 0x22baf:$g3: get_Password • 0x23d3d:$g4: get_CtrlKeyDown • 0x23d4d:$g5: get_ShiftKeyDown • 0x23d5e:$g6: get_AltKeyDown
0.2.ADOC RFQ-WCMS-18097255.exe.3c61c80.6.raw.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x22ae0:$a20: get_LastAccessed • 0x24c05:$a30: set_GuidMasterKey • 0x22b94:$a33: get_Clipboard • 0x22ba2:$a34: get_Keyboard • 0x23d4d:$a35: get_ShiftKeyDown • 0x23d5e:$a36: get_AltKeyDown • 0x22baf:$a37: get_Password • 0x235d3:$a38: get_PasswordHash • 0x24456:$a39: get_DefaultCredentials
0.2.ADOC RFQ-WCMS-18097255.exe.3889930.3.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x4c3be:$s10: logins • 0x4bef7:$s11: credential • 0x48db4:$g1: get_Clipboard • 0x48dc2:$g2: get_Keyboard • 0x48dcf:$g3: get_Password • 0x49f5d:$g4: get_CtrlKeyDown • 0x49f6d:$g5: get_ShiftKeyDown • 0x49f7e:$g6: get_AltKeyDown

Source	Rule	Description	Author	Strings
Click to see the 21 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

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)

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

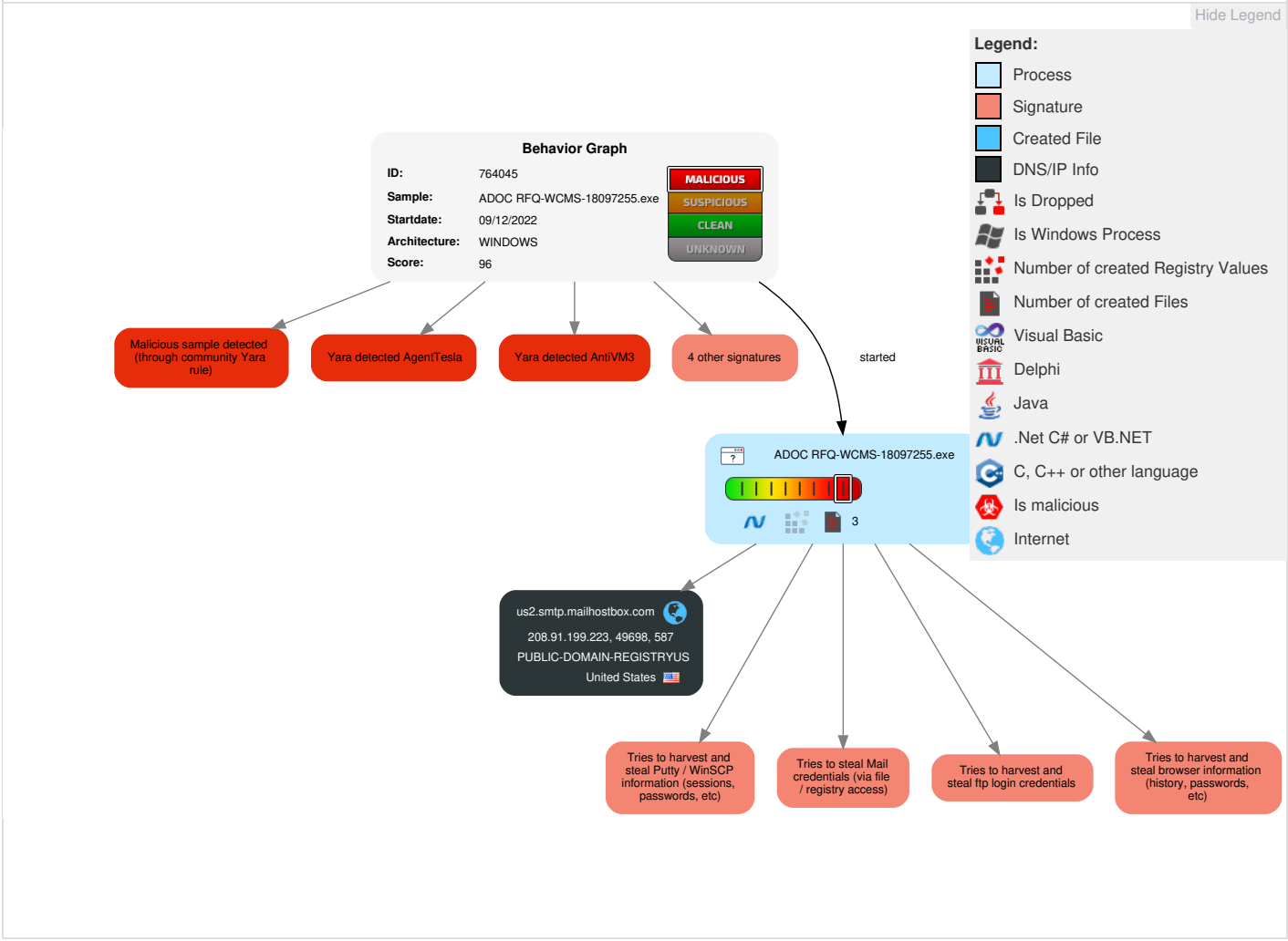
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	Path Interception	1 Disable or Modify Tools	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Software Packing	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

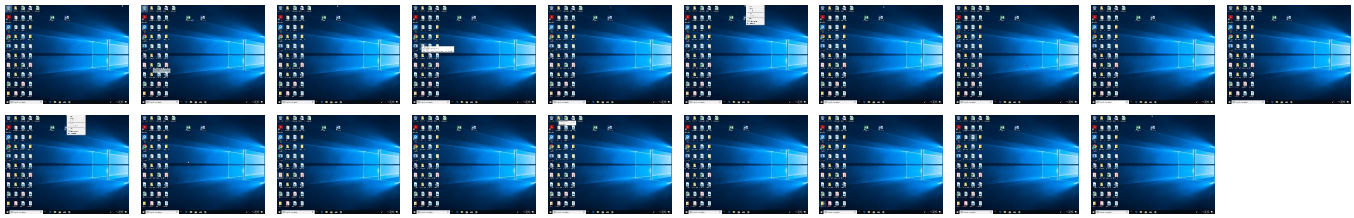
Behavior Graph



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
ADOC RFQ-WCMS-18097255.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://CtxmCtXtvGR51e3orE.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high

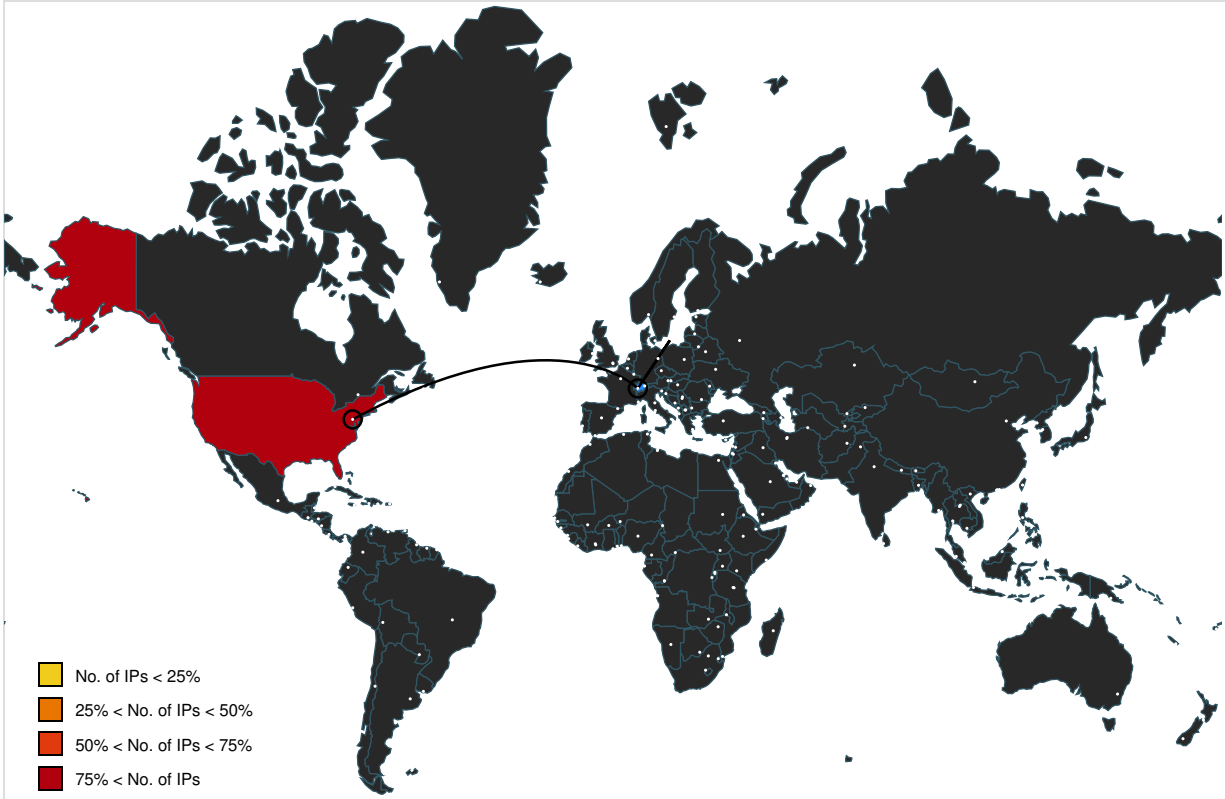
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.520037204.0000000009830000.00000004.00000800.00020000.00000000.sdmp, ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.507971659.0000000002B6A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.520037204.0000000009830000.00000004.00000800.00020000.00000000.sdmp, ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.507971659.0000000002B6A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.507971659.0000000002B6A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://CtxmCtXtvGR51e3orE.org	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.505811223.0000000002881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.505811223.0000000002881000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.sectigo.com0A	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.520037204.0000000009830000.00000004.00000800.00020000.00000000.sdmp, ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.507971659.0000000002B6A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	ADOC RFQ-WCMS-18097255.exe, 00000000.00000002.516330292.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.223	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764045
Start date and time:	2022-12-09 11:04:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ADOC RFQ-WCMS-18097255.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
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:	mal96.troj.spyw.evad.winEXE@1/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- 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
11:05:12	API Interceptor	753x Sleep call for process: ADOC RFQ-WCMS-18097255.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.555023841660244
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:	ADOC RFQ-WCMS-18097255.exe
File size:	1003520
MD5:	856317033475c7932f8cbf88ec2b7ef8
SHA1:	6b24fa54a990477bde13f64144d5d5a1187c40b9
SHA256:	15700616b67e3ac2d97cfb221762dca3b2b36cc9d3e1cf7ca8737acc9bb4db84
SHA512:	58231da8dfb1eec9d94841ef9d5474d64e13f31365d517eecc28f17c71851762a383b8a7837db446e7fb17aaa546d8728ef36e2425683fc07536fa330bc89f6f
SSDEEP:	12288:b1fhB01+YyFwG5JKp5ctm1V63em1nHATF+JRS1TWRfg3ZpFL:b1fhC1Jy95JKLf63eDqxIJpF
TLSH:	0E257DD5ABF2A026F48F72522418369DDC35BD43774BE19667723B4082D48FFB6A8483
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.....0..H.....~f... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4f667e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xE8FF4486 [Sat Nov 14 13:22:14 2093 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf662c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf8000	0x398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xfa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xf6610	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xf4684	0xf4800	False	0.8147017590107362	data	7.556547919849989	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xf8000	0x398	0x400	False	0.3828125	data	2.924448333381374	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	0xfa000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

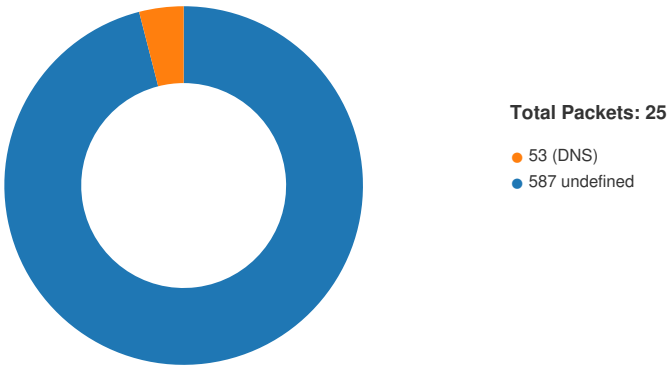
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xf8058	0x33c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:05:30.268661022 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:30.435899973 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:30.436017036 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:30.991494894 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:30.991981030 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:31.160293102 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:31.160362959 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:31.160856962 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:31.328228951 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:31.418936968 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:31.586025000 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:31.586055040 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:31.586244106 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:31.586386919 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:31.586409092 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:31.586472988 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:31.588968992 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:31.657943964 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:31.753552914 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:31.791228056 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:31.958822012 CET	587	49698	208.91.199.223	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:05:32.002902031 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:32.138349056 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:32.306432962 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:32.310359001 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:32.480194092 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:32.481578112 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:32.654700994 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:32.655360937 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:32.825046062 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:32.825598955 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:33.015599966 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:33.017049074 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:33.185446978 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:33.187422991 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:33.187670946 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:33.188152075 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:33.188152075 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:05:33.354585886 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:33.355048895 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:33.483477116 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:05:33.535815001 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:07:10.197741032 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:07:10.365978003 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:07:10.366503000 CET	587	49698	208.91.199.223	192.168.2.3
Dec 9, 2022 11:07:10.366581917 CET	49698	587	192.168.2.3	208.91.199.223
Dec 9, 2022 11:07:10.368838072 CET	49698	587	192.168.2.3	208.91.199.223

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:05:30.229001999 CET	62704	53	192.168.2.3	8.8.8.8
Dec 9, 2022 11:05:30.248526096 CET	53	62704	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 11:05:30.229001999 CET	192.168.2.3	8.8.8.8	0xe412	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 11:05:30.248526096 CET	8.8.8.8	192.168.2.3	0xe412	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:05:30.248526096 CET	8.8.8.8	192.168.2.3	0xe412	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:05:30.248526096 CET	8.8.8.8	192.168.2.3	0xe412	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:05:30.248526096 CET	8.8.8.8	192.168.2.3	0xe412	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 9, 2022 11:05:30.991494894 CET	587	49698	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Dec 9, 2022 11:05:30.991981030 CET	49698	587	192.168.2.3	208.91.199.223	EHLO 960781

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 9, 2022 11:05:31.160362959 CET	587	49698	208.91.199.223	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Dec 9, 2022 11:05:31.160856962 CET	49698	587	192.168.2.3	208.91.199.223	STARTTLS
Dec 9, 2022 11:05:31.328228951 CET	587	49698	208.91.199.223	192.168.2.3	220 2.0.0 Ready to start TLS

Statistics

No statistics

System Behavior

Analysis Process: ADOC RFQ-WCMS-18097255.exe PID: 5788, Parent PID: 3452

General

Target ID:	0
Start time:	11:05:03
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\ADOC RFQ-WCMS-18097255.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ADOC RFQ-WCMS-18097255.exe
Imagebase:	0x500000
File size:	1003520 bytes
MD5 hash:	856317033475C7932F8CBF88EC2B7EF8
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: 00000000.00000002.508080417.0000000002B8E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.513606305.0000000003C61000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000000.00000002.519041329.0000000007040000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.519041329.0000000007040000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.510469030.0000000003881000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.505811223.0000000002881000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.505811223.0000000002881000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.505811223.0000000002881000.00000004.00000800.00020000.00000000.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	6D1BCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D1BCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp7DB0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C007038	GetTempFileNameW

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	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C001B4F	ReadFile

Disassembly

No disassembly