

JOeSandbox Cloud BASIC



ID: 672759

Sample Name: Purchase
order.exe

Cookbook: default.jbs

Time: 11:29:54

Date: 25/07/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report Purchase order.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Telegram RAT	4
Threatname: Agenttesla	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	6
System Summary	6
Data Obfuscation	6
Boot Survival	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	7
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	10
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	12
Public IPs	13
General Information	13
Warnings	14
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	14
IPs	14
Domains	14
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase order.exe.log	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cwyntq2b.npw.psm1	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dz0lxrga.mbt.psm1	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lcn4kimx.j2a.ps1	16
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t3f3sog0.5s0.ps1	16
C:\Users\user\AppData\Local\Temp\tmp1E2.tmp	16
C:\Users\user\AppData\Roaming\lq0j300ya.blp\Chrome\Default\Cookies	17
C:\Users\user\AppData\Roaming\zwLLFjVv.exe	17
C:\Users\user\AppData\Roaming\zwLLFjVv.exe:Zone.Identifier	17
C:\Users\user\Documents\20220725\PowerShell_transcript.123716.NRW_8MvJ.20220725113126.txt	17
C:\Users\user\Documents\20220725\PowerShell_transcript.123716.RgDO1ffS.20220725113128.txt	18
Static File Info	18
General	18
File Icon	18
Static PE Info	19
General	19
Entrypoint Preview	19
Data Directories	21
Sections	21
Resources	21

Imports	21
Network Behavior	21
Snort IDS Alerts	21
Network Port Distribution	22
TCP Packets	22
UDP Packets	23
DNS Queries	23
DNS Answers	23
HTTP Request Dependency Graph	23
HTTPS Proxied Packets	23
Statistics	24
Behavior	24
System Behavior	25
Analysis Process: Purchase order.exePID: 5756, Parent PID: 5900	25
General	25
File Activities	25
File Created	25
File Deleted	25
File Written	25
File Read	27
Analysis Process: powershell.exePID: 3628, Parent PID: 5756	27
General	27
File Activities	28
File Created	28
File Deleted	28
File Written	28
File Read	30
Analysis Process: conhost.exePID: 6032, Parent PID: 3628	33
General	33
Analysis Process: powershell.exePID: 1036, Parent PID: 5756	33
General	33
File Activities	34
File Created	34
File Deleted	34
File Written	34
File Read	35
Analysis Process: conhost.exePID: 5292, Parent PID: 1036	38
General	38
Analysis Process: schtasks.exePID: 6172, Parent PID: 5756	39
General	39
File Activities	39
File Read	39
Analysis Process: conhost.exePID: 6352, Parent PID: 6172	39
General	39
Analysis Process: Purchase order.exePID: 6444, Parent PID: 5756	39
General	39
File Activities	40
File Created	40
File Deleted	40
File Written	41
File Read	41
Registry Activities	41
Disassembly	42

Windows Analysis Report

Purchase order.exe

Overview

General Information

Sample Name:

Purchase order.exe

Analysis ID:

672759

MD5:

24b0be710ed42b..

SHA1:

597bce6e933511..

SHA256:

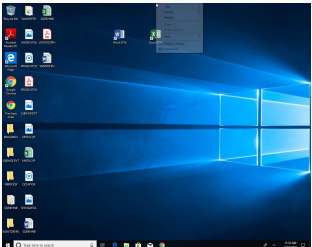
89823f7c472a09..

Tags:

AgentTesla exe

Infos:





Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Malicious sample detected (through...

Yara detected Telegram RAT

Yara detected AgentTesla

Yara detected AntiVM3

Multi AV Scanner detection for drop...

Snort IDS alert for network traffic

Tries to steal Mail credentials (via fi...

Initial sample is a PE file and has a...

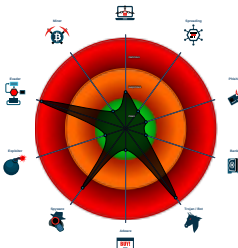
Tries to harvest and steal Putty / W...

Tries to harvest and steal ftp login c...

.NET source code references suspic...

Tries to detect sandboxes and other...

Classification



Process Tree

System is w10x64

Purchase order.exe (PID: 5756 cmdline: "C:\Users\user\Desktop\Purchase order.exe" MD5: 24B0BE710ED42B1EC10224DB8DB55BF6)

powershell.exe (PID: 3628 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\Purchase order.exe" MD5: DBA3E6449E97D4E3DF64527EF7012A10)

conhost.exe (PID: 6032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

powershell.exe (PID: 1036 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roamin glzwLLFjVv.exe" MD5: DBA3E6449E97D4E3DF64527EF7012A10)

conhost.exe (PID: 5292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

schtasks.exe (PID: 6172 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lzwLLFjVv" /XML "C:\Users\user\AppData\Local\Templtmp1E2.tmp" MD5: 15FF7D8324231381BAD48A052F85DF04)

conhost.exe (PID: 6352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

Purchase order.exe (PID: 6444 cmdline: C:\Users\user\Desktop\Purchase order.exe" MD5: 24B0BE710ED42B1EC10224DB8DB55BF6)

cleanup

Malware Configuration

Threatname: Telegram RAT

{

"C2 url": "https://api.telegram.org/bot5573921253:AAHXXq7LrmioCzUGP-9p7LopfbVX0A_ZdQA/sendMessage"

}

Threatname: Agenttesla

{

"Exfil Mode": "Telegram",

"Chat id": "5359531870",

"Chat URL": "https://api.telegram.org/bot5573921253:AAHXXq7LrmioCzUGP-9p7LopfbVX0A_ZdQA/sendDocument"

}

Copyright Joe Security LLC 2022

Page 4 of 42

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.514358204.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000011.00000002.514358204.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000011.00000000.317899591.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000011.00000000.317899591.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000011.00000000.319090095.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
17.0.Purchase order.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
17.0.Purchase order.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
17.0.Purchase order.exe.400000.12.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
17.0.Purchase order.exe.400000.12.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	0x32c49:\$s10: logins 0x326b0:\$s11: credential 0x2ebf0:\$g1: get_Clipboard 0x2ebfe:\$g2: get_Keyboard 0x2ec0b:\$g3: get_Password 0x2fef9:\$g4: get_CtrlKeyDown 0x2ff09:\$g5: get_ShiftKeyDown 0x2ff1a:\$g6: get_AltKeyDown
17.2.Purchase order.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 43 entries

Sigma Signatures

 No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.4 - Destination IP: 149.154.167.220	
Timestamp:	192.168.2.4149.154.167.220497704432851779 07/25/22-11:31:56.998694
SID:	2851779
Source Port:	49770
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file
Multi AV Scanner detection for dropped file
Machine Learning detection for sample
Machine Learning detection for dropped file

Networking



Snort IDS alert for network traffic
Uses the Telegram API (likely for C&C communication)
Yara detected Generic Downloader

System Summary



Malicious sample detected (through community Yara rule)
Initial sample is a PE file and has a suspicious name
.NET source code contains very large array initializations

Data Obfuscation



.NET source code contains method to dynamically call methods (often used by packers)
--

Boot Survival



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

Malware Analysis System Evasion



Yara detected AntiVM3
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion



.NET source code references suspicious native API functions
Injects a PE file into a foreign processes
Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information



Yara detected Telegram RAT
Yara detected AgentTesla
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Tries to harvest and steal ftp login credentials
Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

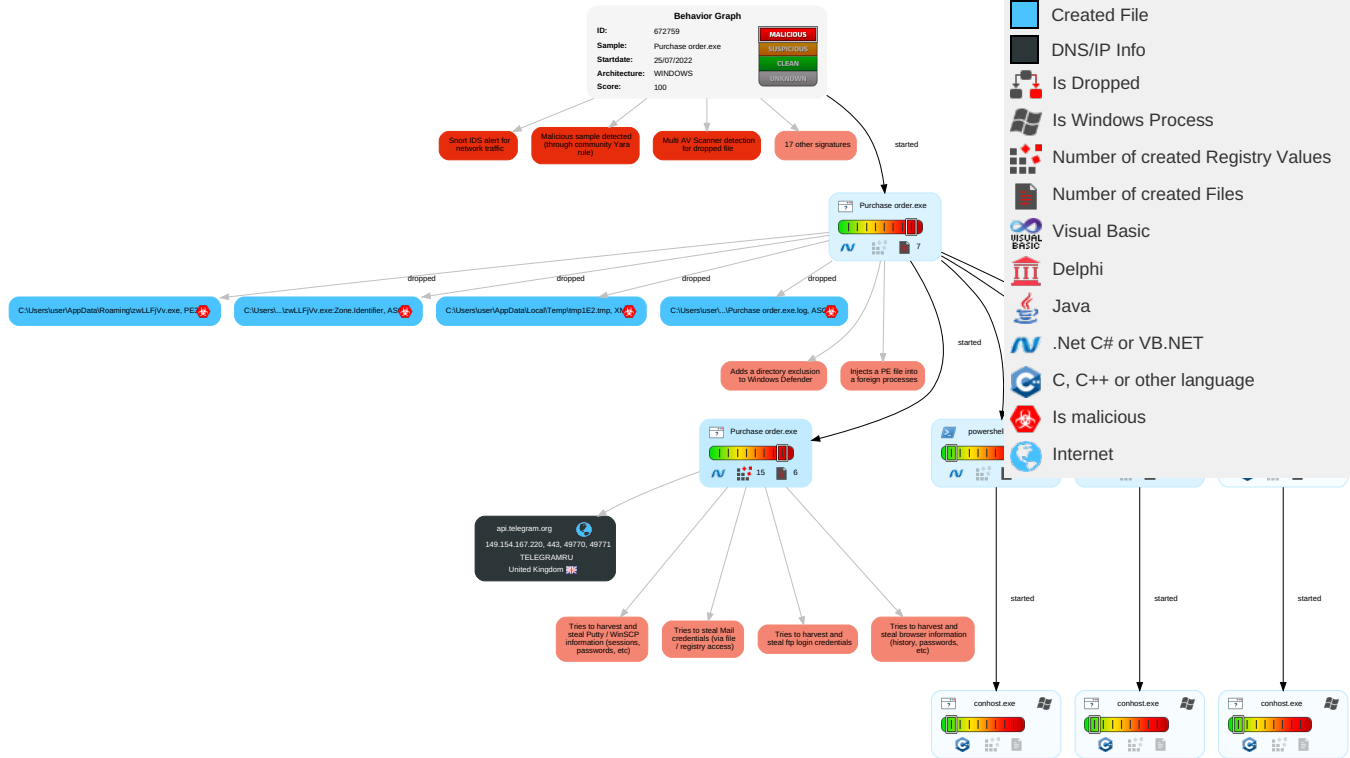


Yara detected Telegram RAT
Yara detected AgentTesla

Mitre Att&ck Matrix

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

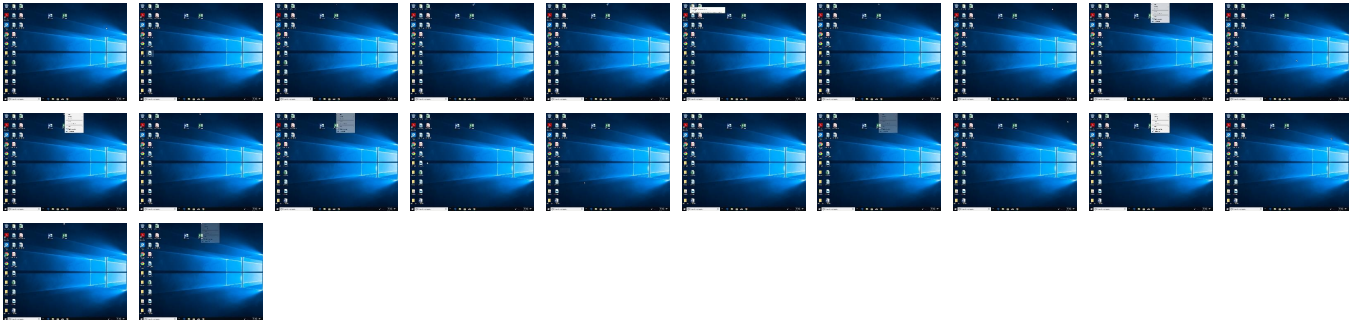
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Purchase order.exe	61%	Virustotal		Browse
Purchase order.exe	29%	Metadefender		Browse
Purchase order.exe	77%	ReversingLabs	ByteCode-MSIL.Trojan.RemL oader	
Purchase order.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\zwLLFjVv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\zwLLFjVv.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Roaming\zwLLFjVv.exe	77%	ReversingLabs	ByteCode-MSIL.Trojan.RemL oader	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.0.Purchase order.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
17.0.Purchase order.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
17.0.Purchase order.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
17.0.Purchase order.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
17.0.Purchase order.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
17.2.Purchase order.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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://8Kj1IVLMB7Pu.org	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://https://8Kj1IVLMB7Pu.orgx	0%	Avira URL Cloud	safe	
http://eloKlh.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.telegram.orgD8	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5573921253:AAHXKq7IrmioCzUGP-9p7lopfbVX0A_ZdQA/sendDocument	false		high

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Purchase order.exe, 00000011.00000002.519664519.0000000002A91000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false		high
http://www.fontbureau.com	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false		high
http://www.fontbureau.com/designersG	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false		high
http://www.fontbureau.com/designers/?	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false		high
http://www.founder.com.cn/cn/bThe	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://https://api.telegram.org	Purchase order.exe, 00000011.00000002.52 4365447.0000000002DE6000.00000004.000008 00.00020000.00000000.sdm	false		high
http://https://8Kj1IVLMB7Pu.org	Purchase order.exe, 00000011.00000002.52 3818002.0000000002D85000.00000004.000008 00.00020000.00000000.sdm, Purchase order.exe, 00000011.00000002.524461213.0000000002DFB00 0.00000004.00000800.00020000.00000000.sdm	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	Purchase order.exe, 00000011.00000002.51 9664519.0000000002A91000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://www.tiro.com	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false		high
http://https://api.ipify.org/%\$startupfolder%	Purchase order.exe, 00000011.00000002.51 9664519.0000000002A91000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	low
http://www.goodfont.co.kr	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://www.typography.netD	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false		high
http://www.founder.com.cn/cn/cThe	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	Purchase order.exe, 00000011.00000002.52 4365447.0000000002DE6000.00000004.000008 00.00020000.00000000.sdm	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Purchase order.exe, 00000000.00000002.33 4385988.0000000006BD2000.00000004.000008 00.00020000.00000000.sdm	false		high
http://https://8Kj1IVLMB7Pu.orgx	Purchase order.exe, 00000011.00000002.52 3818002.0000000002D85000.00000004.000008 00.00020000.00000000.sdm	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://eloKih.com	Purchase order.exe, 00000011.00000002.519664519.0000000002A91000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot5573921253:AAHXKq7IrmioCzUGP-9p7lopfbVX0A_ZdQA/	Purchase order.exe, 00000000.00000002.330214472.0000000003BE1000.00000004.00000800.00020000.00000000.sdmp, Purchase order.exe, 00000011.00000002.514358204.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Purchase order.exe, 00000011.00000000.317109056.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Purchase order.exe, 00000000.00000002.334385988.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejdpaswordPsi/Psi	Purchase order.exe, 00000011.00000002.519664519.0000000002A91000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Purchase order.exe, 00000000.00000002.334385988.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Purchase order.exe, 00000000.00000002.334385988.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot5573921253:AAHXKq7IrmioCzUGP-9p7lopfbVX0A_ZdQA/sendDocumentdocument-----	Purchase order.exe, 00000011.00000002.519664519.0000000002A91000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	Purchase order.exe, 00000000.00000002.334385988.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Purchase order.exe, 00000000.00000002.334385988.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Purchase order.exe, 00000000.00000002.334385988.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Purchase order.exe, 00000000.00000002.334385988.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://api.telegram.org	Purchase order.exe, 00000011.00000002.524849069.0000000002E34000.00000004.00000800.00020000.00000000.sdmp, Purchase order.exe, 00000011.00000002.524461213.0000000002DFB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Purchase order.exe, 00000000.00000002.325636561.0000000002A61000.00000004.00000800.00020000.00000000.sdmp, Purchase order.exe, 00000000.00000002.328322798.0000000002C98000.00000004.00000800.00020000.00000000.sdmp, Purchase order.exe, 00000011.00000002.524365447.0000000002DE6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Purchase order.exe, 00000000.00000002.334385988.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.ipify.org%	Purchase order.exe, 00000011.00000002.519664519.0000000002A91000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://https://api.telegram.orgD8	Purchase order.exe, 00000011.00000002.524849069.0000000002E34000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	672759
Start date and time: 25/07/202211:29:54	2022-07-25 11:29:54 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 35s
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.spyw.evad.winEXE@12/12@2/1
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 1% (good quality ratio 0.6%) - Quality average: 43.4% - Quality standard deviation: 43%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.125.122.176, 20.54.89.106, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:31:21	API Interceptor	587x Sleep call for process: Purchase order.exe modified
11:31:28	API Interceptor	70x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

 No context
--

Domains

 No context
--

ASNs

 No context
--

JA3 Fingerprints

 No context
--

Dropped Files

 No context
--

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase order.exe.log 	
Process:	C:\Users\user\Desktop\Purchase order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFHKHoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCFF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	true
Reputation:	high, 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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72 e6\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\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni .dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22192
Entropy (8bit):	5.602941755239825
Encrypted:	false
SSDEEP:	384:ltCDLiwYdPpY0XHjISBKnwjultIME7nvHg3hlnQML+KfmAV7AZd0MZQvnl++2YZ:EdPpYUB4KwClt/o66LKOpOT+U
MD5:	6BF1CB9177ACA1CF6B315A3A3224A8E4
SHA1:	5B4C05F19B6747A9A0E6E95739EFE50A91A3638C
SHA-256:	77A9F1A9BF84FEE9CFCD40C3966A31BB17396F838C3CE467D841701E517BFCA
SHA-512:	69969FD871FB698B29A22AB3045A277989D38D14BFCAFF050529EBC11E057EFB92B99DA37EA97365F12E8591D1FAD96648F14437D32D064B7A65AAA92E7BFB B
Malicious:	false
Preview:	@...e.....d.....K...f\Y.....M.../.....@.....H.....<@.^.L."My...:P.....Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.....Sy stem.Transactions.<.....):gK..G...\$.1.q.....System.ConfigurationP...../C...J...]).....%Microsoft.PowerShell.Commands.Utility...D.....-D.F.<.;.nt.1System.Configuration.Ins

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_cwyntq2b.npw.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_dz0lxrga.mbt.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_lcn4kimx.j2a.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_t3f3sog0.5s0.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp1E2.tmp 	
Process:	C:\Users\user\Desktop\Purchase order.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1595
Entropy (8bit):	5.146618317444398
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMHEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaixvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTzv
MD5:	7449E54286431D705E80708396FEB892
SHA1:	FAE43DA26541628FBFA662397C6E3B52183EC31E
SHA-256:	1435B3DA2DF4C63468DFED13CE6394CD8D2594167E3A0DF78F7AACAB548D810B
SHA-512:	8A64BD2DB3671786AD58D5155C979FA36D7F88F725E8DCC9C59BF0AD03198A44D60C63D0B25CFFD4A40D5F9D08601C0C7000C4B2E59E12D4D69DFC9B0D499BA
Malicious:	true
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\q0j300ya.blp\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\Purchase order.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@C.....g...8.....

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

Process:	C:\Users\user\Desktop\Purchase order.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	762368
Entropy (8bit):	7.557750533188712
Encrypted:	false
SSDEEP:	12288:AiekMj/31humhJGu/8k9kKuB/04ZZmz3Cr/KNdS2iyNAICj+:Fcmui5kKMc4Lu3rNYwSICS
MD5:	24B0BE710ED42B1EC10224DB8DB55BF6
SHA1:	597BCE6E93351125632E9B92FB2CA35FCA8BC75D
SHA-256:	89823F7C472A09C6062578082579DA7F8CDB093C99DE1A7C92AFA5D741C7316
SHA-512:	810FB68F0199F3BF35B7E8894B9A978AD4533DE9A9B8C6D0E39E260688AE77C6F922A71557F0812FDB815951500D6712EB16D6CAE847701C5E0AEC9E91AF3BD4
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: Metadefender, Detection: 29%, Browse - Antivirus: ReversingLabs, Detection: 77%
Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$.PE..L..@.`.....0..z...&.....@.. ..@.....K.....".....w......H.....text...y...z.....`.rsrc.....\$.@..@.rel oc.....@..B.....H.....H.....8{.3.....0.....{...8.....}...8.....}...8...s...}...8...s...}...8....& ...8...8.....E.....8.....*...0.....{...8.....}...8.....}...8...s...}...8...s...}...8....&8...8.....E.....8.....}...8...*0.....{...8.....}...8.....} 8....s....}...8....s....}...8....s....}...8....(....&8...8.....E.....8.....}...8...*0.....{...8.....}...8.....}(...

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

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

C:\Users\user\Documents\20220725\PowerShell_transcript.123716.NRW_8MvJ.20220725113126.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):	3503
Entropy (8bit):	5.281115465537372
Encrypted:	false
SSDEEP:	96:BZ4gjkN+qDo1ZU3ZBjkN+qDo1Z2qNP0cP0cP01ZO:0LbbB
MD5:	C4711DA066B3F4BA4A5DB3273B68C574
SHA1:	F058150793E7C046701061D019DACF4639B01DE4
SHA-256:	656BE0FDFB384A86DBAA1C8C2D4B29EC23DA679055B7CA2B4F800AE0FB757238
SHA-512:	2D0BEA90563C55BEED9DC72D6544F449EE6DB017C49F0968A7D0E8FAE4BF673CE345353B32DE602042FA9BD41B0AB26E9D23EC88F8731FD557AFF3519EA558D
Malicious:	false
Preview:	.*****.Windows PowerShell transcript start..Start time: 20220725113127..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 123716 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Purchase order.exe..Process ID: 3628..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: 20220725113127..*****.PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Purchase order.exe..*****.Command start time: 20220725113518..*****.PS>TerminatingError(Add-MpPreference): "A positional parameter cannot be found

C:\Users\user\Documents\20220725\PowerShell_transcript.123716.RgD01ff5.20220725113128.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):	5781
Entropy (8bit):	5.403428760580261
Encrypted:	false
SSDEEP:	96:BZAJkNvqDo1ZiZNjkNvqDo1Z6sSUjZajkNvqDo1ZxNkVZK:l
MD5:	185E0761D6F263BA9BC7E1A1E296BDA3
SHA1:	EF49535B7049E46E2A887B23DB64FA81B48D8DA2
SHA-256:	23BBFBFE0E32757C66A3D5554A0E217965DA27DD4771FAADB6202BFA73E01151B
SHA-512:	9505B24D0FFBC96BDEAD77DE8C7920D1093FD56D2F44A5B1A7C4EE745873E74805EC80C7893C4C7FBC7BEC72BDC6201FBB70BD2C416B0293CC248D0F7B6EAB0
Malicious:	false
Preview:	.*****.Windows PowerShell transcript start..Start time: 20220725113131..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 123716 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\zwLLFjVv.exe..Process ID: 1036..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: 20220725113131..*****.PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\zwLLFjVv.exe..*****.Windows PowerShell transcript start..Start time: 20220725113606..Username: computer\user..RunAs User: computer\user..C

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.557750533188712
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:	762368
MD5:	24b0be710ed42b1ec10224db8db55bf6
SHA1:	597bce6e93351125632e9b92fb2ca35fca8bc75d
SHA256:	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316
SHA512:	810fb68f0199f3bf35b7e8894b9a978ad4533de9a9b8c6d0e39e260688ae77c6f922a71557f0812fdb815951500d6712eb16d6cae847701c5e0aec9e91af3bd4
SSDEEP:	12288:AiekMj/31humhJGu/8k9kKuB/04ZZmz3Cr/KNdS2iyNAICj+:FcnumiU5kKMc4Lu3rNYwSICS
TLSH:	12F4CF1A762BDD03C27C03B6C5C6145883F08606D16AD7CB6FDA62D61A03BEADDC9787
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....\$......PE..L...@.`.....0..z...&.....@..@.....

File Icon



Icon Hash: b271c0cecce47182

Static PE Info

General

Entrypoint:	0x4b990e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xF8609E40 [Thu Jan 19 02:38:56 2102 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction

jmp dword ptr [00402000h]

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

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

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb98c0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xba000	0x22bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb9877	0x1c	.text
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	

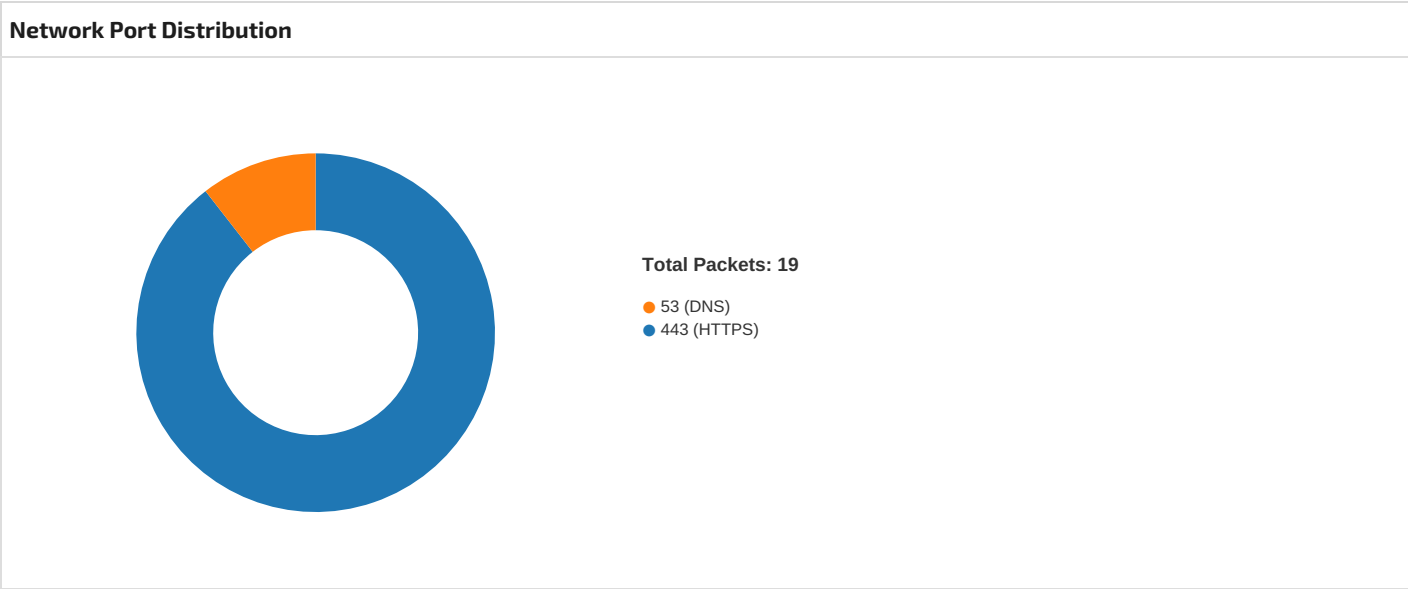
Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb7914	0xb7a00	False	0.8241629084411164	data	7.562644649566881	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x22bc	0x2400	False	0.8819444444444444	data	7.431495246733818	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0xba0e8	0x1e5b	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xbbf44	0x14	data		
RT_VERSION	0xbbf58	0x364	data		

Imports	
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4149.154.167.2 20497704432851779 07/25/22- 11:31:56.998694	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49770	443	192.168.2.4	149.154.167.220



TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 25, 2022 11:31:56.344516039 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:56.344588995 CEST	443	49770	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:56.344723940 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:56.401355982 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:56.401386023 CEST	443	49770	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:56.497241974 CEST	443	49770	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:56.497452974 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:56.500705004 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:56.500732899 CEST	443	49770	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:56.501100063 CEST	443	49770	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:56.615852118 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:56.968137026 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:56.996541977 CEST	443	49770	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:56.998573065 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:57.044523954 CEST	443	49770	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:57.097374916 CEST	443	49770	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:57.097480059 CEST	443	49770	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:57.097645998 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:57.100749016 CEST	49770	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:59.331939936 CEST	49771	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:59.331970930 CEST	443	49771	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:59.332041025 CEST	49771	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:59.332478046 CEST	49771	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:59.332493067 CEST	443	49771	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:59.389746904 CEST	443	49771	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:59.394855022 CEST	49771	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:59.394885063 CEST	443	49771	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:59.443284035 CEST	443	49771	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:59.443842888 CEST	49771	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:59.443865061 CEST	443	49771	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:59.597321987 CEST	443	49771	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:59.597443104 CEST	443	49771	149.154.167.220	192.168.2.4
Jul 25, 2022 11:31:59.597534895 CEST	49771	443	192.168.2.4	149.154.167.220
Jul 25, 2022 11:31:59.603838921 CEST	49771	443	192.168.2.4	149.154.167.220

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 25, 2022 11:31:56.290285110 CEST	60758	53	192.168.2.4	8.8.8.8
Jul 25, 2022 11:31:56.309506893 CEST	53	60758	8.8.8.8	192.168.2.4
Jul 25, 2022 11:31:59.313266993 CEST	60647	53	192.168.2.4	8.8.8.8
Jul 25, 2022 11:31:59.330569029 CEST	53	60647	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 25, 2022 11:31:56.290285110 CEST	192.168.2.4	8.8.8.8	0x5e15	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jul 25, 2022 11:31:59.313266993 CEST	192.168.2.4	8.8.8.8	0xa273	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 25, 2022 11:31:56.309506893 CEST	8.8.8.8	192.168.2.4	0x5e15	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jul 25, 2022 11:31:59.330569029 CEST	8.8.8.8	192.168.2.4	0xa273	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49770	149.154.167.220	443	C:\Users\user\Desktop\Purchase order.exe

[illegible]

System Behavior

Analysis Process: Purchase order.exe PID: 5756, Parent PID: 5900

General

Target ID:	0
Start time:	11:31:02
Start date:	25/07/2022
Path:	C:\Users\user\Desktop\Purchase order.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase order.exe"
Imagebase:	0x710000
File size:	762368 bytes
MD5 hash:	24B0BE710ED42B1EC10224DB8DB55BF6
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: 00000000.00000002.330214472.0000000003BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.330214472.0000000003BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.328322798.0000000002C98000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.325636561.0000000002A61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DC7CF06	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	6DC7CF06	unknown
C:\Users\user\AppData\Roaming\zwLLFjVv.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	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\zwLLFjVv.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	6C01DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1E2.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C017038	GetTempFile NameW
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	6DF8C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1E2.tmp	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zwLLFjVv.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 40 fd 60 fd 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 7a 0b 00 00 26 00 00 00 00 00 0e fd 0b 00 00 20 00 00 00 fd 0b 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 00 0c 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PEL@`0z& @ @	success or wait	3	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\zwLLFjVv.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	6C01DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\mp1E2.tmp	0	1595	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" x mlns="http://schemas.mic rosoft .com/windows/2004/02/m it/task"> <RegistrationInfo> <Date>2014-10- 25T14:27:44.8929027</ Date> <Author>computer\user </Author> </RegistrationInfo>	success or wait	1	6C011B4F	WriteFile

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	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DF8C907	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	6DC55705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefaf3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile	

Analysis Process: powershell.exe PID: 3628, Parent PID: 5756	
General	
Target ID:	8
Start time:	11:31:24
Start date:	25/07/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\Purchase order.exe
Imagebase:	0x10000
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	6DC7CF06	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	6DC7CF06	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	6BF75B28	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	6BF75B28	unknown	
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_lcn4kimx.j2a.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C011E60	CreateFileW	
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_cwyntq2b.npw.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C011E60	CreateFileW	
C:\Users\user\Documents\20220725	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW	
C:\Users\user\Documents\20220725\PowerShell_transcript.123716.NRW_8MvJ.20220725113126.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6C011E60	CreateFileW	

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lcn4kimx.j2a.ps1	success or wait	1	6C016A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cwyntq2b.npw.psm1	success or wait	1	6C016A95	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_lcn4kimx.j2a.ps1	0	1	31	1	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_cwyntq2b.npw.psm1	0	1	31	1	success or wait	1	6C011B4F	WriteFile
C:\Users\user\Documents\20220725\PowerShell_transcript.123716.NRW_8MvJ.20220725113126.txt	0	3	ff		success or wait	1	6C011B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1088	2044	01 00 00 00 00 00 00 00 01 00 00 00 fd 37 fd 2c fd 66 69 44 fd 17 fd 1a fd 0d fd fd fd 00 00 00 0e 00 2a 00 4d 69 63 72 6f 73 6f 66 74 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 49 6e 66 72 61 73 74 72 75 63 74 75 72 65 2e 4e 61 74 69 76 65 00 00 00 08 00 03 00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40	7.fiD*Microsoft.Managem ent.Inf rastructure.NativeT@>@ @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@	success or wait	10	6DF476FC	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	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlibb1a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DC61F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	6DC3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6DC3D72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C011B4F	ReadFile

Analysis Process: conhost.exe PID: 6032, Parent PID: 3628

General

Target ID:	10
Start time:	11:31:24
Start date:	25/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: powershell.exe PID: 1036, Parent PID: 5756

General

Target ID:	12
Start time:	11:31:25
Start date:	25/07/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\zwLLFjVv.exe
Imagebase:	0x10000
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	6DC7CF06	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	6DC7CF06	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	6BF75B28	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	6BF75B28	unknown
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_t3f3sog0.5s0.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_dz0lxrga.mbt.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\Documents\20220725\PowerShell_transcript.123716.RgDO1ffS.20220725113128.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6C011E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_t3f3sog0.5s0.ps1	success or wait	1	6C016A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dz0lxrga.mbt.psm1	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	167	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	186	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	207	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	236	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	244	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	253	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
unknown	261	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF75B28	unknown
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_t3f3sog0.5s0.ps1	0	1	31	1	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_dz0lxrga.mbt.psm1	0	1	31	1	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_lcn4kimx.j2a.ps1	0	3	31	1	success or wait	1	6C011B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lcn4kimx.j2a.ps1	3	675	75 6e 6b 6e 6f 77 6e	unknown	success or wait	44	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 64 14 00 00 19 00 00 00 4b 0c fd 03 66 08 5c 08 59 08 00 00 fd 01 4d 00 07 00 2f 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@edKfYM/@	success or wait	1	6DF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6DF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 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 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 45 4d 00	T@>@@V@H@X@[@N T@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@:@BMDmE;@:@<@ <@<@W@M@EM	success or wait	11	6DF476FC	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	6DC55705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC5CA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\lb219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DC61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6DC6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\lb219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C011B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	3	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	3	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	59	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C011B4F	ReadFile

Analysis Process: conhost.exe PID: 5292, Parent PID: 1036

General

Target ID:	14
Start time:	11:31:26
Start date:	25/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6172, Parent PID: 5756

General

Target ID:	15
Start time:	11:31:26
Start date:	25/07/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\zwLLFjVv" /XML "C:\Users\user\AppData\Local\Temp\tmp1E2.tmp
Imagebase:	0x1320000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1E2.tmp	unknown	2	success or wait	1	132AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1E2.tmp	unknown	1596	success or wait	1	132ABD9	ReadFile

Analysis Process: conhost.exe PID: 6352, Parent PID: 6172

General

Target ID:	16
Start time:	11:31:29
Start date:	25/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA77DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Purchase order.exe PID: 6444, Parent PID: 5756

General

Target ID:	17
Start time:	11:31:32
Start date:	25/07/2022
Path:	C:\Users\user\Desktop\Purchase order.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase order.exe

Imagebase:	0x720000
File size:	762368 bytes
MD5 hash:	24B0BE710ED42B1EC10224DB8DB55BF6
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: 00000011.00000002.514358204.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000002.514358204.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000000.317899591.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000000.317899591.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000000.319090095.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000000.319090095.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000000.317109056.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000000.317109056.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.519664519.0000000002A91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000011.00000002.519664519.0000000002A91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.519664519.0000000002A91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000000.319891552.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000000.319891552.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DC7CF06	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	6DC7CF06	unknown	
C:\Users\user\AppData\Roaming\q0j300ya.blp	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW	
C:\Users\user\AppData\Roaming\q0j300ya.blp\Chrome	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW	
C:\Users\user\AppData\Roaming\q0j300ya.blp\Chrome\Default	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW	
C:\Users\user\AppData\Roaming\q0j300ya.blp\Chrome\Default\Cookies	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	6C01DD66	CopyFileW	

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\q0j300ya.blp\Chrome\Default\Cookies	success or wait	1	6C016A95	DeleteFileW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Disassembly

 No disassembly