ID: 323806
Sample Name: Mixtec New Order And Price List Requsting Form_pdf.exe
Cookbook: default.jbs
Time: 15:22:06
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

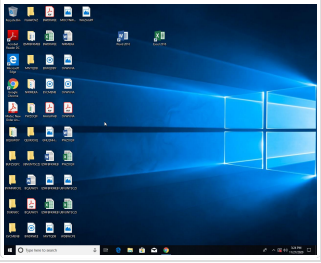
Analysis Report Mixtec New Order And Price List Requs…

Overview

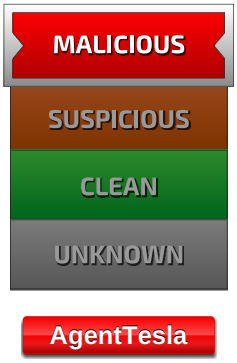
General Information

Sample Name:	Mixtec New Order And Price List Requsting Form_pdf.exe
Analysis ID:	323806
MD5:	efab4797e8f0bd0..
SHA1:	4020126b35149fa.
SHA256:	961945f660c7884.
Tags:	exe

Most interesting Screenshot:



Detection

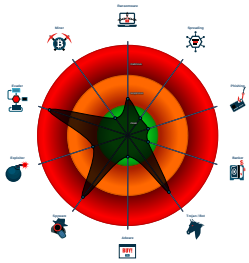


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Icon mismatch, binary includes an ic…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- Mixtec New Order And Price List Requsting Form_pdf.exe (PID: 4680 cmdline: 'C:\Users\user\Desktop\Mixtec New Order And Price List Requsting Form_pdf.exe' MD5: EFAB4797E8F0BD00F13D6303B9875CA9)
  - Mixtec New Order And Price List Requsting Form_pdf.exe (PID: 6008 cmdline: C:\Users\user\Desktop\Mixtec New Order And Price List Requsting Form_pdf.exe MD5: EFAB4797E8F0BD00F13D6303B9875CA9)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.674943529.0000000002E11000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.914822411.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.677332059.0000000003E9D000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.674981503.0000000002E58000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.916693049.0000000002EB1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 5 entries

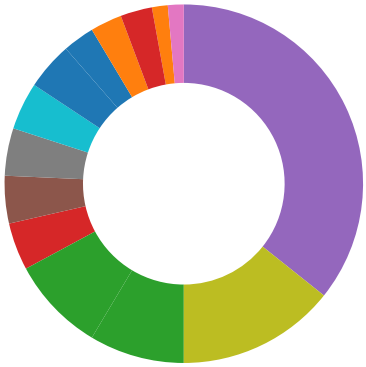
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Mixtec New Order And Price List Requsting Form _pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- 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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Uses the Telegram API (likely for C&C communication)

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

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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)

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)

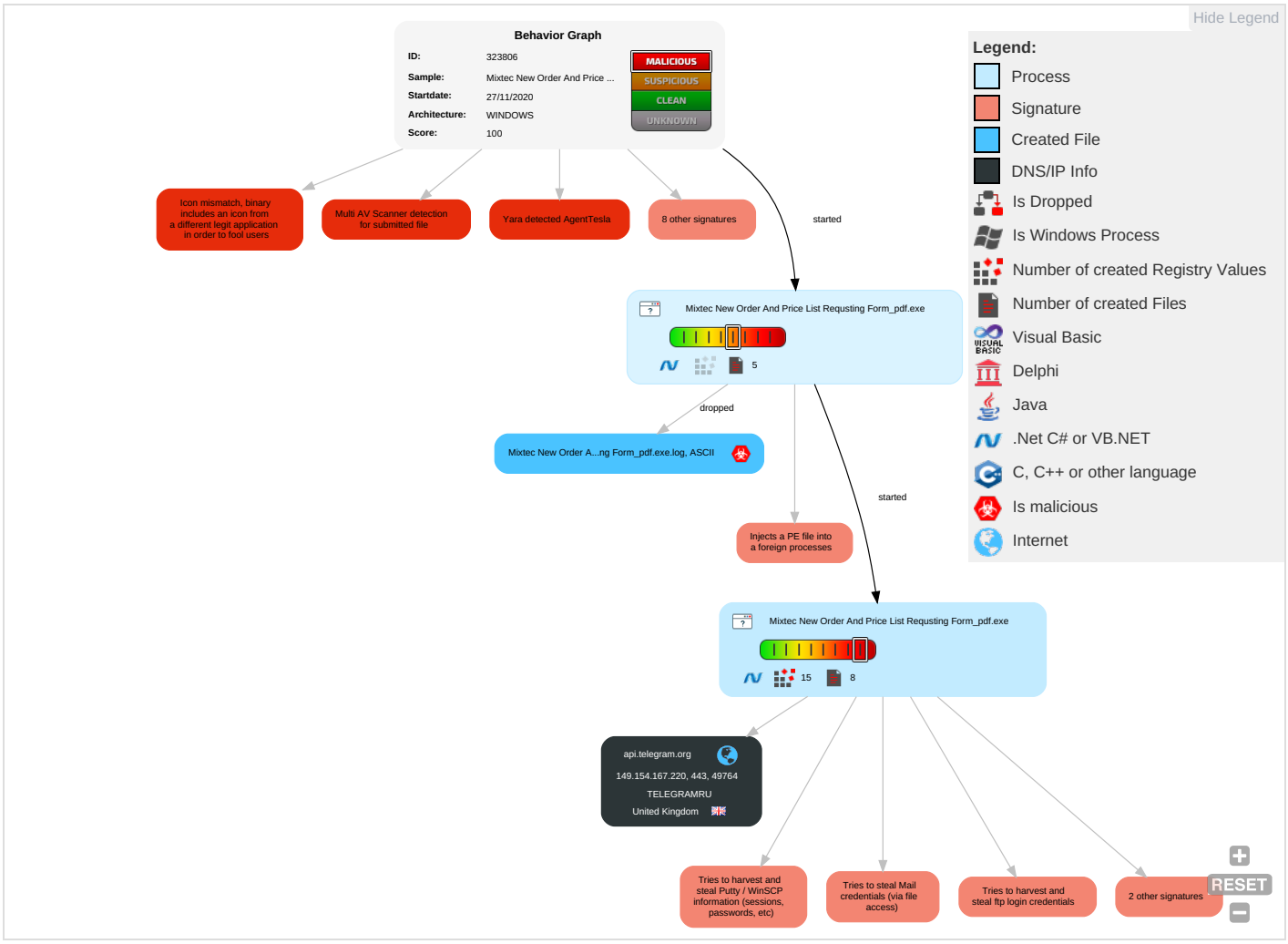
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	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	Web Serv
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 1 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Enc Cha
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non App Laye Prot
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Virtualization/Sandbox Evasion 1 3	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	App Laye Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Falll Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mult Com
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Use
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	App Laye

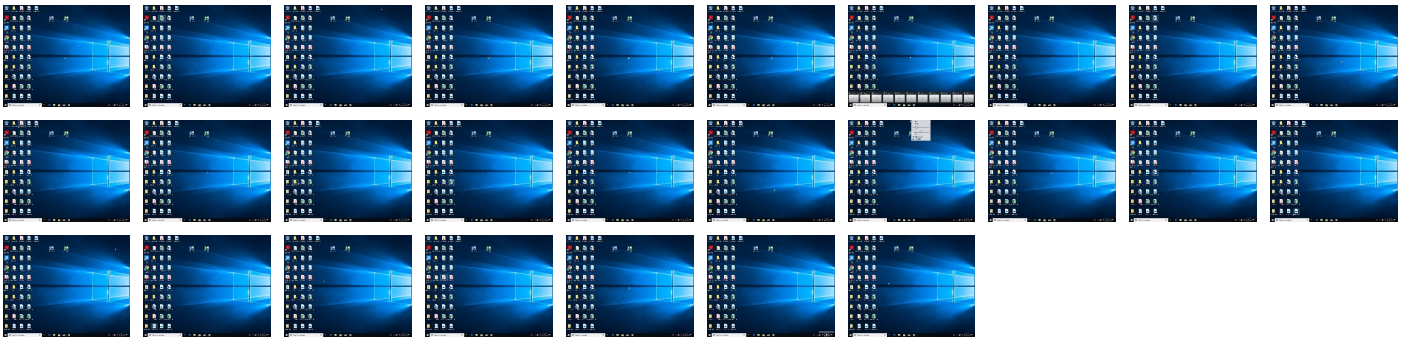
Behavior Graph



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
Mixtec New Order And Price List Requsting Form_pdf.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Mixtec New Order And Price List Requsting Form_pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://p88gKnqaJsC65fXB.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	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://api.telegram.orgx&	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://HIScld.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

