ID: 531732
Sample Name: Purchase Order PO20211027STK.exe
Cookbook: default.jbs
Time: 10:05:34
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Purchase Order PO20211027STK.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection Evasion: 5
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 11
Static File Info 11
General 11
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Rich Headers 12
Data Directories 12
Sections 12
Resources 12
Imports 12
Possible Origin 12
Network Behavior 13
Snort IDS Alerts 13
Network Port Distribution 13
TCP Packets 13
UDP Packets 13
DNS Queries 13
DNS Answers 13
SMTP Packets 13
Code Manipulations 14
Statistics 14
Behavior 14

System Behavior 14
Analysis Process: Purchase Order PO20211027STK.exe PID: 4660 Parent PID: 7748 14
General 14
File Activities 14
File Created 14
File Written 14
File Read 14
Analysis Process: SPORENE.exe PID: 2100 Parent PID: 4660 14
General 15
File Activities 15
Analysis Process: CasPol.exe PID: 528 Parent PID: 2100 15
General 15
File Activities 15
File Created 15
File Written 15
File Read 15
Analysis Process: conhost.exe PID: 1720 Parent PID: 528 15
General 15
File Activities 16
Disassembly 16
Code Analysis 16

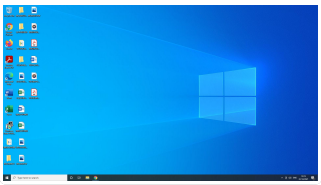
Windows Analysis Report Purchase Order PO20211027…

Overview

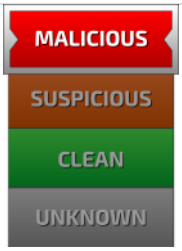
General Information

Sample Name:	Purchase Order PO20211027STK.exe
Analysis ID:	531732
MD5:	2f2102ec5776497.
SHA1:	1d3dd4ed88af22c.
SHA256:	7768da29cc4ef93..
Infos:	

Most interesting Screenshot:



Detection



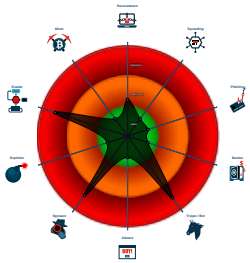
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- 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
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64native**
- Purchase Order PO20211027STK.exe (PID: 4660 cmdline: "C:\Users\user\Desktop\Purchase Order PO20211027STK.exe" MD5: 2F2102EC5776497950E89E419515EFEE)
  - SPORENE.exe (PID: 2100 cmdline: C:\Users\user\AppData\Local\Temp\SPORENE.exe MD5: 582A642DF36CDAC38982E4842F370B44)
    - CasPol.exe (PID: 528 cmdline: C:\Users\user\AppData\Local\Temp\SPORENE.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
      - conhost.exe (PID: 1720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "qualitat@construccionsjpallas.comzXHR1YDJL5smtp.construccionsjpallas.comfrankkeneth01@gmail.com"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://onedrive.live.com/download?cid=5A15FDA1AE98540B&r"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.214269025674.000000000F00000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000A.00000002.219015661495.000000001DF51000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.219015661495.000000001 DF51000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: CasPol.exe PID: 528	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: CasPol.exe PID: 528	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:

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

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)

