ID: 358189
Sample Name: Purchase order.exe
Cookbook: default.jbs
Time: 07:44:44
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

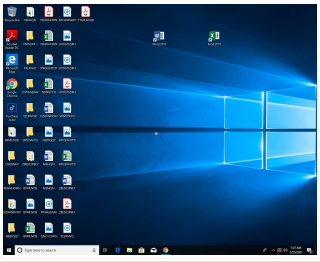
Analysis Report Purchase order.exe

Overview

General Information

Sample Name:	Purchase order.exe
Analysis ID:	358189
MD5:	98be4d3bb20538..
SHA1:	8919195923883f3.
SHA256:	df61b9c866c5ceb..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

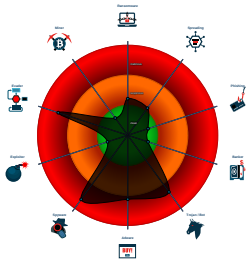
AgentTesla

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

Signatures

- Multi AV Scanner detection for dropp…
- Yara detected AgentTesla
- .NET source code contains very larg…
- Bypasses PowerShell execution pol…
- Contains functionality to log keystro…
- Drops PE files to the startup folder
- Initial sample is a PE file and has a …
- Installs a global keyboard hook
- Powershell drops PE file
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…

Classification



Startup

- **System is w10x64**
- Purchase order.exe (PID: 7072 cmdline: 'C:\Users\user\Desktop\Purchase order.exe' MD5: 98BE4D3BB2053810801FADEB32884ACD)
  - powershell.exe (PID: 7128 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\Purchase order.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase order.exe (PID: 5132 cmdline: C:\Users\user\Desktop\Purchase order.exe MD5: 98BE4D3BB2053810801FADEB32884ACD)
  - Purchase order.exe (PID: 2040 cmdline: C:\Users\user\Desktop\Purchase order.exe MD5: 98BE4D3BB2053810801FADEB32884ACD)
- Drivers.exe (PID: 5988 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' MD5: 98BE4D3BB2053810801FADEB32884ACD)
  - powershell.exe (PID: 7032 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Drivers.exe (PID: 4924 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe MD5: 98BE4D3BB2053810801FADEB32884ACD)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.337349475.00000000057B0000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
00000002.00000002.334741254.00000000040B9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.334741254.00000000040B9000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	

Source	Rule	Description	Author	Strings
00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 17 entries				

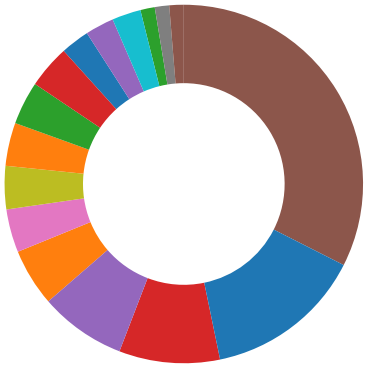
Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.Drivers.exe.4b20000.7.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
11.2.Drivers.exe.358f940.3.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
2.2.Purchase order.exe.42223b8.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.Drivers.exe.4b20000.7.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
2.2.Purchase order.exe.411f940.3.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 17 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Compliance:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to log keystrokes (.Net Source)

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Powershell drops PE file

Data Obfuscation:

Yara detected Beds Obfuscator

Boot Survival:

Drops PE files to the startup folder

Malware Analysis System Evasion:

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

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

Yara detected Beds Obfuscator

HIPS / PFW / Operating System Protection Evasion:

Bypasses PowerShell execution policy

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

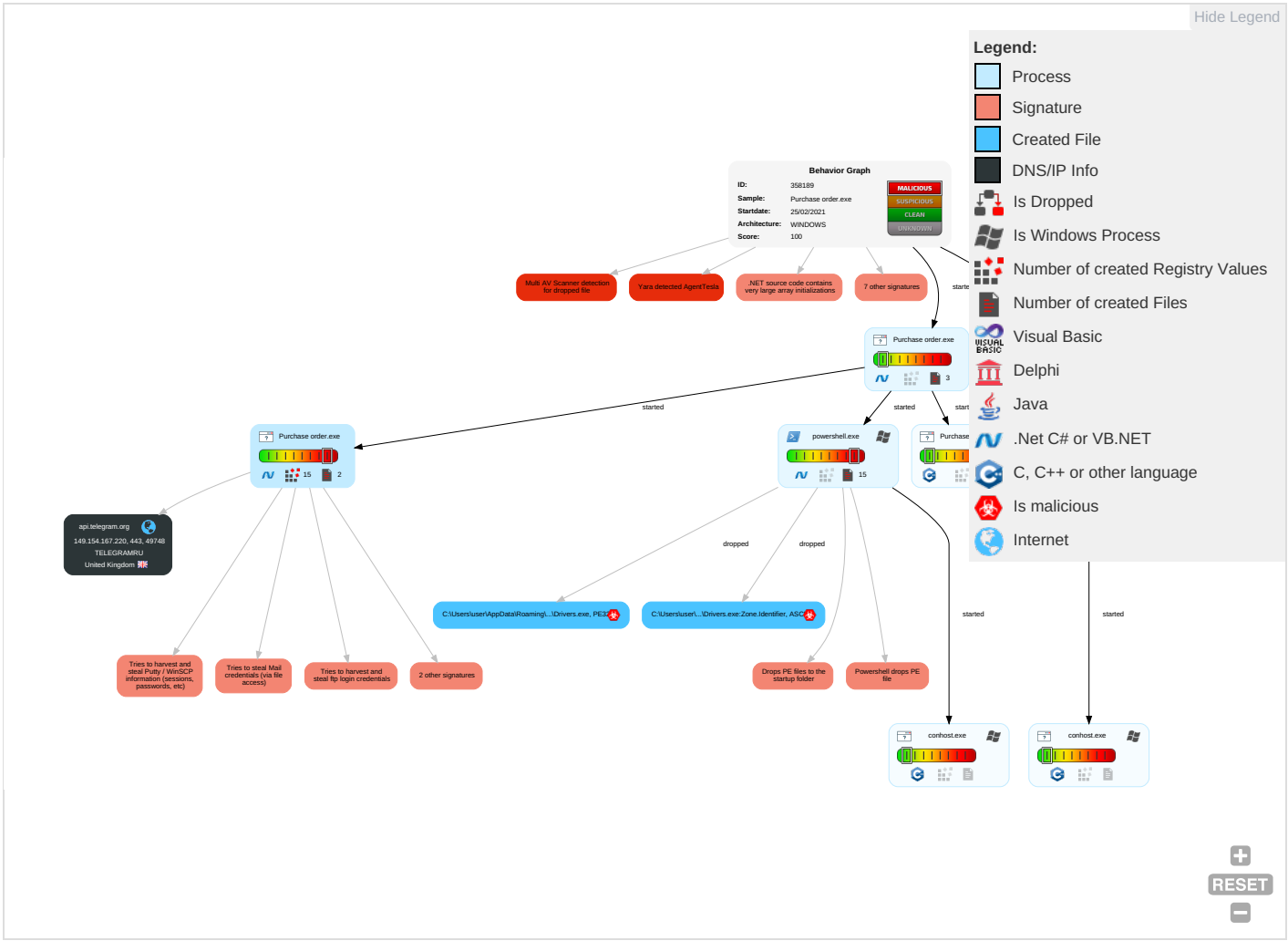
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	PowerShell 2	Registry Run Keys / Startup Folder 1 2	Process Injection 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1 2	Obfuscated Files or Information 2	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 2 1 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

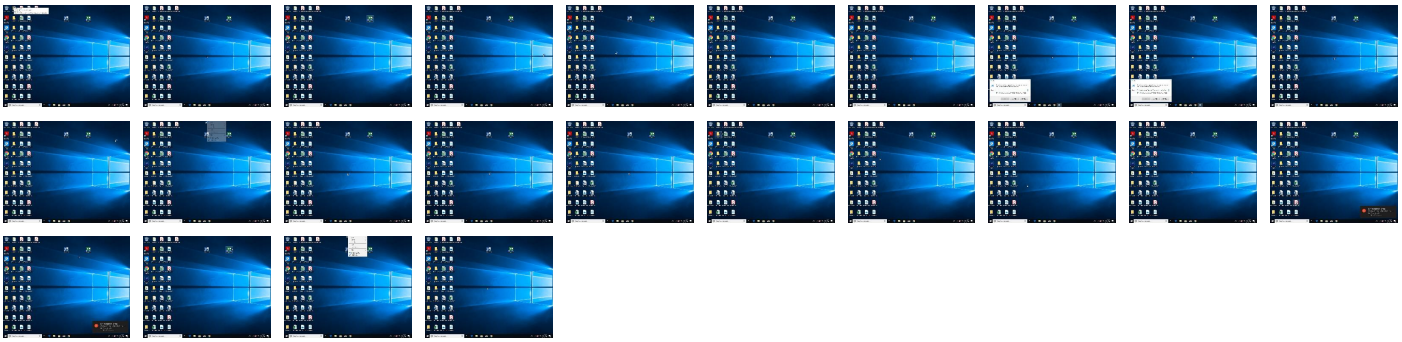
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	28%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.Purchase order.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
17.2.Drivers.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://Aa8zauZezuE3202C2Z.com	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://api.telegram.org4)l	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.microsoft.coo.	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.pngHz	0%	Avira URL Cloud	safe	
http://https://api.telegram.orgD8)l	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://jotaSG.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

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

URLs from Memory and Binaries

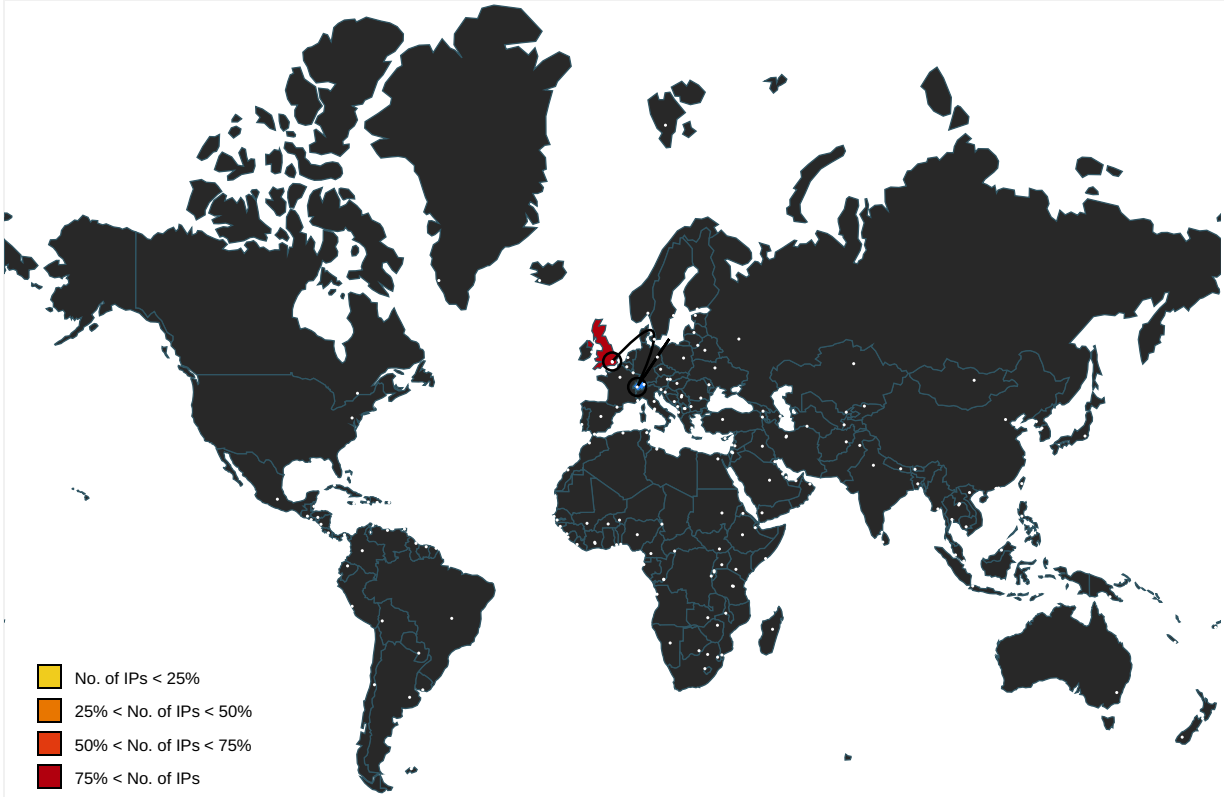
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Purchase order.exe, 00000007.00000002.599811556.00000000033E1000.00000004.00000001.sdmp, Drivers.exe, 00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://nuget.org/NuGet.exe	powershell.exe, 00000003.00000002.393564228.0000000005408000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.536141435.0000000005C75000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	Drivers.exe, 00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://Aa8zauZezuE3202C2Z.com	Purchase order.exe, 00000007.00000002.599811556.00000000033E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot1670019254:AAH89qmQqzYne6MnIySolVTT-8E2raVN0Ko/	Purchase order.exe, 00000002.00000002.334741254.00000000040B9000.00000004.00000001.sdmp, Purchase order.exe, 00000007.00000002.592269588.0000000000402000.00000040.00000001.sdmp, Drivers.exe, 0000000B.00000002.423935619.0000000003529000.00000004.00000001.sdmp, Drivers.exe, 00000011.00000002.592230208.0000000000402000.00000040.00000001.sdmp	false		high
http://https://api.telegram.org	Purchase order.exe, 00000007.00000002.601601404.000000000374A000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000003.00000002.392234936.00000000044E2000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000003.504047446.0000000007E23000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.531885745.0000000004D50000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Purchase order.exe, 00000007.00000002.599811556.00000000033E1000.00000004.00000001.sdmp, Drivers.exe, 00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000003.00000002.392234936.00000000044E2000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000003.504047446.0000000007E23000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.531885745.0000000004D50000.00000004.00000001.sdmp	false		high
http://certificates.godaddy.com/repository/0	Purchase order.exe, 00000007.00000002.607397136.0000000006BB8000.00000004.00000001.sdmp	false		high
http://certs.godaddy.com/repository/1301	Purchase order.exe, 00000007.00000002.607397136.0000000006BB8000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 0000000F.00000002.536141435.0000000005C75000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000000F.00000002.536141435.0000000005C75000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org4)l	Purchase order.exe, 00000007.00000002.601601404.000000000374A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://blog.naver.com/cubemit314Ghttp://projectofsonagi.tistory.com/	Purchase order.exe, 00000002.00000002.334741254.00000000040B9000.00000004.00000001.sdmp, Drivers.exe, 0000000B.00000002.423935619.0000000003529000.00000004.00000001.sdmp	false		high
http://crl.godaddy.com/gdig2s1-1823.crl0	Purchase order.exe, 00000007.00000002.607397136.0000000006BB8000.00000004.00000001.sdmp	false		high
http://https://certs.godaddy.com/repository/0	Purchase order.exe, 00000007.00000002.607397136.0000000006BB8000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/Pester/Pester	powershell.exe, 00000003.00000002.392234936.00000000044E2000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000003.504047446.0000000007E23000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.531885745.0000000004D50000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%$	Purchase order.exe, 00000007.00000002.599811556.00000000033E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.microsoft.coo.	Purchase order.exe, 00000007.00000002.607485458.0000000006BF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.godaddy.com/gdroot-g2.crl0F	Purchase order.exe, 00000007.00000002.607397136.0000000006BB8000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/PesterHz	powershell.exe, 00000003.00000002.392234936.00000000044E2000.00000004.00000001.sdmp	false		high
http://https://contoso.com/	powershell.exe, 0000000F.00000002.536141435.0000000005C75000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000003.00000002.393564228.0000000005408000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.536141435.0000000005C75000.00000004.00000001.sdmp	false		high
http://crl.godaddy.com/gdroot.crl0F	Purchase order.exe, 00000007.00000002.607397136.0000000006BB8000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.pngHz	powershell.exe, 00000003.00000002.392234936.00000000044E2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.orgD8)l	Purchase order.exe, 00000007.00000002.602072770.000000000379E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	Drivers.exe, 00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.apache.org/licenses/LICENSE-2.0.htmlHz	powershell.exe, 00000003.00000002.392234936.00000000044E2000.00000004.00000001.sdmp	false		high
http://api.telegram.org	Purchase order.exe, 00000007.00000002.601672353.000000000375E000.00000004.00000001.sdmp	false		high
http://certificates.godaddy.com/repository/gdig2.crt0	Purchase order.exe, 00000007.00000002.607397136.0000000006BB8000.00000004.00000001.sdmp	false		high
http://jotaSG.com	Drivers.exe, 00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot1670019254:AAH89qmQqzYne6MnIySolVTT-8E2raVN0Ko/sendDocument	Purchase order.exe, 00000007.00000002.601601404.000000000374A000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000003.00000002.392035603.00000000043A1000.00000004.00000001.sdmp, Purchase order.exe, 00000007.00000002.601601404.000000000374A000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.531608455.0000000004C11000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot1670019254:AAH89qmQqzYne6MnIySolVTT-8E2raVN0Ko/sendDocumentdocument-----	Purchase order.exe, 00000007.00000002.599811556.00000000033E1000.00000004.00000001.sdmp, Drivers.exe, 00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Purchase order.exe, 00000002.00000002.334741254.00000000040B9000.00000004.00000001.sdmp, Purchase order.exe, 00000007.00000002.592269588.0000000000402000.00000040.00000001.sdmp, Drivers.exe, 0000000B.00000002.423935619.0000000003529000.00000004.00000001.sdmp, Drivers.exe, 00000011.00000002.592230208.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358189
Start date:	25.02.2021
Start time:	07:44:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase order.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:	30

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@14/13@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, wermgr.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 92.122.145.220, 168.61.161.212, 52.255.188.83, 104.43.139.144, 51.11.168.160, 104.43.193.48, 2.20.142.210, 2.20.142.209, 51.103.5.159, 52.155.217.156, 92.122.213.194, 92.122.213.247, 20.54.26.129, 40.126.31.1, 40.126.31.135, 20.190.159.138, 40.126.31.6, 40.126.31.4, 40.126.31.8, 40.126.31.139, 40.126.31.141, 23.218.208.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/358189/sample/Purchase order.exe

Simulations

Behavior and APIs

Time	Type	Description
07:45:57	API Interceptor	699x Sleep call for process: Purchase order.exe modified
07:46:00	API Interceptor	59x Sleep call for process: powershell.exe modified
07:46:05	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
07:46:58	API Interceptor	307x Sleep call for process: Drivers.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	WHz0D1UERA.exe	Get hash	malicious	Browse	
	g6ys6ZH0HO.exe	Get hash	malicious	Browse	
	OC 136584.PDF.exe	Get hash	malicious	Browse	
	Quote_13940007.exe	Get hash	malicious	Browse	
	SKBM 0222.exe	Get hash	malicious	Browse	
	crypted.exe	Get hash	malicious	Browse	
	PO-735643-SALES.exe	Get hash	malicious	Browse	
	muOvK6dngg.exe	Get hash	malicious	Browse	
	SKBM 0222..exe	Get hash	malicious	Browse	
	PO 86540.exe	Get hash	malicious	Browse	
	Unterlagen PDF.exe	Get hash	malicious	Browse	
	JFAaEh5hB6.exe	Get hash	malicious	Browse	
	BMfilGROO2.exe	Get hash	malicious	Browse	
	Inv_874520.exe	Get hash	malicious	Browse	
	Inv_95736.scr.exe	Get hash	malicious	Browse	
	purchase_order.exe	Get hash	malicious	Browse	
	RFQ_2345.exe	Get hash	malicious	Browse	
	Rechnung.exe	Get hash	malicious	Browse	
	Shipping_Doc.exe	Get hash	malicious	Browse	
	Purchase_Order16-122020.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	WHz0D1UERA.exe	Get hash	malicious	Browse	• 149.154.167.220
	g6ys6ZH0HO.exe	Get hash	malicious	Browse	• 149.154.167.220
	OC 136584.PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quote_13940007.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222.exe	Get hash	malicious	Browse	• 149.154.167.220
	crypted.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO-735643-SALES.exe	Get hash	malicious	Browse	• 149.154.167.220
	muOvK6dngg.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222..exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 86540.exe	Get hash	malicious	Browse	• 149.154.167.220
	Unterlagen PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 149.154.167.220
	BMfilGROO2.exe	Get hash	malicious	Browse	• 149.154.167.220
	Inv_874520.exe	Get hash	malicious	Browse	• 149.154.167.220
	Inv_95736.scr.exe	Get hash	malicious	Browse	• 149.154.167.220
	REVISED_INVOICE_Company_BankDetails_fle_doc.xlsx.exe	Get hash	malicious	Browse	• 149.154.167.220
	purchase_order.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ_2345.exe	Get hash	malicious	Browse	• 149.154.167.220
	Rechnung.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping_Doc.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	WHz0D1UERA.exe	Get hash	malicious	Browse	• 149.154.167.220
	g6ys6ZH0HO.exe	Get hash	malicious	Browse	• 149.154.167.220
	OC 136584.PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quote_13940007.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222.exe	Get hash	malicious	Browse	• 149.154.167.220
	crypted.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO-735643-SALES.exe	Get hash	malicious	Browse	• 149.154.167.220
	muOvK6dngg.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222..exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 86540.exe	Get hash	malicious	Browse	• 149.154.167.220
	Unterlagen PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 149.154.167.220
	BMfiIGROO2.exe	Get hash	malicious	Browse	• 149.154.167.220
	Inv_874520.exe	Get hash	malicious	Browse	• 149.154.167.220
	Inv_95736.scr.exe	Get hash	malicious	Browse	• 149.154.167.220
	purchase_order.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ_2345.exe	Get hash	malicious	Browse	• 149.154.167.220
	Rechnung.exe	Get hash	malicious	Browse	• 149.154.167.220
	Shipping_Doc.exe	Get hash	malicious	Browse	• 149.154.167.220
	Purchase_Order16-122020.exe	Get hash	malicious	Browse	• 149.154.167.220

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	HblVSJaQa1.exe	Get hash	malicious	Browse	• 149.154.167.220
	FspMzSMtYA.exe	Get hash	malicious	Browse	• 149.154.167.220
	New Po #0126733 2021.exe	Get hash	malicious	Browse	• 149.154.167.220
	530000.exe	Get hash	malicious	Browse	• 149.154.167.220
	Bitcoin Mining 2021 Feb.exe	Get hash	malicious	Browse	• 149.154.167.220
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 149.154.167.220
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 149.154.167.220
	EOrg2020.exe	Get hash	malicious	Browse	• 149.154.167.220
	Bitcoin Mining 2021 Feb.exe	Get hash	malicious	Browse	• 149.154.167.220
	AZjP1E0nRZ.exe	Get hash	malicious	Browse	• 149.154.167.220
	x0yccMVTIb.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WHz0D1UERA.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe	Get hash	malicious	Browse	• 149.154.167.220
	1i0Bvmiuqg.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	• 149.154.167.220
	OC 136584.PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quote_13940007.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222.exe	Get hash	malicious	Browse	• 149.154.167.220
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Drivers.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21q1KDLI4M9XKbbDLI4MWuPJKiUrRZ9I0ZKm:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9px
MD5:	3A72FBECA73A61C00EECBDEC37EAD411
SHA1:	E2330F7B3182A857BB477B2492DDECC2A8488211
SHA-256:	2D4310C4AB9ADEFD6169137CD8973D23D779EDD968B8B39DBC072BF888D0802C
SHA-512:	260EBFB3045513A0BA14751A6B67C95CDA83DD122DC8510EF89C9C42C19F076C8C40645E0795C15ADDF57DB65513DD73EB3C5D0C883C6FB1C34165BE35AE38 9
Malicious:	false
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase order.exe.log	
Process:	C:\Users\user\Desktop\Purchase order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21q1KDLI4M9XKbbDLI4MWuPJKiUrRZ9I0ZKm:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9px
MD5:	3A72FBECA73A61C00EECBDEC37EAD411
SHA1:	E2330F7B3182A857BB477B2492DDECC2A8488211
SHA-256:	2D4310C4AB9ADEFD6169137CD8973D23D779EDD968B8B39DBC072BF888D0802C
SHA-512:	260EBFB3045513A0BA14751A6B67C95CDA83DD122DC8510EF89C9C42C19F076C8C40645E0795C15ADDF57DB65513DD73EB3C5D0C883C6FB1C34165BE35AE38 9
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase order.exe.log	
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8003
Entropy (8bit):	4.839308921501875
Encrypted:	false
SSDEEP:	192:yxoe5oVsm5emdVVFn3eGOVpN6K3bkkjo59gkjDt4iWN3yBGHh9smidcU6CXpOTik:DBVoGIpN6KQkj2Wkjh4iUx0mib4J
MD5:	937C6E940577634844311E349BD4614D
SHA1:	379440E933201CD3E6E6BF9B0E61B7663693195F
SHA-256:	30DC628AB2979D2CF0D281E998077E5721C68B9BBA61610039E11FDC438B993C
SHA-512:	6B37FE533991631C8290A0E9CC0B4F11A79828616BEF0233B4C57EC7C9DCBFC274FB7E50FC920C4312C93E74CE621B6779F10E4016E9FD794961696074BDFBF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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):	19640
Entropy (8bit):	5.572484966310125
Encrypted:	false
SSDEEP:	384:2t9+Xm2S0uuaR30+biRISBKn7ul9bpaeQ9QRbp2cQwpPTDwiqWJI5jw:q6aR3P/4K7ulDat9qoRgszWJI
MD5:	82FF6947CCC8C0CD577C594B9F9804D9
SHA1:	8F4B30A204F6769EE80AD43A37621C0020EBAE76
SHA-256:	3FBA5040D96FCC73B0BB50A535B7F8ACB0C66592072A6625684CD556C763E8AD
SHA-512:	AB54A229F3030EE75B65326A65D35D6AB89D3FDAFA6AF732453196896AF0DB4A9B3AC99958A836110633A69A3C4B5FB77038A80D9340E0666817AF6AD30ED596
Malicious:	false
Reputation:	low
Preview:	@...e.....'.g.T.T...Z...'.r.....@.....H.....<@.^.L."My...:?..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)V.....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.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_00vk02bh.l3e.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jdd0wdgo.1sf.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_k3u3tnr4.sav.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y4ubbksp.mot.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	544256
Entropy (8bit):	7.296683876210466
Encrypted:	false
SSDEEP:	12288:+cQS8AfwkDQl5YClyDAPxxJ/sRP7S0wvGtf:+cn8AfwDl5YClrxj/t0w+t
MD5:	98BE4D3BB2053810801FADEB32884ACD
SHA1:	8919195923883F3842FF78210AB6C6C1E448A10B
SHA-256:	DF61B9C866C5CEB278E173814DDF975B70B5B2E9FCBC5B482326E4163C2E1086
SHA-512:	4055EA00FDF72A82C2D75D7C2DFECDA9E4011708380A493FD6597015779247A03B12262DDA618A88C6AF0EC7447132322C675F1F27A16885CB78DB9728986BD1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 28%

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....6`.....0..... .....@.. ..... .@.....W.....B..... ..... ..H.....text..... ..... ..`.rsrc...B.....@..@.reloc..... .....L.....@..B.....H.....0.....3...T9..Vf.....(.....(....).....(.....s....('....*.(.....*".(.....*6.{....o.....*.s.....*.(/....*..{....*"..}....*.. {....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..r...p}.....(J...}.....r...p}.....W...%...}.....(....*.....%.(K...(L....%.r?..p.%.(.....%.r...p.(M.....*..{....*"..}....*^..}.....(a.....(&....*^...ob. ..(!.....(c....*6.~....(....&*.(E...r_..p(.....~....~.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe:Zone.Identifier	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210225\PowerShell_transcript.899552.84Dp3uuP.20210225074538.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):	1201
Entropy (8bit):	5.161841529627427
Encrypted:	false
SSDEEP:	24:BxSAc7vBVLazx2DOXCgQRabuVM5fWOHjeTKKjX4CIym1ZJXuRabuVM5XnxSAZS:BZwvTL0oOduA+OqDYB1ZJuA3ZZS
MD5:	0DFD33867C55121FFE904CB48324BA7C
SHA1:	EC28CEA1FF2C1903454BE114B1A45601A7F2841A
SHA-256:	26C4FBB8EE86ADC508CCCDE90E9AE3A07AFA06FB9B53F03E33B9AEA905377334
SHA-512:	53D88A52E40DEEB49B40192C2C5BE05778C8CB38F4F8DD37D58E780C37D889C87FE7BF0D868AEF7E3FD5BE0F06AABC65B3490433FBE6F414E363B9C283C463CB
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225074553..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 899552 (Microsoft Windows NT 10.0.17134.0)..Host Application: Powershell.exe -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\Purchase order.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'..Process ID: 7128..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: 20210225074554..**********..PS>Copy-Item 'C:\Users\user\Desktop\Purchase order.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'..**********

C:\Users\user\Documents\20210225\PowerShell_transcript.899552.Nq+y45_q.20210225074621.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):	3951
Entropy (8bit):	5.314377925178523
Encrypted:	false
SSDEEP:	96:BZETL0NlEWqDo1ZKE9ZTTL0NlEWqDo1ZGZxY6HY6HU6vZe:u
MD5:	2E00D0DF7C077195D4F75EC25FBF7D17
SHA1:	FFCA4D5ACB27279BDCED9E75D14BA26213B44D7B
SHA-256:	68AE9A540AF7F57822E45679F3AA45DFB8BF7F1D1DE60FBC535C8D31F11FA637
SHA-512:	8BE5D910DDAEEA0C787359E2C969F0295F0112BEB2C974D295651949B2FD5110879AD91301551998245557 4DD83BF824C0365E583165555AA087B25BE7FEB96B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225074643..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 899552 (Microsoft Windows NT 10.0.17134.0)..Host Application: Powershell.exe -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'..Process ID: 7032..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: 20210225074643..**********..PS>Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\eng

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.296683876210466
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Purchase order.exe
File size:	544256
MD5:	98be4d3bb2053810801fadeb32884acd
SHA1:	8919195923883f3842ff78210ab6c6c1e448a10b
SHA256:	df61b9c866c5ceb278e173814ddf975b70b5b2e9fcbc5b482326e4163c2e1086
SHA512:	4055ea00fdf72a82c2d75d7c2dfecda9e4011708380a493fd6597015779247a03b12262dda618a88c6af0ec7447132322c675f1f27a16885cb78db9728986bd1
SSDEEP:	12288:+cQS8AfwkDQl5YClyDAPxxJ/sRP7S0wvGtf:+cn8AfwDl5YClrxj/t0w+t
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....6`.....0..... ....@.. ..... @.....

File Icon

Icon Hash:	c29ae2e8b9b88670

Static PE Info

General

Entrypoint:	0x46d0fe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60369DF3 [Wed Feb 24 18:41:55 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0x6d0a4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6e000	0x19642	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6b104	0x6b200	False	0.942199350933	data	7.98094912825	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x19642	0x19800	False	0.0767176011029	data	1.97122010304	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6e220	0x98f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x6ebb0	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x7f3d8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x83600	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x85ba8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x86c50	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x870b8	0x5a	data		
RT_VERSION	0x87114	0x344	data		
RT_MANIFEST	0x87458	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

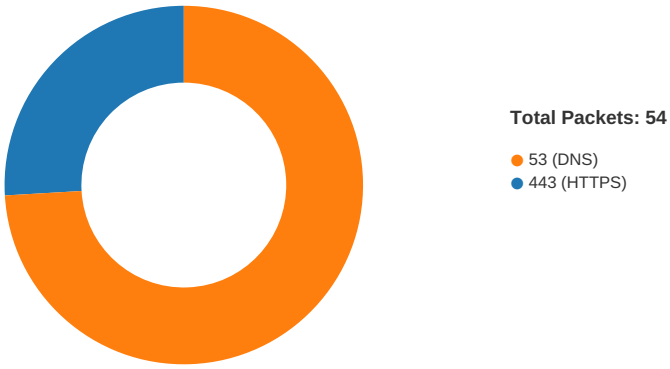
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	16.0.0.0
InternalName	POWERPNT.exe
FileVersion	16.0.0.0
CompanyName	Microsoft Corporation
Comments	Microsoft PowerPoint
ProductName	Microsoft Office 2016
ProductVersion	16.0.0.0
FileDescription	POWERPNT
OriginalFilename	POWERPNT.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:47:37.818101883 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:37.869913101 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:37.870048046 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:38.054549932 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:38.109113932 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:38.110987902 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:38.111008883 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:38.111023903 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:38.111037016 CET	443	49748	149.154.167.220	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:47:38.111148119 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:38.112062931 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:38.112078905 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:38.112287045 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:38.120388031 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:38.174921989 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:38.223704100 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:38.865050077 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:38.925525904 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:38.928488016 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:39.025962114 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:39.538077116 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:39.583225965 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:39.931586027 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:39.982371092 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:39.982395887 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:39.982677937 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:40.033467054 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:40.424951077 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:40.429474115 CET	49748	443	192.168.2.6	149.154.167.220
Feb 25, 2021 07:47:40.480272055 CET	443	49748	149.154.167.220	192.168.2.6
Feb 25, 2021 07:47:40.480581045 CET	49748	443	192.168.2.6	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:45:27.833833933 CET	54513	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:45:27.882523060 CET	53	54513	8.8.8.8	192.168.2.6
Feb 25, 2021 07:45:28.249928951 CET	62044	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:45:28.322299004 CET	53	62044	8.8.8.8	192.168.2.6
Feb 25, 2021 07:45:29.272773027 CET	63791	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:45:29.324351072 CET	53	63791	8.8.8.8	192.168.2.6
Feb 25, 2021 07:45:30.477871895 CET	64267	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:45:30.526504040 CET	53	64267	8.8.8.8	192.168.2.6
Feb 25, 2021 07:45:31.658081055 CET	49448	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:45:31.712163925 CET	53	49448	8.8.8.8	192.168.2.6
Feb 25, 2021 07:45:33.108897924 CET	60342	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:45:33.159143925 CET	53	60342	8.8.8.8	192.168.2.6
Feb 25, 2021 07:45:33.992043018 CET	61346	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:45:34.042870998 CET	53	61346	8.8.8.8	192.168.2.6
Feb 25, 2021 07:45:58.763430119 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:45:58.815009117 CET	53	51774	8.8.8.8	192.168.2.6
Feb 25, 2021 07:45:59.649032116 CET	56023	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:45:59.697731018 CET	53	56023	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:00.453399897 CET	58384	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:00.502321005 CET	53	58384	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:02.654409885 CET	60261	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:02.703193903 CET	53	60261	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:03.897804976 CET	56061	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:03.952090979 CET	53	56061	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:04.880928993 CET	58336	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:04.931982040 CET	53	58336	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:05.839903116 CET	53781	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:05.889086008 CET	53	53781	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:07.119414091 CET	54064	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:07.179316044 CET	53	54064	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:08.293875933 CET	52811	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:08.342838049 CET	53	52811	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:17.447737932 CET	55299	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:17.500386000 CET	53	55299	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:18.552854061 CET	63745	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:18.602615118 CET	53	63745	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:19.561132908 CET	50055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:19.610884905 CET	53	50055	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:46:21.826067924 CET	61374	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:21.883124113 CET	53	61374	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:24.523447990 CET	50339	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:24.572088957 CET	53	50339	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:32.903569937 CET	63307	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:33.915173054 CET	63307	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:33.974131107 CET	53	63307	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:34.741507053 CET	49694	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:34.800889015 CET	53	49694	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:35.554100990 CET	54982	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:35.572737932 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:35.614238024 CET	53	54982	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:35.629693985 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:35.657224894 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:35.717067957 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:36.573292971 CET	62116	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:36.633711100 CET	53	62116	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:37.389599085 CET	63816	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:37.449058056 CET	53	63816	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:38.372221947 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:38.422899008 CET	53	55014	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:39.503551960 CET	62208	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:39.553471088 CET	53	62208	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:41.097889900 CET	57574	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:41.149591923 CET	53	57574	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:42.437510014 CET	51818	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:42.496706963 CET	53	51818	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:43.218672037 CET	56628	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:43.278783083 CET	53	56628	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:53.585944891 CET	60778	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:53.646032095 CET	53	60778	8.8.8.8	192.168.2.6
Feb 25, 2021 07:46:54.289232969 CET	53799	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:46:54.338109970 CET	53	53799	8.8.8.8	192.168.2.6
Feb 25, 2021 07:47:08.816586971 CET	54683	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:47:08.879374981 CET	53	54683	8.8.8.8	192.168.2.6
Feb 25, 2021 07:47:10.785978079 CET	59329	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:47:10.837296963 CET	53	59329	8.8.8.8	192.168.2.6
Feb 25, 2021 07:47:12.237906933 CET	64021	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:47:12.312980890 CET	53	64021	8.8.8.8	192.168.2.6
Feb 25, 2021 07:47:37.528059959 CET	56129	53	192.168.2.6	8.8.8.8
Feb 25, 2021 07:47:37.584954023 CET	53	56129	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 07:47:37.528059959 CET	192.168.2.6	8.8.8.8	0x7e5	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
Feb 25, 2021 07:46:53.646032095 CET	8.8.8.8	192.168.2.6	0x3d85	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:47:37.584954023 CET	8.8.8.8	192.168.2.6	0x7e5	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTPS Packets

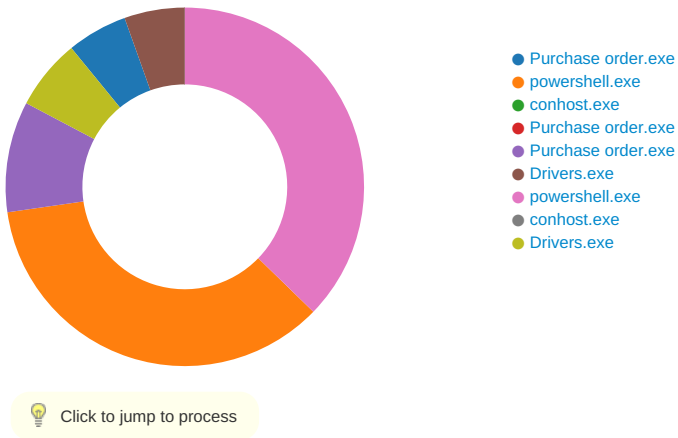
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 07:47:38.112062931 CET	149.154.167.220	443	192.168.2.6	49748	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Purchase order.exe PID: 7072 Parent PID: 6140

General

Start time:	07:45:34
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Purchase order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase order.exe'
Imagebase:	0xd20000
File size:	544256 bytes
MD5 hash:	98BE4D3BB2053810801FADEB32884ACD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000002.00000002.337349475.00000000057B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.334741254.00000000040B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000002.00000002.334741254.00000000040B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000003.324926849.0000000001303000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase order.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase order.exe.log	unknown	706	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",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_v4.0.3	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown

Analysis Process: powershell.exe PID: 7128 Parent PID: 7072

General

Start time:	07:45:36
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\Purchase order.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'
Imagebase:	0xd30000
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:\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	6E0FCF06	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	6E0FCF06	unknown
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	6CEA5B28	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	6CEA5B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_k3u3tnr4.sav.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_00vk02bh.l3e.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\Documents\20210225	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\Documents\20210225\PowerShell_transcript.899552.84Dp3uuP.20210225074538.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.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	6CF4DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF4DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_k3u3tnr4.sav.ps1	success or wait	1	6CF46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_00vk02bh.l3e.psm1	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_k3u3tnr4.sav.ps1	unknown	1	31	1	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_00vk02bh.l3e.psm1	unknown	1	31	1	success or wait	1	6CF41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210225\PowerShell_transcript.899552.84Dp3uuP.20210225074538.txt	unknown	3	ef bb bf	...	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.899552.84Dp3uuP.20210225074538.txt	unknown	746	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 31 30 32 32 35 30 37 34 35 35 33 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 38 39 39 35 35 32 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 start..Start time: 20210225074553..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 899552 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	11	6CF41B4F	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 f3 9d 36 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 b2 06 00 00 9a 01 00 00 00 00 00 fe d0 06 00 00 20 00 00 00 e0 06 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 a0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L.....6`.......... ....0................. ....@.. ....@.................	success or wait	3	6CF4DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.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	6CF4DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 16 0f 00 00 17 00 00 00 e9 0d 45 05 a4 08 90 08 53 07 00 00 00 00 c0 02 40 00 c7 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....E... ..S.....@.....@.....	success or wait	1	6E3C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 27 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .:'..... .	success or wait	17	6E3C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	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	6E3C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	6E3C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	8	6E3C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 54 01 40 00 f9 3e 40 01 09 06 80 00 33 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 16 3b 40 01 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 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 09 0c 80 00 58 64 40 01 56 64 40 01 fb 2a 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 1b 3b 40 01 3c 4d 40 01 24 4d 40 01 19 3b 40 01 bc 3c 40 01 38 4d 40 01 3f 4d 40	....T.@..>@.....3g@./g@..5@.- 5@...@.V.@.H.@.X.@.[.@..;@.NT @.HT@..S@..S@.hT@..S@..S@..S@. \.@..T@..T@.@X@.?X@..T@.....Xd @.Vd@..*@..S@..S@..T @..T@.xT@. zT@..T@.=M@.DM@.:M @."M@. M@.!M @.;M@..D@..D@.@M@..;@.<M@.$M@..;@..<@.8M@.?M@	success or wait	8	6E3C76FC	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	6E0D5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0DCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0D5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E0E1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6E0E203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	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	6CF41B4F	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	6CF41B4F	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	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	134	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: conhost.exe PID: 7144 Parent PID: 7128

General

Start time:	07:45:36
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: Purchase order.exe PID: 5132 Parent PID: 7072

General

Start time:	07:45:37
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Purchase order.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Purchase order.exe
Imagebase:	0x1f0000
File size:	544256 bytes
MD5 hash:	98BE4D3BB2053810801FADEB32884ACD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Purchase order.exe PID: 2040 Parent PID: 7072

General

Start time:	07:45:38
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Purchase order.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase order.exe
Imagebase:	0xf90000
File size:	544256 bytes
MD5 hash:	98BE4D3BB2053810801FADEB32884ACD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.592269588.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.599811556.00000000033E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.599811556.00000000033E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	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	6E0FCF06	unknown

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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\61a5e227-f6c6-41e9-9473-64959ad1a25b	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF41B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: Drivers.exe PID: 5988 Parent PID: 3440

General

Start time:	07:46:14
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'
Imagebase:	0x10000
File size:	544256 bytes
MD5 hash:	98BE4D3BB2053810801FADEB32884ACD
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: 0000000B.00000002.423935619.0000000003529000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000000B.00000002.423935619.0000000003529000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000003.412342681.0000000000756000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000000B.00000002.429837387.0000000004B20000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 28%, ReversingLabs
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	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Drivers.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Drivers.exe.log	unknown	706	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",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_v4.0.3	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown

Analysis Process: powershell.exe PID: 7032 Parent PID: 5988

General

Start time:	07:46:17
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'
Imagebase:	0xd30000
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:\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	6E0FCF06	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	6E0FCF06	unknown
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	6CEA5B28	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	6CEA5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jdd0wdgo.1sf.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y4ubbksp.mot.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\Documents\20210225\PowerShell_transcript.899552.Nq+y45_q.20210225074621.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jdd0wdgo.1sf.ps1	success or wait	1	6CF46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y4ubbksp.mot.psm1	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jdd0wdgo.1sf.ps1	unknown	1	31	1	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y4ubbksp.mot.psm1	unknown	1	31	1	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.899552.Nq+y45_q.20210225074621.txt	unknown	3	ef bb bf	...	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.899552.Nq+y45_q.20210225074621.txt	unknown	793	2a 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 31 30 32 32 35 30 37 34 36 34 33 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 38 39 39 35 35 32 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 start..Start time: 20210225074643..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 899552 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	27	6CF41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3907	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 12 00 00 00 e0 11 00 00 17 00 00 00 8f 0a 27 05 67 05 54 05 54 05 00 00 5a 01 8f 01 27 00 72 0a 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....'.g.T.T...Z...'.r.....@.....	success or wait	1	6E3C76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3f 00 00 00 0e 00 20 00	H.....<@.^...L."My..:?..... .	success or wait	18	6E3C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	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	18	6E3C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E3C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	6E3C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 56 00 40 00 98 01 40 00 fa 00 40 00 ce 67 40 01 99 01 40 00 fb 00 40 00 54 01 40 00 f9 3e 40 01 33 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 56 01 00 00 48 01 00 00 58 01 00 00 5b 01 00 00 4e 54 00 01 48 54 00 01 f4 53 00 01 8b 53 00 01 68 54 00 01 91 53 00 01 fa 53 00 01 82 53 00 01 5c 01 00 00 00 54 00 01 02 54 00 01 40 58 00 01 3f 58 00 01 1c 54 00 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40	.....V.@...@...@..g@...@. ..@.T.@..>@.3g@./g@..5@.-5@...@.V...H...X... [...NT..HT...S.. .S..hT...S...S...S..\....T...T ..@X..? X...T...S@..S@..T@..T@. xT@.zT@..T@.=M@.DM @.:M@."M@. M @.!M@.;M@..D@..D@.@ M@.<M@.$M@.8M@.? M@.EM@..q@	success or wait	9	6E3C76FC	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	6E0D5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0DCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0D5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile

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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E0E1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	16636	success or wait	1	6E0E203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	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	6CF41B4F	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	6CF41B4F	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	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CF41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: conhost.exe PID: 7120 Parent PID: 7032

General

Start time:	07:46:17
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: Drivers.exe PID: 4924 Parent PID: 5988

General

Start time:	07:46:19
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
Imagebase:	0x800000
File size:	544256 bytes
MD5 hash:	98BE4D3BB2053810801FADEB32884ACD
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: 00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.597984590.0000000002C31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.592230208.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	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	6E0FCF06	unknown

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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Disassembly

Code Analysis