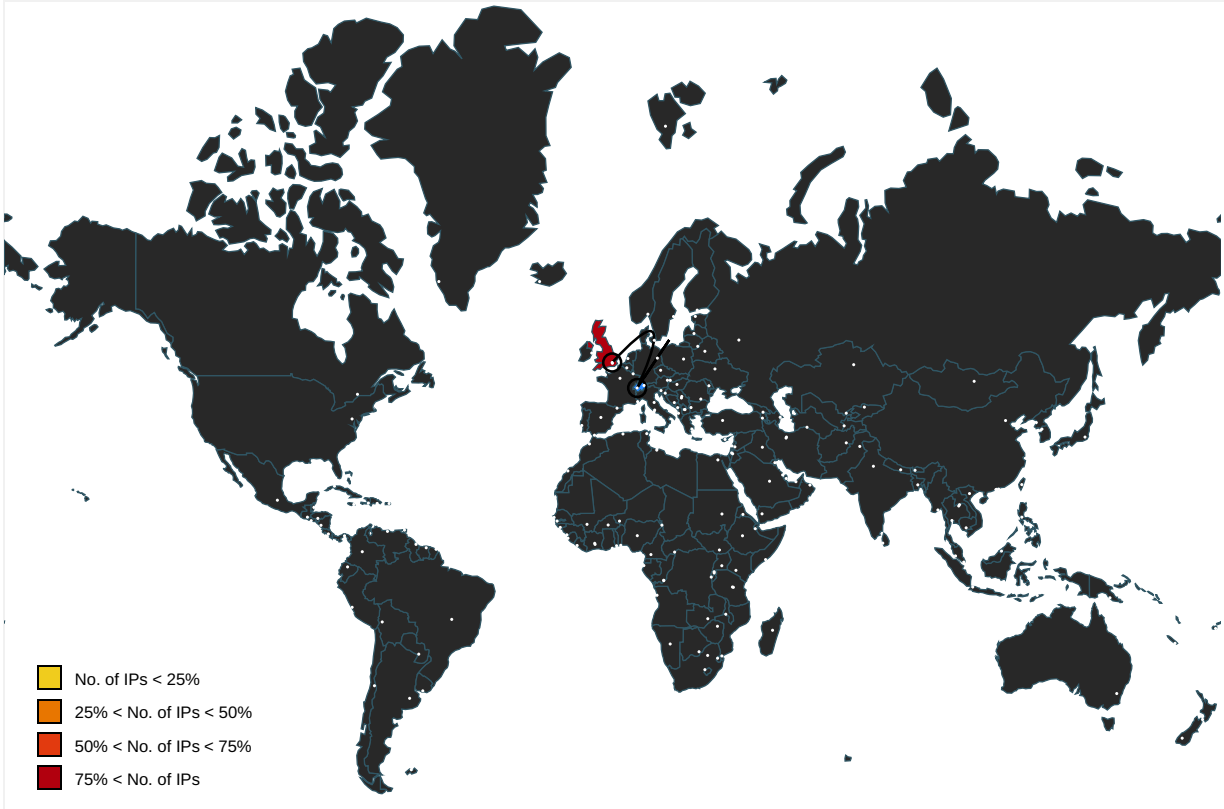
Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.godaddy.com/gdroot-g2.crl0F	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.917110372.000000 0002FD3000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.916693049.000000 0002EB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.916693049.000000 0002EB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.917047288.000000 0002F9B000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.916693049.000000 0002EB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.godaddy.com/repository/0	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.917110372.000000 0002FD3000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot1383627647:AAFPZ_rXJwpP1cKfEFo3ihYu1fzqORkFnc8/sendDocument	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.917047288.000000 0002F9B000.00000004.00000001.sdmp	false		high
http://certs.godaddy.com/repository/1301	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.917110372.000000 0002FD3000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot1383627647:AAFPZ_rXJwpP1cKfEFo3ihYu1fzqORkFnc8/	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000000.00000002.677332059.000000 0003E9D000.00000004.00000001.sdmp, Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.914822411.0000000000402000.00000040.00000001.sdmp	false		high
http://crl.godaddy.com/gdroot.crl0F	Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.917110372.000000 0002FD3000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://p88gKnqaJsC65fXB.com	Mixtec New Order And Price List Requsting Form_pdf.exe, 0000 0001.00000002.916693049.000000 0002EB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.godaddy.com/gdig2s1-1823.crl0	Mixtec New Order And Price List Requsting Form_pdf.exe, 0000 0001.00000002.917110372.000000 0002FD3000.00000004.00000001.sdmp	false		high
http://https://certs.godaddy.com/repository/0	Mixtec New Order And Price List Requsting Form_pdf.exe, 0000 0001.00000002.917110372.000000 0002FD3000.00000004.00000001.sdmp	false		high
http://certificates.godaddy.com/repository/gdig2.crt0	Mixtec New Order And Price List Requsting Form_pdf.exe, 0000 0001.00000002.917110372.000000 0002FD3000.00000004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Mixtec New Order And Price List Requsting Form_pdf.exe, 0000 0000.00000002.677332059.000000 0003E9D000.00000004.00000001.sdmp, Mixtec New Order And Price List Requsting Form_pdf.exe, 00000001.00000002.914822411.000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.orgx&	Mixtec New Order And Price List Requsting Form_pdf.exe, 0000 0001.00000002.917047288.000000 0002F9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.orgGETMozilla/5.0	Mixtec New Order And Price List Requsting Form_pdf.exe, 0000 0001.00000002.916693049.000000 0002EB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://HIScld.com	Mixtec New Order And Price List Requsting Form_pdf.exe, 0000 0001.00000002.916693049.000000 0002EB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://api.telegram.org/bot1383627647:AAFPZ_rXJwpP1cKfEFo3ihYu1fzqORkFnc8/sendDocumentdocument-----	Mixtec New Order And Price List Requsting Form_pdf.exe, 0000 0001.00000002.916693049.000000 0002EB1000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	unknown	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323806
Start date:	27.11.2020
Start time:	15:22:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Mixtec New Order And Price List Requsting Form_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:	13
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@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 63% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 98% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 40.88.32.150, 51.104.139.180, 104.42.151.234, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.104.144.132 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/323806/sample/Mixtec New Order And Price List Requsting Form_pdf.exe

Simulations

Behavior and APIs

Time	Type	Description
15:23:05	API Interceptor	609x Sleep call for process: Mixtec New Order And Price List Requsting Form_pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	SecuriteInfo.com.Trojan.PackedNET.469.31999.exe	Get hash	malicious	Browse	
	RFQ URGENT NEW ORDER#001_XLS.EXE	Get hash	malicious	Browse	
	PO#MT20-0582.exe	Get hash	malicious	Browse	
	Urgent Requesting For Quotation And Samples _pdf.exe	Get hash	malicious	Browse	
	TOOL.exe	Get hash	malicious	Browse	
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	
	kiiDjfpu2x.exe	Get hash	malicious	Browse	
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	
	A payment from Blue Wing Limited is coming your way_pdf.exe	Get hash	malicious	Browse	
	List Of Orders.exe	Get hash	malicious	Browse	
	Payment Proof.exe	Get hash	malicious	Browse	
	Rosato Trading Impex Ltd Company Profile And Proposals_pdf.exe	Get hash	malicious	Browse	
	aMrIsacjClGbmOJ.exe	Get hash	malicious	Browse	
	Request For Quotation for Supply of Promotional Items_pdf.exe	Get hash	malicious	Browse	
	57lZU9zR2o.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5dmLKUQ1l8.exe	Get hash	malicious	Browse	
	wzeuo83tK6.exe	Get hash	malicious	Browse	
	M7RcGGAR4D.exe	Get hash	malicious	Browse	
	d6MeQBxbJl.exe	Get hash	malicious	Browse	
	ALVA TRADERS REQUEST FOR QUOTATION RFQ NOVEMBER 2020_pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	SecuriteInfo.com.Trojan.PackedNET.469.31999.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ URGENT NEW ORDER#001_XLS.EXE	Get hash	malicious	Browse	• 149.154.167.220
	PO#MT20-0582.exe	Get hash	malicious	Browse	• 149.154.167.220
	Urgent Requesting For Quotation And Samples _pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	TOOL.exe	Get hash	malicious	Browse	• 149.154.167.220
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 149.154.167.220
	kiiDjfpu2x.exe	Get hash	malicious	Browse	• 149.154.167.220
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	List Of Orders.exe	Get hash	malicious	Browse	• 149.154.167.220
	Payment Proof.exe	Get hash	malicious	Browse	• 149.154.167.220
	Rosato Trading Impex Ltd Company Profile And Proposals_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	aMrIsacjClGbmOJ.exe	Get hash	malicious	Browse	• 149.154.167.220
	Request For Quotation for Supply of Promotional Items_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	57lZU9zR2o.exe	Get hash	malicious	Browse	• 149.154.167.220
	5dmLKUQ1l8.exe	Get hash	malicious	Browse	• 149.154.167.220
	wzeuo83tK6.exe	Get hash	malicious	Browse	• 149.154.167.220
	M7RcGGAR4D.exe	Get hash	malicious	Browse	• 149.154.167.220
	d6MeQBxbJl.exe	Get hash	malicious	Browse	• 149.154.167.220
	ALVA TRADERS REQUEST FOR QUOTATION RFQ NOVEMBER 2020_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO Lists.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	SecuriteInfo.com.Trojan.PackedNET.469.31999.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ URGENT NEW ORDER#001_XLS.EXE	Get hash	malicious	Browse	• 149.154.167.220
	PO#MT20-0582.exe	Get hash	malicious	Browse	• 149.154.167.220
	Urgent Requesting For Quotation And Samples _pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	TOOL.exe	Get hash	malicious	Browse	• 149.154.167.220
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 149.154.167.220
	kiiDjfpu2x.exe	Get hash	malicious	Browse	• 149.154.167.220
	http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php	Get hash	malicious	Browse	• 149.154.167.99
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	A payment from Blue Wing Limited is coming your way_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	List Of Orders.exe	Get hash	malicious	Browse	• 149.154.167.220
	Payment Proof.exe	Get hash	malicious	Browse	• 149.154.167.220
	Rosato Trading Impex Ltd Company Profile And Proposals_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	aMrIsacjClGbmOJ.exe	Get hash	malicious	Browse	• 149.154.167.220
	Request For Quotation for Supply of Promotional Items_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	57lZU9zR2o.exe	Get hash	malicious	Browse	• 149.154.167.220
	5dmLKUQ1l8.exe	Get hash	malicious	Browse	• 149.154.167.220
	wzeuo83tK6.exe	Get hash	malicious	Browse	• 149.154.167.220
	M7RcGGAR4D.exe	Get hash	malicious	Browse	• 149.154.167.220
	d6MeQBxbJl.exe	Get hash	malicious	Browse	• 149.154.167.220

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 149.154.167.220
	guy1.exe	Get hash	malicious	Browse	• 149.154.167.220
	guy2.exe	Get hash	malicious	Browse	• 149.154.167.220
	Exodus.exe	Get hash	malicious	Browse	• 149.154.167.220
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	#A06578987.xlsm	Get hash	malicious	Browse	• 149.154.167.220
	Order 51897.exe	Get hash	malicious	Browse	• 149.154.167.220
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	98650107.pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 149.154.167.220
	Izezma64.dll	Get hash	malicious	Browse	• 149.154.167.220
	fuxenm32.dll	Get hash	malicious	Browse	• 149.154.167.220
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 149.154.167.220
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 149.154.167.220
	ER mexico.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28272.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.BackDoor.SpyBotNET.25.6057.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.ArtemisTrojan.exe	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Mixtec New Order And Price List Requsting Form_pdf.exe.log	
Process:	C:\Users\user\Desktop\Mixtec New Order And Price List Requsting Form_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EEFF
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

C:\Users\user\AppData\Roaming\bj2ger30.nli\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Mixtec New Order And Price List Requsting Form_pdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
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):	7.252382148970084
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:	Mixtec New Order And Price List Requsting Form_pdf.exe
File size:	820224
MD5:	efab4797e8f0bd00f13d6303b9875ca9
SHA1:	4020126b35149fafa6447dbdfd3183a5d9c35dc8
SHA256:	961945f660c788431e4da67d6e3730ab4e3283979ad8d67df4c4bcdcb4a9f6e0

General

SHA512:	02ae0a107ba3de2d8b42238efef115fc0f8e8c5dac4935fe8456f31229dc4d43dbf4eddb5683448c8d25f71a2a6120bfa3bae85024838f78c7fcb91e57e3b284
SSDEEP:	12288:xpix4SQSY88WFKNbj8VlAW3CpQuoJtta+66K3S5zPvEKdAA:x85QSYbEKNbj6iDIto+ES5LvEYA
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...7u._..............P.................. ... .@.. ....@................................

File Icon

Icon Hash:	6eecccccd6d2f2f2

Static PE Info

General

Entrypoint:	0x4b12e6
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:	0x5FBF7537 [Thu Nov 26 09:28:23 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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 [00402000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb1294	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb2000	0x18b20	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xcc000	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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xaf2ec	0xaf400	False	0.739544790924	data	7.36789714747	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb2000	0x18b20	0x18c00	False	0.145369712753	data	4.30181145694	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xcc000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb21a8	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb4750	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb57f8	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xb5c60	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb9e88	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xca6b0	0x4c	data		
RT_VERSION	0xca6fc	0x424	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

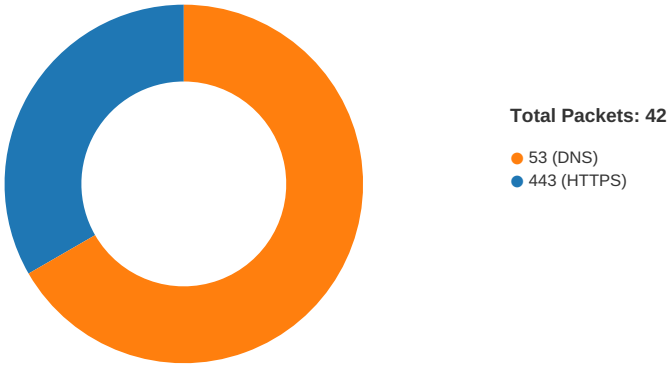
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Token Software 2014 - 2020 (GNU GPL)

Description	Data
Assembly Version	1.0.0.0
InternalName	Lvzz.exe
FileVersion	1.0.0.0
CompanyName	Token Softwares
LegalTrademarks	
Comments	Manages the creation and activation of profiles in the X3 games created by Egosoft.
ProductName	Profile Manager
ProductVersion	1.0.0.0
FileDescription	Profile Manager
OriginalFilename	Lvzz.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:24:39.459635973 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.485847950 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.486130953 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.529746056 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.555977106 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.558221102 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.558284044 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.558326960 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.558357954 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.558495998 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.558640957 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.559365988 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.559397936 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.559514999 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.564354897 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.591655016 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.634963989 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.683909893 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.710134029 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:39.712035894 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:39.785216093 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:40.094177961 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:40.150559902 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:40.341192961 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:40.367254972 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:40.367285967 CET	443	49764	149.154.167.220	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:24:40.368422031 CET	49764	443	192.168.2.4	149.154.167.220
Nov 27, 2020 15:24:40.394510031 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:40.663216114 CET	443	49764	149.154.167.220	192.168.2.4
Nov 27, 2020 15:24:40.713143110 CET	49764	443	192.168.2.4	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:22:50.262288094 CET	53	63153	8.8.8.8	192.168.2.4
Nov 27, 2020 15:22:50.895369053 CET	52991	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:22:50.933079004 CET	53	52991	8.8.8.8	192.168.2.4
Nov 27, 2020 15:22:51.604521990 CET	53700	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:22:51.631544113 CET	53	53700	8.8.8.8	192.168.2.4
Nov 27, 2020 15:22:52.298070908 CET	51726	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:22:52.333729982 CET	53	51726	8.8.8.8	192.168.2.4
Nov 27, 2020 15:22:53.361721992 CET	56794	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:22:53.397445917 CET	53	56794	8.8.8.8	192.168.2.4
Nov 27, 2020 15:22:54.119982004 CET	56534	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:22:54.147253036 CET	53	56534	8.8.8.8	192.168.2.4
Nov 27, 2020 15:22:55.027089119 CET	56627	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:22:55.054198027 CET	53	56627	8.8.8.8	192.168.2.4
Nov 27, 2020 15:22:55.895437002 CET	56621	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:22:55.922679901 CET	53	56621	8.8.8.8	192.168.2.4
Nov 27, 2020 15:22:56.722337008 CET	63116	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:22:56.749411106 CET	53	63116	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:15.291197062 CET	64078	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:15.318430901 CET	53	64078	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:27.540543079 CET	64801	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:27.576241970 CET	53	64801	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:30.826165915 CET	61721	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:30.853243113 CET	53	61721	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:32.863733053 CET	51255	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:32.890868902 CET	53	51255	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:34.683542013 CET	61522	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:34.724205971 CET	53	61522	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:35.626945972 CET	52337	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:35.654254913 CET	53	52337	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:36.158838034 CET	55046	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:36.194300890 CET	53	55046	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:36.682311058 CET	49612	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:36.718034983 CET	53	49612	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:37.042001963 CET	49285	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:37.077581882 CET	53	49285	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:37.512676954 CET	50601	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:37.548232079 CET	53	50601	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:37.718394041 CET	60875	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:37.762166977 CET	53	60875	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:37.937123060 CET	56448	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:37.972867966 CET	53	56448	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:38.394171000 CET	59172	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:38.421222925 CET	53	59172	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:38.993247986 CET	62420	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:39.020297050 CET	53	62420	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:39.661814928 CET	60579	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:39.689001083 CET	53	60579	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:40.008387089 CET	50183	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:40.043953896 CET	53	50183	8.8.8.8	192.168.2.4
Nov 27, 2020 15:23:57.156949043 CET	61531	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:23:57.193651915 CET	53	61531	8.8.8.8	192.168.2.4
Nov 27, 2020 15:24:30.108196020 CET	49228	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:24:30.135262012 CET	53	49228	8.8.8.8	192.168.2.4
Nov 27, 2020 15:24:31.672214031 CET	59794	53	192.168.2.4	8.8.8.8
Nov 27, 2020 15:24:31.715881109 CET	53	59794	8.8.8.8	192.168.2.4
Nov 27, 2020 15:24:39.405692101 CET	55916	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:24:39.432935953 CET	53	55916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:24:39.405692101 CET	192.168.2.4	8.8.8.8	0xfe03	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:24:39.432935953 CET	8.8.8.8	192.168.2.4	0xfe03	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

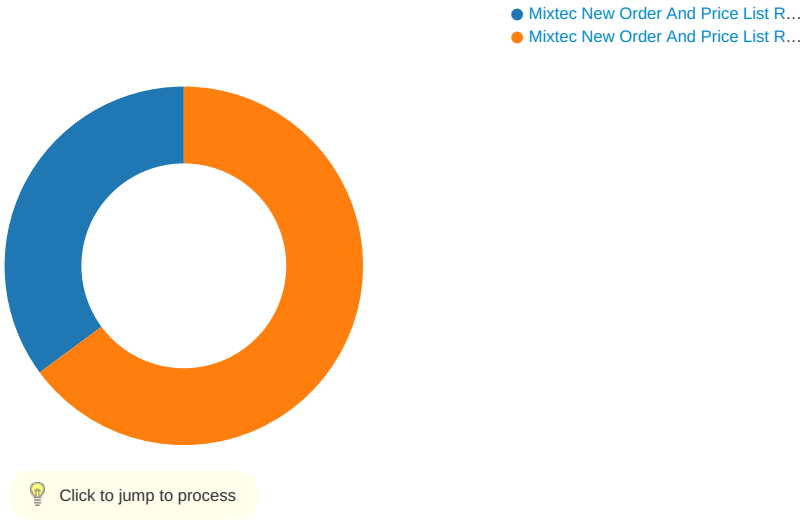
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 15:24:39.559365988 CET	149.154.167.220	443	192.168.2.4	49764	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Mixtec New Order And Price List Requsting Form_pdf.exe PID: 4680 Parent PID: 5964

General

Start time:	15:22:55
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\Mixtec New Order And Price List Requsting Form_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Mixtec New Order And Price List Requsting Form_pdf.exe'
Imagebase:	0x770000
File size:	820224 bytes
MD5 hash:	EFAB4797E8F0BD00F13D6303B9875CA9
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: 00000000.00000002.674943529.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.677332059.0000000003E9D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.674981503.0000000002E58000.00000004.00000001.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	722760AC	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	722760AC	unknown

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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Mixtec New Order And Price List Requsting Form_pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Mixtec New Order And Price List Requsting Form_pdf.exe.log	unknown	916	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7254A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5010093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5010093	ReadFile

Analysis Process: Mixtec New Order And Price List Requsting Form_pdf.exe PID: 6008 Parent PID: 4680

General

Start time:	15:23:06
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\Mixtec New Order And Price List Requsting Form_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Mixtec New Order And Price List Requsting Form_pdf.exe
Imagebase:	0x7c0000
File size:	820224 bytes
MD5 hash:	EFAB4797E8F0BD00F13D6303B9875CA9
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: 00000001.00000002.914822411.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.916693049.0000000002EB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.916693049.0000000002EB1000.00000004.00000001.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	722760AC	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	722760AC	unknown
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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Roaming\bj2ger30.nli	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5914FC9	CreateDirectoryW
C:\Users\user\AppData\Roaming\bj2ger30.nli\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	5914FC9	CreateDirectoryW
C:\Users\user\AppData\Roaming\bj2ger30.nli\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	5914FC9	CreateDirectoryW
C:\Users\user\AppData\Roaming\bj2ger30.nli\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	591508C	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bj2ger30.nli\Chrome\Default\Cookies	success or wait	1	5915146	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bj2ger30.nli\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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	591508C	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5911357	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ff35166b-811f-42b5-a80e-64f28b3742d5	unknown	4096	success or wait	1	5911357	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5911357	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5911357	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5911357	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5911357	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5911357	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5911357	ReadFile
C:\Users\user\AppData\Roaming\bj2ger30.nli\Chrome\Default\Cookies	unknown	16384	success or wait	2	5911357	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis