

JOeSandbox Cloud BASIC



ID: 679221

Sample Name: wKQpOZ58GI

Cookbook: default.jbs

Time: 12:22:04

Date: 05/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report wKQpOZ58Gl	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	4
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	6
AV Detection	6
Networking	6
Key, Mouse, Clipboard, Microphone and Screen Capturing	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	7
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
Private	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\wKQpOZ58Gl.exe.log	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2xb4spy5.adr.ps1	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h1mfggue.sz5.psm1	15
C:\Users\user\AppData\Local\Temp\tmp92BC.tmp	16
C:\Users\user\AppData\Roaming\kqruryFrIFc.exe	16
C:\Users\user\AppData\Roaming\kqruryFrIFc.exe:Zone.Identifier	16
C:\Users\user\AppData\Roaming\kbu4uc5.tjf\Chrome\Default\Cookies	17
C:\Users\user\Documents\20220805\PowerShell_transcript.390120.zw_Mb_9m.20220805122336.txt	17
Static File Info	17
General	17
File Icon	18
Static PE Info	18
General	18
Entrypoint Preview	18
Data Directories	20
Sections	20
Resources	20
Imports	20

Network Behavior	21
Snort IDS Alerts	21
Network Port Distribution	21
TCP Packets	21
UDP Packets	22
DNS Queries	22
DNS Answers	22
HTTP Request Dependency Graph	22
HTTPS Proxied Packets	22
Statistics	23
Behavior	23
System Behavior	24
Analysis Process: wKQpOZ58Gl.exePID: 3676, Parent PID: 6060	24
General	24
File Activities	24
File Created	24
File Deleted	25
File Written	25
File Read	26
Analysis Process: powershell.exePID: 6088, Parent PID: 3676	27
General	27
File Activities	27
File Created	27
File Deleted	28
File Written	28
File Read	29
Analysis Process: conhost.exePID: 6084, Parent PID: 6088	32
General	32
Analysis Process: schtasks.exePID: 6124, Parent PID: 3676	32
General	32
File Activities	33
File Read	33
Analysis Process: conhost.exePID: 3772, Parent PID: 6124	33
General	33
Analysis Process: wKQpOZ58Gl.exePID: 3276, Parent PID: 3676	33
General	33
Analysis Process: wKQpOZ58Gl.exePID: 3760, Parent PID: 3676	33
General	33
File Activities	34
File Created	34
File Deleted	34
File Written	34
File Read	35
Registry Activities	35
Disassembly	36

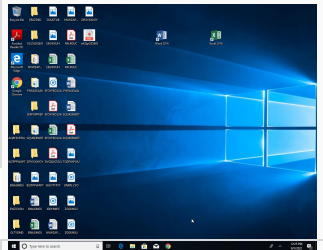
Windows Analysis Report

wKQp0Z58GL

Overview

General Information

Sample Name:	wKQpOZ58GI (renamed file extension from none to exe)
Analysis ID:	679221
MD5:	f7c9cf1410373a6..
SHA1:	97cf7689f3b6dfd..
SHA256:	b5a23c2ef617a9..
Tags:	exe
Infos:	



Detection

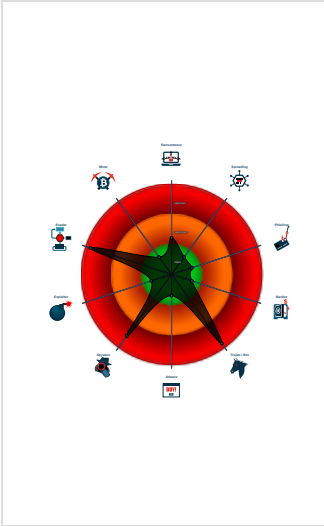
The figure displays the AgentTesla logo, which consists of a red rounded rectangle with the text "AgentTesla" in white. Above the logo is a vertical bar composed of four colored segments: red (top), brown, green, and grey (bottom). Each segment contains a white or grey text label: "MALICIOUS" (red), "SUSPICIOUS" (brown), "CLEAN" (green), and "UNKNOWN" (grey). The "MALICIOUS" segment is highlighted with a white border and a white arrow pointing right.

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
- Antivirus / Scanner detection for sub...
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop...
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi...
- Tries to harvest and steal Putty / W...

Classification



Process Tree

- System is w10x64
-  **wKqP0Z58Gl.exe** (PID: 3676 cmdline: "C:\Users\user\Desktop\wKqP0Z58Gl.exe" MD5: F7C9CF1410373A60A5C5A5E02AA4BD3C)
 -  **powershell.exe** (PID: 6088 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roamin gl\kqruryFrIc.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
 -  **conhost.exe** (PID: 6084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 -  **schtasks.exe** (PID: 6124 cmdline: C:\Windows\System32\schtasks.exe /Create /TN "Updates\kqruryFrIc" /XML "C:\Users\user\AppData\Local\Temp\tmp92BC.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
 -  **conhost.exe** (PID: 3772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 -  **wKqP0Z58Gl.exe** (PID: 3276 cmdline: C:\Users\user\Desktop\wKqP0Z58Gl.exe MD5: F7C9CF1410373A60A5C5A5E02AA4BD3C)
 -  **wKqP0Z58Gl.exe** (PID: 3760 cmdline: C:\Users\user\Desktop\wKqP0Z58Gl.exe MD5: F7C9CF1410373A60A5C5A5E02AA4BD3C)
- cleanup

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5589784704:AAHKB3hx6EncDiLnSpjVqiBsp072Mevw-S8/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1428352550",
  "Chat URL": "https://api.telegram.org/bot5589784704:AAHB3hx6EncDiLnSpjVqiBsp072Mevw-S8/sendDocument"
}
```

Yara Signatures

Memory Dumps				
Source	Rule	Description	Author	Strings
0000000E.00000000.431826209.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000000.431826209.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000E.00000000.431826209.0000000000402000.0000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x300eb:\$a13: get_DnsResolver 0x2e909:\$a20: get_LastAccessed 0x30a7f:\$a27: set_InternalServerPort 0x30d9b:\$a30: set_GuidMasterKey 0x2ea10:\$a33: get_Clipboard 0x2ea1e:\$a34: get_Keyboard 0x2fd1b:\$a35: get_ShiftKeyDown 0x2fd2c:\$a36: get_AltKeyDown 0x2ea2b:\$a37: get_Password 0x2f4cb:\$a38: get_PasswordHash 0x304eb:\$a39: get_DefaultCredentials
00000000.00000002.441112036.000000000272A000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000E.00000002.633873650.0000000002901000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
0.2.wKQpOZ58Gl.exe.4084120.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.wKQpOZ58Gl.exe.4084120.9.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.wKQpOZ58Gl.exe.4084120.9.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	0x30e60:\$s10: logins 0x308c7:\$s11: credential 0x2ce10:\$g1: get_Clipboard 0x2ce1e:\$g2: get_Keyboard 0x2ce2b:\$g3: get_Password 0x2e10b:\$g4: get_CtrlKeyDown 0x2e11b:\$g5: get_ShiftKeyDown 0x2e12c:\$g6: get_AltKeyDown
0.2.wKQpOZ58Gl.exe.4084120.9.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x2e4eb:\$a13: get_DnsResolver 0x2cd09:\$a20: get_LastAccessed 0x2ee7f:\$a27: set_InternalServerPort 0x2f19b:\$a30: set_GuidMasterKey 0x2ce10:\$a33: get_Clipboard 0x2ce1e:\$a34: get_Keyboard 0x2e11b:\$a35: get_ShiftKeyDown 0x2e12c:\$a36: get_AltKeyDown 0x2ce2b:\$a37: get_Password 0x2d8cb:\$a38: get_PasswordHash 0x2e8eb:\$a39: get_DefaultCredentials
0.2.wKQpOZ58Gl.exe.404f900.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 23 entries				

Sigma Signatures	
	No Sigma rule has matched

Snort Signatures	
ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.6 - Destination IP: 149.154.167.220	
Timestamp:	192.168.2.6149.154.167.220497834432851779 08/05/22-12:24:11.625878
SID:	2851779
Source Port:	49783
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped 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

Key, Mouse, Clipboard, Microphone and Screen Capturing



Installs a global keyboard hook

System Summary



Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation



.NET source code contains potential unpacker

Boot Survival



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

Malware Analysis System Evasion



Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion



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



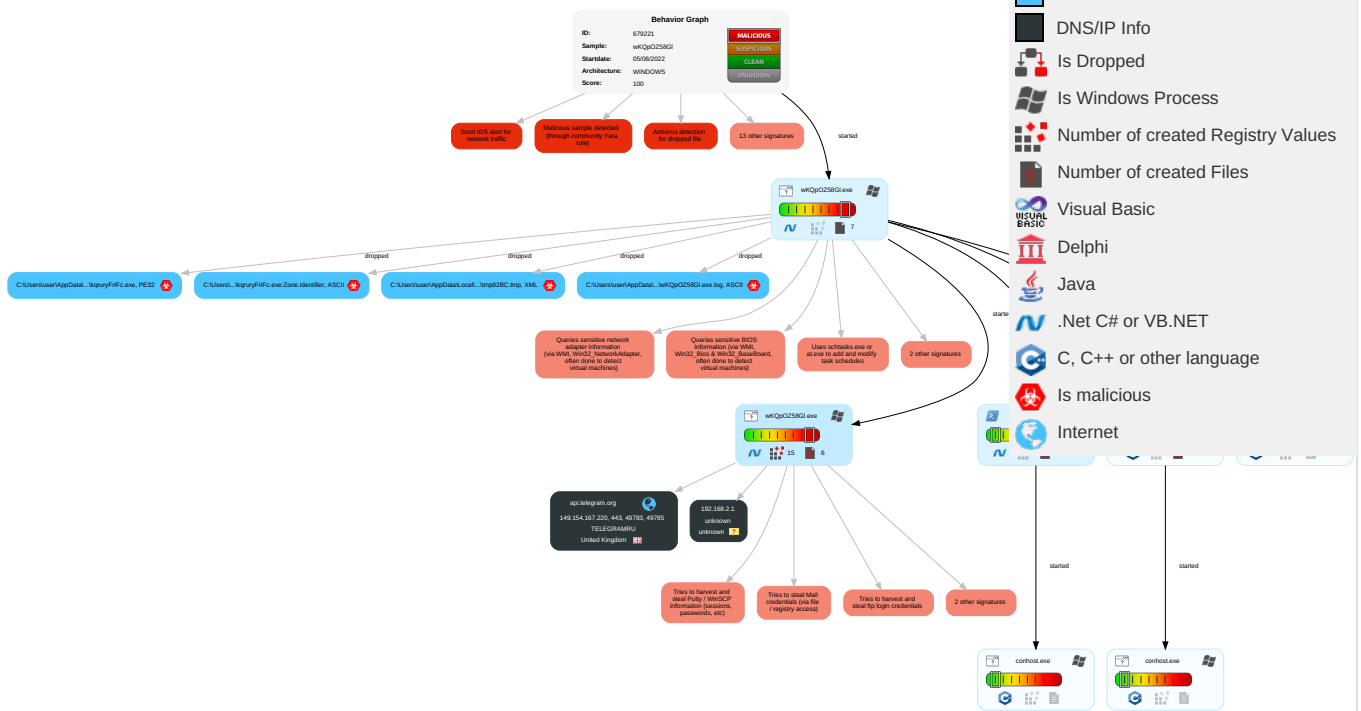
Yara detected Telegram RAT

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 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 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Deobfuscate/Decode Files or Information	1 1 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	At (Linux)	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 1 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	1 Clipboard Data	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

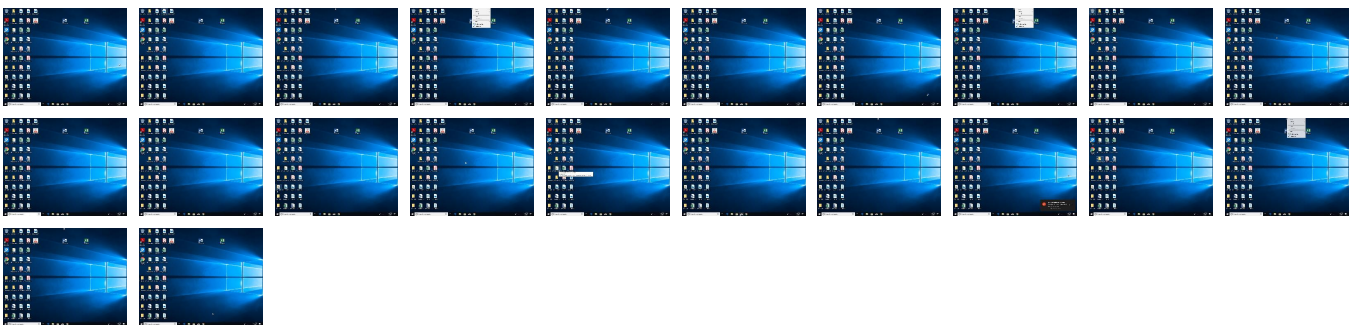
Behavior Graph



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
wKQpOZ58Gl.exe	58%	Virustotal		Browse
wKQpOZ58Gl.exe	26%	Metadefender		Browse
wKQpOZ58Gl.exe	69%	ReversingLabs	Win32.Trojan.Wore flint	
wKQpOZ58Gl.exe	100%	Avira	TR/AD.AgentTesla .gcmza	
wKQpOZ58Gl.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kqruryFrlFc.exe	100%	Avira	TR/AD.AgentTesla .gcmza	
C:\Users\user\AppData\Roaming\kqruryFrlFc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kqruryFrlFc.exe	58%	Virustotal		Browse
C:\Users\user\AppData\Roaming\kqruryFrlFc.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Roaming\kqruryFrlFc.exe	69%	ReversingLabs	Win32.Trojan.Wore flint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.wKQpOZ58GI.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://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://dhp6cb4d3QXSx5sRI.net	0%	Avira URL Cloud	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://sOkRpA.com	0%	Virustotal		Browse
http://sOkRpA.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejdpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.telegram.orgD8	0%	URL Reputation	safe	

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/bot5589784704:AAHKB3hx6EncDiLmSpjVqiBsp072Mevw-S8/sendDocument	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	wKQpOZ58GI.exe, 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot5589784704:AAHKB3hx6EncDiLmSpjVqiBsp072Mevw-S8/	wKQpOZ58GI.exe, 00000000.00000002.447462860.0000000004018000.00000004.00000800.00020000.00000000.sdmp, wKQpOZ58GI.exe, 0000000E.00000000.431826209.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.telegram.org	wKQpOZ58GI.exe, 0000000E.00000002.639234728.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot5589784704:AAHKB3hx6EncDiLmSpjVqiBsp072Mevw-S8/sendDocumentdocument-----	wKQpOZ58GI.exe, 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	wKQpOZ58GI.exe, 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.tiro.com	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://github.com/princ3od/MaterialSurfaceKhhttps://www.linkedin.com/in/princ3od/%princ3od	wKQpOZ58GI.exe, kqruryFrIFc.exe.0.dr	false		high
http://www.fontbureau.com/designers	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org/%startpfolder%	wKQpOZ58GI.exe, 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://www.goodfont.co.kr	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://dhp6cb4d3QXSx5sRI.net	wKQpOZ58GI.exe, 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp, wKQpOZ58GI.exe, 0000000E.00000002.639326716.0000000002C66000.00000004.00000800.00020000.00000000.sdmp, wKQpOZ58GI.exe, 0000000E.00000002.639182904.0000000002C49000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.sajatytypeworks.com	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.typography.netD	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://fontfabrik.com	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://sOkRpA.com	wKQpOZ58GI.exe, 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.telegram.org4	wKQpOZ58GI.exe, 0000000E.00000002.639234728.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	wKQpOZ58GI.exe, 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.urwpp.deDPlease	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://api.telegram.org	wKQpOZ58GI.exe, 0000000E.00000002.639326716.0000000002C66000.00000004.00000800.00020000.00000000.sdmp, wKQpOZ58GI.exe, 0000000E.00000002.639615093.0000000002C9E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	wKQpOZ58GI.exe, 00000000.00000002.441112036.000000000272A000.00000004.00000800.00020000.00000000.sdmp, wKQpOZ58GI.exe, 0000000E.00000002.639234728.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	wKQpOZ58GI.exe, 00000000.00000002.455171417.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.ipify.org%	wKQpOZ58GI.exe, 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://https://api.telegram.orgD8	wKQpOZ58GI.exe, 0000000E.00000002.639615093.0000000002C9E000.00000004.00000800.00020000.00000000.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679221
Start date and time: 05/08/2022 12:22:04	2022-08-05 12:22:04 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wKQpOZ58GI (renamed file extension from none to 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:	26
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@11/9@2/2

EGA Information:	Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Adjust boot time - Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.
- Report size exceeded maximum capacity and may have missing b ehavior information.
- Report size getting too big, t oo many NtAllocateVirtualMemory calls found.
- Report size getting too big, t oo many NtOpenKeyEx calls found.
- Report size getting too big, t oo many NtProtectVirtualMemory calls found.
- Report size getting too big, t oo many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:23:31	API Interceptor	507x Sleep call for process: wKQpOZ58Gl.exe modified
12:23:38	API Interceptor	22x 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\wKQpOZ58Gl.exe.log 

Process:	C:\Users\user\Desktop\wKQpOZ58Gl.exe
File Type:	ASCII text, with CRLF line terminators

Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA277EECB2A3CBD03CB7E8E23D736000F890B17AA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
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, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System4f0a7eefa3cd3e0ba98b5ebddbbbc72e6\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\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\lb219d4630d26b88041b59c21

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):	22140
Entropy (8bit):	5.606020442711728
Encrypted:	false
SSDEEP:	384:2tCDBCVRpIziWlovXSB+kjultlQ87nvOL3Ss3YEMtEm+e+AV7kjWDwLYI++BYv:CRplw2o/4NCitLzDKK4oKB
MD5:	5194DEF9DA74FB9BDB66C72345F51F77
SHA1:	E133CA2899438B5BFFC0D9C07B239DA11FB7A027
SHA-256:	B227685E644F4F90A63543D29B18F2B1066913A43E2B4D80550828EFEF49481F
SHA-512:	F304A557D7931353E5D708AA853EDA34B3736852BC741B6D0BA7CA020483D066BDA7150689A813F038DD51FE4027CAA14FFAE949B8008A3955FDEADAB7D0E948
Malicious:	false
Reputation:	low
Preview:	@...e.....W.....>y.....@.....H.....<@.^L."My.....Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managem 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_2xb4spy5.adr.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_h1mfggue.sz5.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6A E
Malicious:	true
Preview:	[ZoneTransfer]....Zoneld=0

C:\Users\user\AppData\Roaming\lkbu4uc5.tjf\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\lwKQpOZ58Gl.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoplvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBoplvZXC/aIX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1AB8B57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Preview:	SQLite format 3.....@C......g... .8.....

C:\Users\user\Documents\20220805\PowerShell_transcript.390120.zw_Mb_9m.20220805122336.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):	5823
Entropy (8bit):	5.379640905451343
Encrypted:	false
SSDEEP:	96:BZyTLRNbtyqDo1ZerZsTLRNbtyqDo1ZaHt5tPtjZsTLRNbtyqDo1ZRgt/ttFZy:KTQtDt2B11c
MD5:	AA51436F359F179B13C378A25400B57B
SHA1:	5475ECFCCB96DDC21AEE9E1F7AF15CB7FC631709
SHA-256:	0A69FABF20881D38889AD87BB59058651DAD9B9E449BD4E668ADE2F244E4E7E3
SHA-512:	2C53C83181B92B4F64766FD51445E641B921AD543BC48604E8DF0074ED995EAAA3710B1DF06745063C682AA1995C2C2045EDB76A5FF3B314030EBBD53D3F5DE
Malicious:	false
Preview:	.*****.Windows PowerShell transcript start..Start time: 20220805122338..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 390120 (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\kqruryFrIFc.exe..Process ID: 6088..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCCompatibleVersions: 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: 20220805122338..*****.PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData ta\Roaming\kqruryFrIFc.exe..*****.Windows PowerShell transcript start..Start time: 20220805122644..Username: computer\user..RunAs User: DES

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.692214428514328
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:	wKQpOZ58Gl.exe
File size:	801280
MD5:	f7c9cf1410373a60a5c5a5e02aa4bd3c

SHA1:	97cf7689f3b6dfd0efd37e7f16aa1bd2cfe537de
SHA256:	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245
SHA512:	cf5bf661e5a61d3d64bae9db4d0ffadabc37ba0afe9bec668f8c284d0b37627658744b6ef9d12976f191a96462bc997a6a9f426ca1b1e48785f41b13b9ec64f
SSDEEP:	12288:hk2xg+ugGp2SrKUhwx3YjusvkRgutp43ARSepVIAnlFxCn9nLtzHeb:y2xgP01D3tRgutOzepVIAILGnc
TLSH:	0205E090B9689B22D67EE7F8947121106BF17C66252AE79D2EC134CE0CB3F944E31E53
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......PE.L.....h.....0..>... ..@....@.....@.....@.....

File Icon



Icon Hash:	13332f0f0f3b3313
------------	------------------

Static PE Info

General

Entrypoint:	0x4c3e96
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xED6817C1 [Mon Mar 19 19:00:17 2096 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[ccv] =
```

Page 10 of 10

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

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc3e44	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x14f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc3e28	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	0xc1e9c	0xc2000	False	0.8389678640463918	data	7.704114614834008	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x14f8	0x1600	False	0.2373934659090909	data	4.363906918934409	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0xc40e8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_GROUP_ICON	0xc5190	0x14	data		
RT_VERSION	0xc51a4	0x354	data		

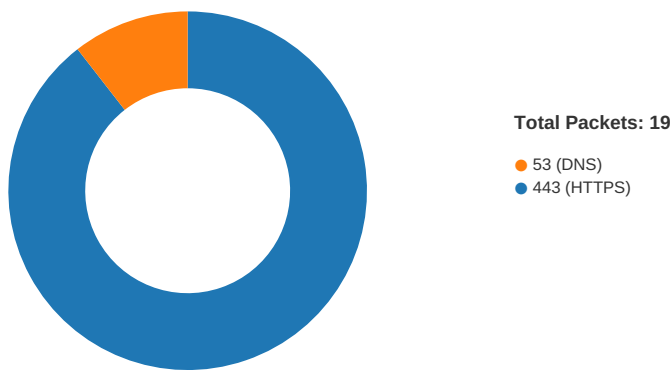
Imports	
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

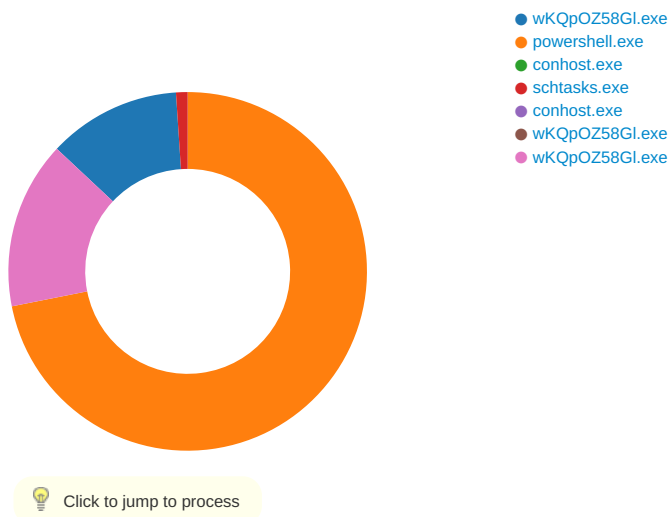
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6149.154.167.2 20497834432851779 08/05/22- 12:24:11.625878	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49783	443	192.168.2.6	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:24:10.854499102 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:10.854537964 CEST	443	49783	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:10.854635954 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:10.924236059 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:10.924259901 CEST	443	49783	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:10.994270086 CEST	443	49783	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:10.994432926 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:11.000766993 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:11.000791073 CEST	443	49783	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:11.001038074 CEST	443	49783	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:11.059721947 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:11.595803976 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:11.622961998 CEST	443	49783	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:11.625746965 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:11.667386055 CEST	443	49783	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:11.726914883 CEST	443	49783	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:11.727098942 CEST	443	49783	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:11.727216005 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:11.728471994 CEST	49783	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:15.063647032 CEST	49785	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:15.063714027 CEST	443	49785	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:15.063843012 CEST	49785	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:15.064291000 CEST	49785	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:15.064317942 CEST	443	49785	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:15.123514891 CEST	443	49785	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:15.128974915 CEST	49785	443	192.168.2.6	149.154.167.220
Aug 5, 2022 12:24:15.129007101 CEST	443	49785	149.154.167.220	192.168.2.6
Aug 5, 2022 12:24:15.182610989 CEST	443	49785	149.154.167.220	192.168.2.6



System Behavior

Analysis Process: wKQpOZ58Gl.exe PID: 3676, Parent PID: 6060

General

Target ID:	0
Start time:	12:23:11
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\wKQpOZ58Gl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\wKQpOZ58Gl.exe"
Imagebase:	0x10000
File size:	801280 bytes
MD5 hash:	F7C9CF1410373A60A5C5A5E02AA4BD3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.441112036.000000000272A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.447462860.0000000004018000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.447462860.0000000004018000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.447462860.0000000004018000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6CE2CF06	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	6CE2CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kqruryFrIFc.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	6BC7DD66	CopyFileW
C:\Users\user\AppData\Roaming\kqruryFrIFc.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	6BC7DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp92BC.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6BC77038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR\v4.0.32\UsageLogs\wKQpOZ58Gl.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D13C78D	CreateFileW

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp92BC.tmp				success or wait	1	6BC76A95	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kqruryFrIFc.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 00 40 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 fd 17 68 fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 20 0c 00 00 18 00 00 00 00 00 00 fd 3e 0c 00 00 20 00 00 00 40 0c 00 00 00 40 00 00 20 00 00 02 00 00 04 00 00 00 00 00 00 04 00 00 00 00 00 00 fd 0c 00 00 02 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PELh0 > @@@@	success or wait	4	6BC7DD66	CopyFileW
C:\Users\user\AppData\Roaming\kqruryFrIFc.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	6BC7DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mp92BC.tmp	0	1610	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" 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	6BC71B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\wkQpOZ58Gl.exe.log	0	1308	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,"Win RT","N otApp",12,"System.Wind ows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c 56 1934e089",03,"System, Version=4.0.0.0, Culture=neutral, Publ icKeyToken=b77a5c5619 34e089"," C:\Windows\assembly\Na tiveImages_v4.0.3	success or wait	1	6D13C907	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	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD603DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC71B4F	ReadFile

Analysis Process: powershell.exe PID: 6088, Parent PID: 3676

General

Target ID:	5
Start time:	12:23:35
Start date:	05/08/2022
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\kqruryFrIc.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	6CE2CF06	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	6CE2CF06	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	6BBD5B28	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	6BBD5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_2xb4spy5.adr.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6BC71E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_h1mfggue.sz5.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6BC71E60	CreateFileW
C:\Users\user\Documents\20220805	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6BC7BEFF	CreateDirect oryW
C:\Users\user\Documents\20220805\PowerShell_transcr ipt.390120.zw_Mb_9m.20220805122336.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6BC71E60	CreateFileW

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2xb4spy5.adr.ps1	success or wait	1	6BC76A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h1mfggue.sz5.psm1	success or wait	1	6BC76A95	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	6BBD5B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBD5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBD5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBD5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBD5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBD5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBD5B28	unknown
C:\Users\user\AppData\Local\Temp_PSscriptPolicyTest_2xb4spy5.adr.ps1	0	1	31	1	success or wait	1	6BC71B4F	WriteFile
C:\Users\user\AppData\Local\Temp_PSscriptPolicyTest_h1mfggue.sz5.psm1	0	1	31	1	success or wait	1	6BC71B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.390120.zw_Mb_9m.20220805122336.txt	0	3	ff		success or wait	1	6BC71B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.390120.zw_Mb_9m.20220805122336.txt	3	687	2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 38 30 35 31 32 32 33 33 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 39 30 31 32 30 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	*****Windows PowerShell transcript startStart time: 20220805122338Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 390120 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	44	6BC71B4F	WriteFile
C:\Users\user\AppData\Local\Microsofft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 57 14 00 00 19 00 00 00 fd 0e fd 05 20 09 18 09 fd 08 00 00 3e 01 79 00 0b 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eW >y@	success or wait	1	6D0F76FC	WriteFile
C:\Users\user\AppData\Local\Microsofft\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 3a 00 00 00 0e 00 20 00	H<@"^L"My::	success or wait	17	6D0F76FC	WriteFile
C:\Users\user\AppData\Local\Microsofft\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	6D0F76FC	WriteFile
C:\Users\user\AppData\Local\Microsofft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6D0F76FC	WriteFile
C:\Users\user\AppData\Local\Microsofft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6D0F76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-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 54 01 40 00 fd 29 40 01 fd 3e 40 01 fd 29 40 01 23 29 40 01 5c 64 40 01 5a 64 40 01 5b 64 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 09 06 fd 00 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 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 42 4d 40 01 fd 44 40	T@)@>@)@#)@ld@Zd @[d@@V@H@X@[@N T@HT@S@S@hT@S@ S@S@\\@T@T@@X@? X@ T@S@S@T@T@xT@z T@T@=M@DM@:M@" M@ M@!M@;M@D@D@@M @<M@\$M@8M@? M@Xd @Vd@*@BM@D@	success or wait	11	6D0F76FC	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	6CE05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlibb1a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD603DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE0CA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-NonInteractive	unknown	64	success or wait	1	6CE11F73	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Modules\AnalysisCache	unknown	4096	success or wait	1	6BC71B4F	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Modules\AnalysisCache	unknown	62	success or wait	1	6BC71B4F	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Modules\AnalysisCache	unknown	4096	success or wait	1	6BC71B4F	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTaskAppBackgroundTask.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTaskAppBackgroundTask.psd1	unknown	4096	end of file	1	6BC71B4F	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	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BC71B4F	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	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BC71B4F	ReadFile

Analysis Process: conhost.exe PID: 6084, Parent PID: 6088

General

Target ID:	6
Start time:	12:23:35
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6124, Parent PID: 3676

General

Target ID:	7
Start time:	12:23:36
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\kqruryFrIFc" /XML "C:\Users\user\AppData\Local\Temp\tmp92BC.tmp
Imagebase:	0x30000
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\tmp92BC.tmp	unknown	2	success or wait	1	3AB22	ReadFile	
C:\Users\user\AppData\Local\Temp\tmp92BC.tmp	unknown	1611	success or wait	1	3ABD9	ReadFile	

Analysis Process: conhost.exe PID: 3772, Parent PID: 6124

General	
Target ID:	9
Start time:	12:23:37
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: wKQpOZ58Gl.exe PID: 3276, Parent PID: 3676

General	
Target ID:	10
Start time:	12:23:40
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\wKQpOZ58Gl.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\wKQpOZ58Gl.exe
Imagebase:	0x170000
File size:	801280 bytes
MD5 hash:	F7C9CF1410373A60A5C5A5E02AA4BD3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wKQpOZ58Gl.exe PID: 3760, Parent PID: 3676

General	
Target ID:	14
Start time:	12:23:45
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\wKQpOZ58Gl.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\wKQpOZ58Gl.exe
Imagebase:	0x4a0000
File size:	801280 bytes
MD5 hash:	F7C9CF1410373A60A5C5A5E02AA4BD3C
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: 0000000E.00000000.431826209.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.431826209.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000E.00000000.431826209.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.633873650.0000000002901000.00000004.00000800.00020000.00000000.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	6CE2CF06	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	6CE2CF06	unknown
C:\Users\user\AppData\Roaming\lkbu4uc5.tjf	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6BC7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\lkbu4uc5.tjf\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	6BC7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\lkbu4uc5.tjf\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	6BC7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\lkbu4uc5.tjf\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	6BC7DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\lkbu4uc5.tjf\Chrome\Default\Cookies	success or wait	1	6BC76A95	DeleteFileW

File Written

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

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

Disassembly

 No disassembly