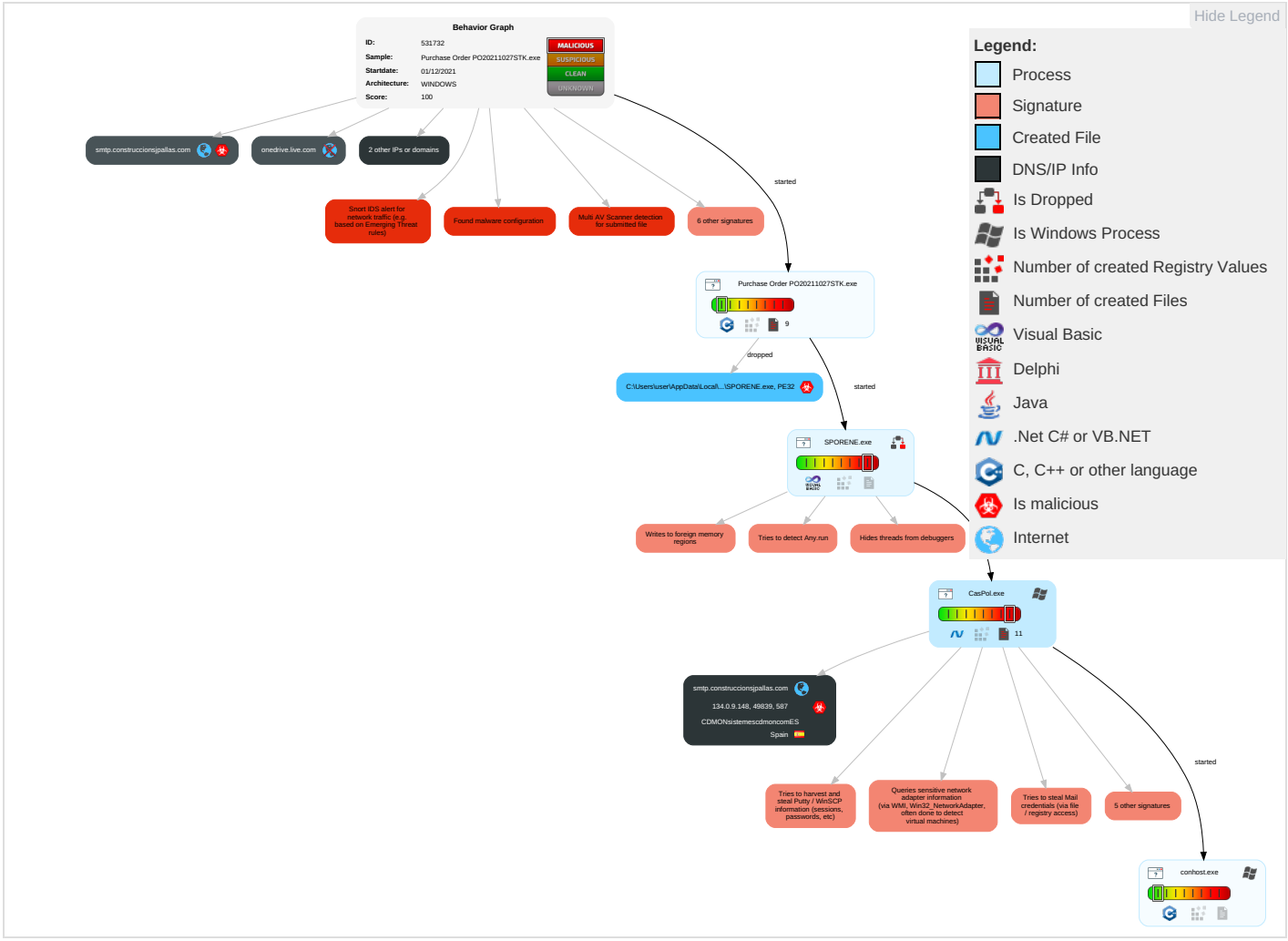
Remote Access Functionality:

- 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	Access Token Manipulation 1	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	Process Injection 1 1 2	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)	DLL Side-Loading 1	Access Token Manipulation 1	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)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Lay Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	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	System Information Discovery 1 1 7	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Use Port

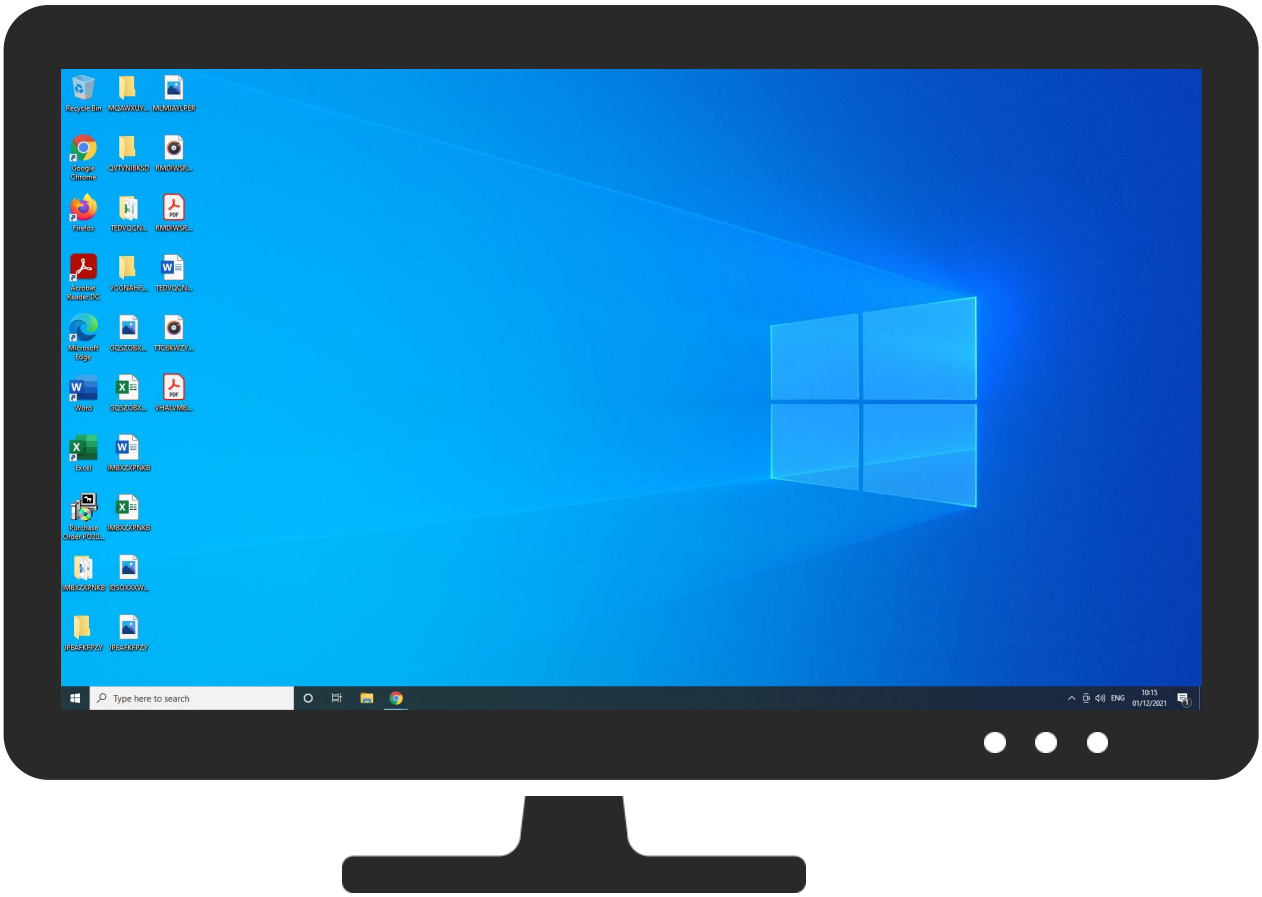
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Purchase Order PO20211027STK.exe	16%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\SPORENE.exe	9%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	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%	Virustotal		Browse
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://https://api.ipify.org%4	0%	Avira URL Cloud	safe	
http://smtp.construccionsjpallas.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	Avira URL Cloud	safe	
http://SukKLs.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://bBdyMHz8DHQmQ5qFFNz.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.construccionsjpallas.com	134.0.9.148	true	true		unknown
onedrive.live.com	unknown	unknown	false		high
ervtqq.bl.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=5A15FDA1AE98540B&r	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
134.0.9.148	smtp.construccionsjpallas.com	Spain		197712	CDMONsistemescdmoncomES	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531732
Start date:	01.12.2021
Start time:	10:05:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order PO20211027STK.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:	17
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@6/2@3/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 88% • 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
10:08:34	API Interceptor	2530x 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
CDMONsistemescdmoncomES	2YnVgiNH23	Get hash	malicious	Browse	• 46.16.59.125
	D3ccF8FfwAXrqsU.exe	Get hash	malicious	Browse	• 185.66.41.21
	EB94D7mept3gdSh.exe	Get hash	malicious	Browse	• 185.66.41.21
	aVzUZCHkko.exe	Get hash	malicious	Browse	• 185.66.41.201
	$RAULIU9.exe	Get hash	malicious	Browse	• 185.42.105.5
	3f52697f_by_Libranalysis.exe	Get hash	malicious	Browse	• 46.16.61.50
	0000000654.pdf.exe	Get hash	malicious	Browse	• 46.16.61.50
	0000000654.pdf.exe	Get hash	malicious	Browse	• 46.16.61.50
	ordine n#U00b0 276.exe	Get hash	malicious	Browse	• 46.16.61.250
	ordine n#U00b0 276.exe	Get hash	malicious	Browse	• 46.16.61.250
	a5FVSNazgr.exe	Get hash	malicious	Browse	• 46.16.61.250
	HdgnMEvcFK.exe	Get hash	malicious	Browse	• 46.16.61.250
	RTStyEQJpZ.exe	Get hash	malicious	Browse	• 46.16.61.250
	PAGO.xlsx	Get hash	malicious	Browse	• 46.16.61.250
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 46.16.61.250
	Zapytanie -20216470859302.exe	Get hash	malicious	Browse	• 46.16.61.250
	njGJ1eW44wshoMr.exe	Get hash	malicious	Browse	• 46.16.62.134
	3nG9LW7Z21dxUoM.exe	Get hash	malicious	Browse	• 46.16.62.134
	keeFDE9dhCGNNez.exe	Get hash	malicious	Browse	• 46.16.62.134
	74tF1foMeQyUMCh.exe	Get hash	malicious	Browse	• 46.16.62.134

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\SPORENE.exe	Purchase Order PO20211027STK.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\SPORENE.exe	
Process:	C:\Users\user\Desktop\Purchase Order PO20211027STK.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21321008
Entropy (8bit):	0.09325738133607682
Encrypted:	false
SSDEEP:	3072:mIXeoCC869BrI49jK9oUhJSSjfv8XEHPO:madlYoUZf2EvO
MD5:	582A642DF36CDAC38982E4842F370B44
SHA1:	3DD6D0CECD4CD9414D7DF148F7C46548C5709D62
SHA-256:	361DEDDF3E436753730DBB20842FBD6D1EF2EC27C56CD9DA99E87751C3BBE890
SHA-512:	E9C94417ACEF2B33DED79182C8B397E2693A74D290E78E286AE7576C998BF14F39F370C06BC40C9DFFDF2DE2E7F680AA0F33D74DB508E15EEAF1D31BE8D06E B6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 9%
Joe Sandbox View:	• Filename: Purchase Order PO20211027STK.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM.SM.SM..Q..RM..o.UM.ek.RM.RichSM.....PE..L.. ...5Y.....0C.....$.....@.....@E.....qE.....(.... ....C.....P@E.....0... ....text..... ..`.data...p.....@....rsrc.....C.. ... C.. .....@..@...I.....MSVBVM60.DLL..... ....

\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, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.060974988277113
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	Purchase Order PO20211027STK.exe
File size:	131031
MD5:	2f2102ec5776497950e89e419515efee
SHA1:	1d3dd4ed88af22c3de29c918b37db6f0b73c94c4
SHA256:	7768da29cc4ef93cb4790f664e139d1d8c2972e22fe8840 b6b86c50e15dba347
SHA512:	963b79cb63703ea6a6e8d70bbe76fadc660e10b801283a 3812a76f773ee36210171437794dad0b4ee11e8a2f3464 c88c7463526be03274ffdf48ec81823032a

General

SSDEEP:	3072:gbG7N2kDTHUpou4ubV4QviYqsYLQyI9xxsFIRO7c3fkA:gbE/HUjV4QviYJMQXyFIR2HA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 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:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0x11e0	0x1200	False	0.368489583333	data	4.48173978815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-10:10:01.566879	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49839	587	192.168.11.20	134.0.9.148

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 10:08:22.976635933 CET	192.168.11.20	1.1.1.1	0x5000	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:08:23.579670906 CET	192.168.11.20	1.1.1.1	0x7563	Standard query (0)	ervtqq.bl.files.1drv.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:09:59.463979959 CET	192.168.11.20	1.1.1.1	0xcb15	Standard query (0)	smtp.construccionsjpallas.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:08:22.986366987 CET	1.1.1.1	192.168.11.20	0x5000	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:08:23.766315937 CET	1.1.1.1	192.168.11.20	0x7563	No error (0)	ervtqq.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:08:23.766315937 CET	1.1.1.1	192.168.11.20	0x7563	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:09:59.481276035 CET	1.1.1.1	192.168.11.20	0xcb15	No error (0)	smtp.construccionsjpallas.com		134.0.9.148	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 1, 2021 10:10:01.376899004 CET	587	49839	134.0.9.148	192.168.11.20	220 vxade-59.srv.cat ESMTP
Dec 1, 2021 10:10:01.377335072 CET	49839	587	192.168.11.20	134.0.9.148	EHLO 374653
Dec 1, 2021 10:10:01.405833960 CET	587	49839	134.0.9.148	192.168.11.20	250-vxade-59.srv.cat 250-PIPELINING 250-SIZE 47185920 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN CRAM-MD5 DIGEST-MD5 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Dec 1, 2021 10:10:01.407454014 CET	49839	587	192.168.11.20	134.0.9.148	AUTH login cXVhbGl0YXRAY29uc3RydWNjaW9uc2pwYWxsYXMuY29t

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 1, 2021 10:10:01.436321020 CET	587	49839	134.0.9.148	192.168.11.20	334 UGFzc3dvcmQ6
Dec 1, 2021 10:10:01.468705893 CET	587	49839	134.0.9.148	192.168.11.20	235 2.7.0 Authentication successful
Dec 1, 2021 10:10:01.469347954 CET	49839	587	192.168.11.20	134.0.9.148	MAIL FROM:<qualitat@construccionsjpallas.com>
Dec 1, 2021 10:10:01.501142979 CET	587	49839	134.0.9.148	192.168.11.20	250 2.1.0 Ok
Dec 1, 2021 10:10:01.501499891 CET	49839	587	192.168.11.20	134.0.9.148	RCPT TO:<frankkeneth01@gmail.com>
Dec 1, 2021 10:10:01.535028934 CET	587	49839	134.0.9.148	192.168.11.20	250 2.1.5 Ok
Dec 1, 2021 10:10:01.535347939 CET	49839	587	192.168.11.20	134.0.9.148	DATA
Dec 1, 2021 10:10:01.565152884 CET	587	49839	134.0.9.148	192.168.11.20	354 End data with <CR><LF>.<CR><LF>
Dec 1, 2021 10:10:01.566984892 CET	49839	587	192.168.11.20	134.0.9.148	.
Dec 1, 2021 10:10:01.708368063 CET	587	49839	134.0.9.148	192.168.11.20	250 2.0.0 Ok: queued as 7F0F42130D
Dec 1, 2021 10:11:39.499531984 CET	49839	587	192.168.11.20	134.0.9.148	QUIT
Dec 1, 2021 10:11:39.529752016 CET	587	49839	134.0.9.148	192.168.11.20	221 2.0.0 Bye

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Purchase Order PO20211027STK.exe PID: 4660 Parent PID: 7748

General

Start time:	10:07:25
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\Purchase Order PO20211027STK.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase Order PO20211027STK.exe"
Imagebase:	0x400000
File size:	131031 bytes
MD5 hash:	2F2102EC5776497950E89E419515EFEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: SPORENE.exe PID: 2100 Parent PID: 4660

General

Start time:	10:07:27
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\SPORENE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\SPORENE.exe
Imagebase:	0x400000
File size:	21321008 bytes
MD5 hash:	582A642DF36CDAC38982E4842F370B44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 9%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: CasPol.exe PID: 528 Parent PID: 2100

General

Start time:	10:07:55
Start date:	01/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\SPORENE.exe
Imagebase:	0xa80000
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_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000A.00000000.214269025674.0000000000F00000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.219015661495.000000001DF51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.219015661495.000000001DF51000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 1720 Parent PID: 528

General

Start time:	10:07:56
Start date:	01/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6a3780000
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