ID: 458825
Sample Name: Purchase Order No.48743310321-RCN.pdf.exe
Cookbook: default.jbs
Time: 19:22:13
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

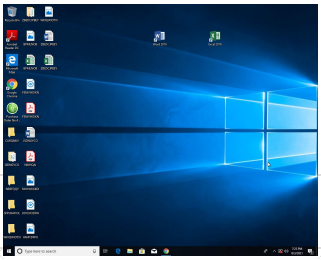
Windows Analysis Report Purchase Order No.48743310…

Overview

General Information

Sample Name:	Purchase Order No.48743310321-RCN.pdf.exe
Analysis ID:	458825
MD5:	2c32499d41cd6c…
SHA1:	c9a9e04a6bcbca…
SHA256:	167b72ba0a1621..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

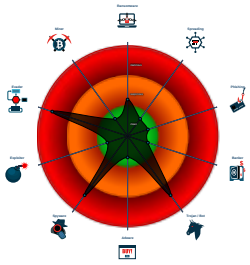
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- Purchase Order No.48743310321-RCN.pdf.exe (PID: 6864 cmdline: 'C:\Users\user\Desktop\Purchase Order No.48743310321-RCN.pdf.exe' MD5: 2C32499D41CD6C7508ECD32F9A6C37CB)
  - Purchase Order No.48743310321-RCN.pdf.exe (PID: 7084 cmdline: C:\Users\user\Desktop\Purchase Order No.48743310321-RCN.pdf.exe MD5: 2C32499D41CD6C7508ECD32F9A6C37CB)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "cspuri@searchnet.co.in",
  "Password": "22june1969",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.372504988.00000000028F4000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.603264270.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.603264270.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.606298016.0000000002EE1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.372935866.0000000003579000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Purchase Order No.48743310321-RCN.pdf.exe.3a99380.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase Order No.48743310321-RCN.pdf.exe.3a99380.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.Purchase Order No.48743310321-RCN.pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.Purchase Order No.48743310321-RCN.pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Purchase Order No.48743310321-RCN.pdf.exe.3a99380.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

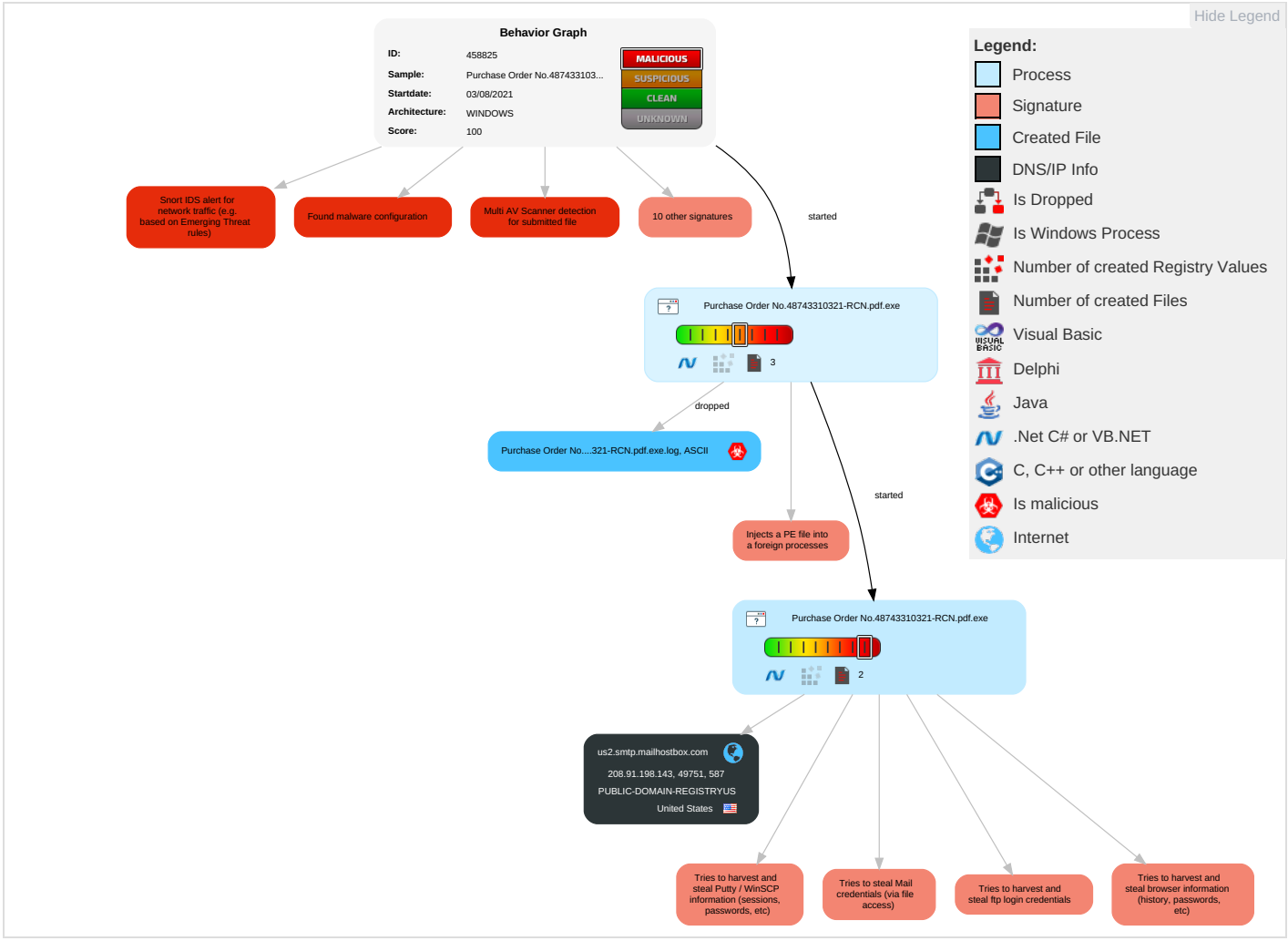
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

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

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
Purchase Order No.48743310321-RCN.pdf.exe	22%	Virustotal		Browse
Purchase Order No.48743310321-RCN.pdf.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Purchase Order No.48743310321-RCN.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.Purchase Order No.48743310321-RCN.pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/.mDgQ	0%	Avira URL Cloud	safe	
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://www.carterandcone.comal	0%	URL Reputation	safe	
http://www.carterandcone.comis	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.compt-bp9	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com)(	0%	Avira URL Cloud	safe	
http://www.urwpp.deco	0%	Avira URL Cloud	safe	
http://fontfabrik.comH	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kra-e	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.tiro.com-pD	0%	Avira URL Cloud	safe	
http://www.sakkal.com-pD	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/os=w	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnH	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnr-f	0%	Avira URL Cloud	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.zhongyicts.com.cnrqwL	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnGt2	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnk	0%	Avira URL Cloud	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.sandoll.co.krU	0%	Avira URL Cloud	safe	
http://www.carterandcone.comEac	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcesZdt	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.krde	0%	Avira URL Cloud	safe	
http://www.carterandcone.comkUIw$	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.carterandcone.comL	0%	Avira URL Cloud	safe	
http://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.carterandcone.comcrCw	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcy	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.tiro.comx	0%	Avira URL Cloud	safe	
http://fontfabrik.comXdu	0%	Avira URL Cloud	safe	
http://www.carterandcone.comopszvs	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comfac	0%	Avira URL Cloud	safe	
http://MBZFdJ.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.comlt	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.carterandcone.comdJsb	0%	Avira URL Cloud	safe	
http://4J6E0P567ihWAlj.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.urwpp.de-pD	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://en.w~zh	0%	Avira URL Cloud	safe	
http://www.tiro.com-jpOz	0%	Avira URL Cloud	safe	
http://fontfabrik.com(	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmBb	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comno	0%	URL Reputation	safe	
http://www.founder.com.cn/cnacs	0%	Avira URL Cloud	safe	
http://www.urwpp.deoApx	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458825
Start date:	03.08.2021
Start time:	19:22:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order No.48743310321-RCN.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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:23:19	API Interceptor	691x Sleep call for process: Purchase Order No.48743310321-RCN.pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	SOA.exe	Get hash	malicious	Browse	
	Invoice.exe	Get hash	malicious	Browse	
	Scan#0068-46c3367.exe	Get hash	malicious	Browse	
	IMG-20210802-WA0587-085.exe	Get hash	malicious	Browse	
	IMG-20210802-WA0587-087.exe	Get hash	malicious	Browse	
	order.PDF.exe	Get hash	malicious	Browse	
	PURCHASE ORDER-PO-S.L 45675675.pdf.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	Pedido urgente.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Zusy.394472.4088.exe	Get hash	malicious	Browse	
	JMIRLIEMHBPEEQvrxjqCV.exe	Get hash	malicious	Browse	
	Aditi Tiwari Resume.pdf.exe	Get hash	malicious	Browse	
	NEW RFQ FROM WEB AFRITECH.doc	Get hash	malicious	Browse	
	Shipment documents pdf.exe	Get hash	malicious	Browse	
	REMITTANCE COPY.exe	Get hash	malicious	Browse	
	ok1.exe	Get hash	malicious	Browse	
	4378e6769c14e63e1b385e955ee06b93.exe	Get hash	malicious	Browse	
	HSBC PAYMENT ADVICE.exe	Get hash	malicious	Browse	
	Doc-67789845678765670987655.exe	Get hash	malicious	Browse	
	Doc-67789845678765670987654.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	SOA.exe	Get hash	malicious	Browse	• 208.91.198.143
	MJLkaPZomUolseU.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.MSIL.Kryptik.56a80396.11710.exe	Get hash	malicious	Browse	• 208.91.199.224
	Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	Scan#0068-46c3367.exe	Get hash	malicious	Browse	• 208.91.198.143
	Scan#0068-46c3366.exe	Get hash	malicious	Browse	• 208.91.199.223
	IMG-20210802-WA0587-085.exe	Get hash	malicious	Browse	• 208.91.198.143
	IMG-20210802-WA0587-087.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.225
	PURCHASE ORDER PO09377 _093640_9307355_2 64378_88479_0E974.exe	Get hash	malicious	Browse	• 208.91.199.225
	order.PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	RFQ #7696679TTR6F.exe	Get hash	malicious	Browse	• 208.91.199.224
	Waybill Doc_027942941.exe	Get hash	malicious	Browse	• 208.91.199.225
	Confirmaci#U00f3n de pago .exe	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	oBNvb4c6bg.exe	Get hash	malicious	Browse	• 208.91.199.224
	TVz86np48Z.exe	Get hash	malicious	Browse	• 208.91.199.223
	Current Vendor Payment Application .doc	Get hash	malicious	Browse	• 208.91.199.224
	XiAn Sunnstatement 27-07-2021 pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	PURCHASE ORDER-PO-S.L 45675675.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	QAP 367893738 Ed 7 pcs.exe	Get hash	malicious	Browse	• 208.91.199.224

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	SOA.exe	Get hash	malicious	Browse	• 208.91.198.143
	QUOTATION LIST FOR NEW ORDER.exe	Get hash	malicious	Browse	• 204.11.58.233
	MJLkaPZomUolseU.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.MSIL.Kryptik.56a80396.11710.exe	Get hash	malicious	Browse	• 208.91.199.224
	Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	Scan#0068-46c3367.exe	Get hash	malicious	Browse	• 208.91.199.224
	Scan#0068-46c3366.exe	Get hash	malicious	Browse	• 208.91.199.223
	bin.exe	Get hash	malicious	Browse	• 119.18.54.122
	IMG-20210802-WA0587-085.exe	Get hash	malicious	Browse	• 208.91.199.224
	IMG-20210802-WA0587-087.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.224
	QUOTE 04202021.exe	Get hash	malicious	Browse	• 103.21.58.16
	PURCHASE ORDER PO09377 _093640_9307355_2 64378_88479_0E974.exe	Get hash	malicious	Browse	• 208.91.199.225
	order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ #7696679TTR6F.exe	Get hash	malicious	Browse	• 208.91.199.224
	Waybill Doc_027942941.exe	Get hash	malicious	Browse	• 208.91.199.225
	Confirmaci#U00f3n de pago .exe	Get hash	malicious	Browse	• 208.91.199.224
	triage_dropped_file.exe	Get hash	malicious	Browse	• 162.222.226.11
	oBNvb4c6bg.exe	Get hash	malicious	Browse	• 208.91.199.224
	TVz86np48Z.exe	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order No.48743310321-RCN.pdf.exe.log	
Process:	C:\Users\user\Desktop\Purchase Order No.48743310321-RCN.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order No.48743310321-RCN.pdf.exe.log	
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):	7.030776607944976
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:	Purchase Order No.48743310321-RCN.pdf.exe
File size:	1343488
MD5:	2c32499d41cd6c7508ecd32f9a6c37cb
SHA1:	c9a9e04a6bcbca11be25bd2d931e02f945840e0e
SHA256:	167b72ba0a1621ff746ce27f61d61e45cfbaf3e206aa7e92dcad19cd94a0f4c9
SHA512:	91cc50f7d048ab12460ca916d7952cfc5e0d05c25edc8fb55e105d7619c7f80b4bb38cac262774745f71be29e3ec69bdc086a5367b4a13ebaa5ca915ab8d8dc8
SSDEEP:	24576:XRQ+2NOcZUUh8z1Ze/7pfHjYrwdJs0kdB1ZuOlZcjrsK3ON:4/ye/7SrQKdvQFO
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....W.a.....P..... .....@.. .....@.....

File Icon

Icon Hash:	f0c2a07179b396e8

Static PE Info

General

Entrypoint:	0x50a8fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x610957C8 [Tue Aug 3 14:50:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x108900	0x108a00	False	0.604084863604	data	6.93312397169	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10c000	0x3f0b8	0x3f200	False	0.744032332921	data	7.0657936223	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-19:25:11.953346	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49751	587	192.168.2.6	208.91.198.143

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 19:25:10.432324886 CEST	192.168.2.6	8.8.8.8	0x3cba	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 19:25:10.466269970 CEST	8.8.8.8	192.168.2.6	0x3cba	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Aug 3, 2021 19:25:10.466269970 CEST	8.8.8.8	192.168.2.6	0x3cba	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Aug 3, 2021 19:25:10.466269970 CEST	8.8.8.8	192.168.2.6	0x3cba	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Aug 3, 2021 19:25:10.466269970 CEST	8.8.8.8	192.168.2.6	0x3cba	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 19:25:11.039252996 CEST	587	49751	208.91.198.143	192.168.2.6	220 us2.outbound.mailhostbox.com ESMTP Postfix
Aug 3, 2021 19:25:11.040591002 CEST	49751	587	192.168.2.6	208.91.198.143	EHLO 701188

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 19:25:11.189573050 CEST	587	49751	208.91.198.143	192.168.2.6	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
Aug 3, 2021 19:25:11.190965891 CEST	49751	587	192.168.2.6	208.91.198.143	AUTH login Y3NwdXJpQHNlYXJjaG5ldC5jby5pbg==
Aug 3, 2021 19:25:11.340886116 CEST	587	49751	208.91.198.143	192.168.2.6	334 UGFzc3dvcmQ6
Aug 3, 2021 19:25:11.494460106 CEST	587	49751	208.91.198.143	192.168.2.6	235 2.7.0 Authentication successful
Aug 3, 2021 19:25:11.495239973 CEST	49751	587	192.168.2.6	208.91.198.143	MAIL FROM:<cspuri@searchnet.co.in>
Aug 3, 2021 19:25:11.645086050 CEST	587	49751	208.91.198.143	192.168.2.6	250 2.1.0 Ok
Aug 3, 2021 19:25:11.645368099 CEST	49751	587	192.168.2.6	208.91.198.143	RCPT TO:<cspuri@searchnet.co.in>
Aug 3, 2021 19:25:11.802509069 CEST	587	49751	208.91.198.143	192.168.2.6	250 2.1.5 Ok
Aug 3, 2021 19:25:11.803154945 CEST	49751	587	192.168.2.6	208.91.198.143	DATA
Aug 3, 2021 19:25:11.952325106 CEST	587	49751	208.91.198.143	192.168.2.6	354 End data with <CR><LF>.<CR><LF>
Aug 3, 2021 19:25:11.954134941 CEST	49751	587	192.168.2.6	208.91.198.143	.
Aug 3, 2021 19:25:12.201294899 CEST	587	49751	208.91.198.143	192.168.2.6	250 2.0.0 Ok: queued as B1BA21C3171

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Purchase Order No.48743310321-RCN.pdf.exe PID: 6864 Parent PID: 6060

General

Start time:	19:23:07
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase Order No.48743310321-RCN.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order No.48743310321-RCN.pdf.exe'
Imagebase:	0x80000
File size:	1343488 bytes
MD5 hash:	2C32499D41CD6C7508ECD32F9A6C37CB
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: 00000000.00000002.372504988.00000000028F4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.372935866.0000000003579000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.372935866.0000000003579000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: Purchase Order No.48743310321-RCN.pdf.exe PID: 7084 Parent PID: 6864

General

Start time:	19:23:20
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase Order No.48743310321-RCN.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order No.48743310321-RCN.pdf.exe
Imagebase:	0xa50000
File size:	1343488 bytes
MD5 hash:	2C32499D41CD6C7508ECD32F9A6C37CB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.603264270.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.603264270.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.606298016.0000000002EE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis