ID: 433181
Sample Name: Recibo de banco.exe
Cookbook: default.jbs
Time: 12:22:22
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

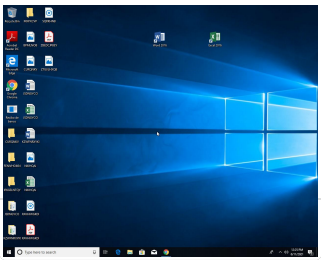
Analysis Report Recibo de banco.exe

Overview

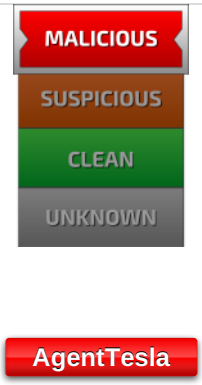
General Information

Sample Name:	Recibo de banco.exe
Analysis ID:	433181
MD5:	af6c540fc4f9468…
SHA1:	33ff91ac3c54b1c…
SHA256:	4d5d550925297c..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

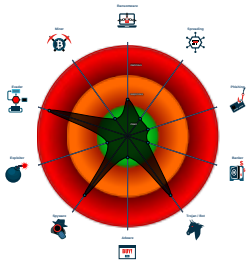


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia…
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- Recibo de banco.exe (PID: 6712 cmdline: 'C:\Users\user\Desktop\Recibo de banco.exe' MD5: AF6C540FC4F9468BA9C85D3DC8266171)
  - Recibo de banco.exe (PID: 7064 cmdline: C:\Users\user\Desktop\Recibo de banco.exe MD5: AF6C540FC4F9468BA9C85D3DC8266171)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "log1@ofilsysterns.comwgqYZDN3smtp.ofilsysterns.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.347288527.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.347288527.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.587665580.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.587665580.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.591218125.00000000028B1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 8 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Recibo de banco.exe.36a2520.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Recibo de banco.exe.36a2520.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.Recibo de banco.exe.36a2520.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Recibo de banco.exe.36a2520.1.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.2.Recibo de banco.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

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

Data Obfuscation:

.NET source code contains potential unpacker

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:

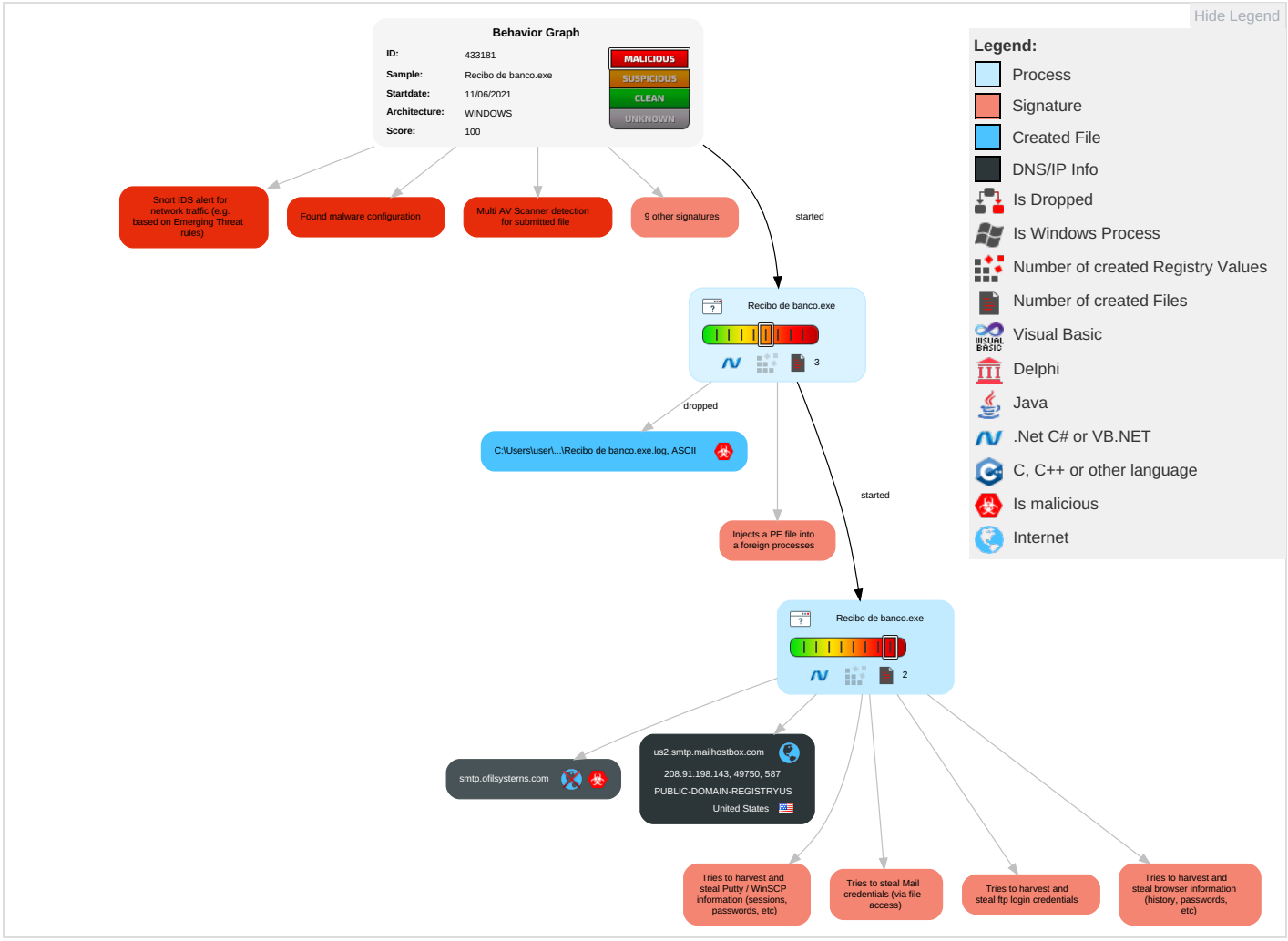
Yara detected AgentTesla

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 1 3	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
Recibo de banco.exe	31%	Virustotal		Browse
Recibo de banco.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.Recibo de banco.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.Recibo de banco.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	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnJ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlM	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.htmlN	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/96	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTCW9	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cncz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ana	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ana	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ana	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://smtp.ofilsysterns.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	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://www.sakkal.com	0%	URL Reputation	safe	
http://nBGXgB.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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://https://rg3WjDm06Kerhe.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comK	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.tiro.como	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.b4u	0%	Avira URL Cloud	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/on	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnva	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma96	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcze9x	0%	Avira URL Cloud	safe	
http://www.tiro.comym	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

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

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:	32.0.0 Black Diamond
Analysis ID:	433181
Start date:	11.06.2021
Start time:	12:22:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Recibo de banco.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:	22
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@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 94% • 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
12:23:27	API Interceptor	650x Sleep call for process: Recibo de banco.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	KC8ZMn81JC.exe	Get hash	malicious	Browse	
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	
	NEW ORDER 112888#.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	
	IFccIK78FD.exe	Get hash	malicious	Browse	
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	
	JK6UI6IKioPWJ6Y.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.832.15445.exe	Get hash	malicious	Browse	
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.MalPack.ADC.15816.exe	Get hash	malicious	Browse	
	nwJ0acvAY2.exe	Get hash	malicious	Browse	
	14dO9bGqKy.exe	Get hash	malicious	Browse	
	2sEHG8pTHtJcOxy.exe	Get hash	malicious	Browse	
	Scan copy proforma invoice_pdf.exe	Get hash	malicious	Browse	
	new order.exe	Get hash	malicious	Browse	
	S. Pools & Water Features Project List 2021.exe	Get hash	malicious	Browse	
	INVOICE FOR PAYMENT_pdf_____ _____.exe	Get hash	malicious	Browse	
	PeZvPwOtkW.exe	Get hash	malicious	Browse	
	PURCHASE ORDER-34002174,pdf.exe	Get hash	malicious	Browse	
	Urgent RFQ_AP65425652_032421,pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	KC8ZMn81JC.exe	Get hash	malicious	Browse	• 208.91.199.224
	Factura PO 1541973.exe	Get hash	malicious	Browse	• 208.91.199.223
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	NEW ORDER 112888#.exe	Get hash	malicious	Browse	• 208.91.199.224
	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	Get hash	malicious	Browse	• 208.91.199.223
	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	• 208.91.198.143
	lFccIK78FD.exe	Get hash	malicious	Browse	• 208.91.198.143
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	• 208.91.199.225
	JK6Ul6IKioPWJ6Y.exe	Get hash	malicious	Browse	• 208.91.198.143
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.832.15445.exe	Get hash	malicious	Browse	• 208.91.198.143
	order 4806125050.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Trojan.PackedNET.831.28325.exe	Get hash	malicious	Browse	• 208.91.199.225
	G8mumaTxk5kFdBG.exe	Get hash	malicious	Browse	• 208.91.198.143
	Trial order 20210609.exe	Get hash	malicious	Browse	• 208.91.199.224
	BP4w3lADAPfOKml.exe	Get hash	malicious	Browse	• 208.91.199.223
	4It7P3KCyYHUWHU.exe	Get hash	malicious	Browse	• 208.91.199.225
	PO -TXGU5022187.xlsx	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	KC8ZMn81JC.exe	Get hash	malicious	Browse	• 208.91.199.224
	audit-1133808478.xlsb	Get hash	malicious	Browse	• 43.225.55.182
	Factura PO 1541973.exe	Get hash	malicious	Browse	• 208.91.199.223
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	NEW ORDER 112888#.exe	Get hash	malicious	Browse	• 208.91.199.224
	oRSxZhDFLi.exe	Get hash	malicious	Browse	• 208.91.199.225
	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	Get hash	malicious	Browse	• 208.91.199.223
	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	• 208.91.199.223
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 207.174.212.247
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	• 208.91.198.143
	lFccIK78FD.exe	Get hash	malicious	Browse	• 208.91.198.143
	Order10 06 2021.doc	Get hash	malicious	Browse	• 162.215.241.145
	PO187439.exe	Get hash	malicious	Browse	• 119.18.54.126
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	• 208.91.199.225
	JK6Ul6IKioPWJ6Y.exe	Get hash	malicious	Browse	• 208.91.198.143
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.832.15445.exe	Get hash	malicious	Browse	• 208.91.198.143
	order 4806125050.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	Bank Swift.doc	Get hash	malicious	Browse	• 162.215.241.145

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Recibo de banco.exe.log	
Process:	C:\Users\user\Desktop\Recibo de banco.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.785964684882353
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:	Recibo de banco.exe
File size:	759296
MD5:	af6c540fc4f9468ba9c85d3dc8266171
SHA1:	33ff91ac3c54b1c0cecb6013c04c8bfc330b6104
SHA256:	4d5d550925297c38f8a922fd35998c7a2aa22227e60a3c28be010d1bc1dab4ac
SHA512:	a03696e06459c9d67f3aa6e6bb1733f2ff8eed2db61448ddd1920baea5e05f6dceedaead67beedcdf6733e322b9f611e5fea27602c5b2e025f6877fc5c611206
SSDEEP:	12288:YCCwh22XqxYM9ilfFKfffj9O9pOXjO8XGbSyG1FVbn4ESGvlqwEC7QtEXyPrZM4F:YCC0HacXjgbxGxbn4EBUCAqqNeBUdt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}..`.....P..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ba8d2
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:	0x60C1C57D [Thu Jun 10 07:55:41 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	0xb88d8	0xb8a00	False	0.84708631305	data	7.79563771234	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x688	0x800	False	0.34814453125	data	3.59798494936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	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
06/11/21-12:25:14.854528	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49750	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
Jun 11, 2021 12:25:11.592786074 CEST	192.168.2.6	8.8.8.8	0xd941	Standard query (0)	smtp.ofilsysterns.com	A (IP address)	IN (0x0001)
Jun 11, 2021 12:25:13.017577887 CEST	192.168.2.6	8.8.8.8	0xb350	Standard query (0)	smtp.ofilsysterns.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 12:25:11.782788038 CEST	8.8.8.8	192.168.2.6	0xd941	No error (0)	smtp.ofilsysterns.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 12:25:11.782788038 CEST	8.8.8.8	192.168.2.6	0xd941	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jun 11, 2021 12:25:11.782788038 CEST	8.8.8.8	192.168.2.6	0xd941	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 11, 2021 12:25:11.782788038 CEST	8.8.8.8	192.168.2.6	0xd941	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 11, 2021 12:25:11.782788038 CEST	8.8.8.8	192.168.2.6	0xd941	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jun 11, 2021 12:25:13.208748102 CEST	8.8.8.8	192.168.2.6	0xb350	No error (0)	smtp.ofilsysterns.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 12:25:13.208748102 CEST	8.8.8.8	192.168.2.6	0xb350	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 11, 2021 12:25:13.208748102 CEST	8.8.8.8	192.168.2.6	0xb350	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jun 11, 2021 12:25:13.208748102 CEST	8.8.8.8	192.168.2.6	0xb350	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 11, 2021 12:25:13.208748102 CEST	8.8.8.8	192.168.2.6	0xb350	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 12:25:13.757102966 CEST	587	49750	208.91.198.143	192.168.2.6	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jun 11, 2021 12:25:13.758383036 CEST	49750	587	192.168.2.6	208.91.198.143	EHLO 887849
Jun 11, 2021 12:25:13.934089899 CEST	587	49750	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
Jun 11, 2021 12:25:13.935868979 CEST	49750	587	192.168.2.6	208.91.198.143	AUTH login bG9nMUBvZmlsc3lzdGVybnMuY29t
Jun 11, 2021 12:25:14.113099098 CEST	587	49750	208.91.198.143	192.168.2.6	334 UGFzc3dvcmQ6
Jun 11, 2021 12:25:14.291471004 CEST	587	49750	208.91.198.143	192.168.2.6	235 2.7.0 Authentication successful
Jun 11, 2021 12:25:14.292757988 CEST	49750	587	192.168.2.6	208.91.198.143	MAIL FROM:<log1@ofilsysterns.com>
Jun 11, 2021 12:25:14.469207048 CEST	587	49750	208.91.198.143	192.168.2.6	250 2.1.0 Ok
Jun 11, 2021 12:25:14.469839096 CEST	49750	587	192.168.2.6	208.91.198.143	RCPT TO:<log1@ofilsysterns.com>
Jun 11, 2021 12:25:14.674042940 CEST	587	49750	208.91.198.143	192.168.2.6	250 2.1.5 Ok
Jun 11, 2021 12:25:14.674583912 CEST	49750	587	192.168.2.6	208.91.198.143	DATA
Jun 11, 2021 12:25:14.852303982 CEST	587	49750	208.91.198.143	192.168.2.6	354 End data with <CR><LF>.<CR><LF>
Jun 11, 2021 12:25:14.855771065 CEST	49750	587	192.168.2.6	208.91.198.143	.
Jun 11, 2021 12:25:15.133091927 CEST	587	49750	208.91.198.143	192.168.2.6	250 2.0.0 Ok: queued as 91FAE78218B

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Recibo de banco.exe PID: 6712 Parent PID: 6004

General

Start time:	12:23:17
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Recibo de banco.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Recibo de banco.exe'
Imagebase:	0x40000
File size:	759296 bytes
MD5 hash:	AF6C540FC4F9468BA9C85D3DC8266171
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: 00000001.00000002.353545264.00000000035F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.353545264.00000000035F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.353089246.0000000002634000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Recibo de banco.exe PID: 7064 Parent PID: 6712

General

Start time:	12:23:29
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Recibo de banco.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Recibo de banco.exe
Imagebase:	0x440000
File size:	759296 bytes
MD5 hash:	AF6C540FC4F9468BA9C85D3DC8266171
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: 00000005.00000000.347288527.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.347288527.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.587665580.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.587665580.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.591218125.00000000028B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.591218125.00000000028B1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis