ID: 830846
Sample Name: izwFjkhFJm.exe
Cookbook: default.jbs
Time: 18:29:52
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

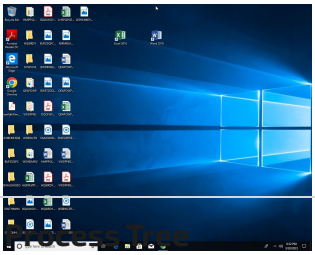
Windows Analysis Report

izwFjkhFJm.exe

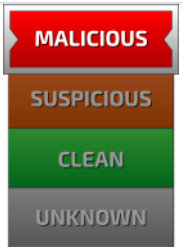
Overview

General Information

Sample Name:	izwFjkhFJm.exe
Original Sample Name:	ae2a3b41292c…
Analysis ID:	830846
MD5:	ae2a3b41292c…
SHA1:	caa30701c548…
SHA256:	65cc1ea27c73…
Tags:	AgentTesla exe Telegram
Infos:	



Detection



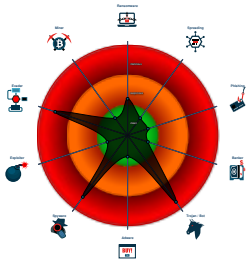
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Creates multiple autostart registry k…
- Tries to harvest and steal Putty / W…
- Encrypted powershell cmdline option…
- Uses the Telegram API (likely for C…
- Contains functionality to register a lo…

Classification



- **System is w10x64**
- izwFjkhFJm.exe (PID: 324 cmdline: C:\Users\user\Desktop\izwFjkhFJm.exe MD5: AE2A3B41292C66A9DD6F10C874C05293)
  - powershell.exe (PID: 6076 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - izwFjkhFJm.exe (PID: 1784 cmdline: C:\Users\user\Desktop\izwFjkhFJm.exe MD5: AE2A3B41292C66A9DD6F10C874C05293)
  - izwFjkhFJm.exe (PID: 2108 cmdline: C:\Users\user\Desktop\izwFjkhFJm.exe MD5: AE2A3B41292C66A9DD6F10C874C05293)
  - izwFjkhFJm.exe (PID: 2312 cmdline: C:\Users\user\Desktop\izwFjkhFJm.exe MD5: AE2A3B41292C66A9DD6F10C874C05293)
  - izwFjkhFJm.exe (PID: 2948 cmdline: C:\Users\user\Desktop\izwFjkhFJm.exe MD5: AE2A3B41292C66A9DD6F10C874C05293)
- Oefdyik.exe (PID: 5104 cmdline: "C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe" MD5: AE2A3B41292C66A9DD6F10C874C05293)
  - powershell.exe (PID: 5292 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Oefdyik.exe (PID: 5344 cmdline: C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe MD5: AE2A3B41292C66A9DD6F10C874C05293)
  - Oefdyik.exe (PID: 6036 cmdline: C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe MD5: AE2A3B41292C66A9DD6F10C874C05293)
- kDPmkTm.exe (PID: 1952 cmdline: "C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe" MD5: AE2A3B41292C66A9DD6F10C874C05293)
  - powershell.exe (PID: 4852 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Oefdyik.exe (PID: 4700 cmdline: "C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe" MD5: AE2A3B41292C66A9DD6F10C874C05293)
  - powershell.exe (PID: 5444 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- kDPmkTm.exe (PID: 6084 cmdline: "C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe" MD5: AE2A3B41292C66A9DD6F10C874C05293)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Malware Configuration

Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot5687731944:AAEDpsUftmaHrKNSGkOlhq0UZLPEvIUd8Bo/sendMessage"
}
```


Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Telegram Url": "https://api.telegram.org/bot5687731944:AAEDpsUftmaHrKNSGkOlhq0UZLPEvIUd8Bo/sendMessage?chat_id=6169364705"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000002.534154582.0000000002F7F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.530484456.0000000003248000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.530484456.0000000003248000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.336146048.0000000005440000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
Process Memory Space: izwFjkhFJm.exe PID: 2948	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.izwFjkhFJm.exe.5440000.4.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 149.154.167.220	
Timestamp:	192.168.2.3149.154.167.220497154432851779 03/20/23-18:33:24.869717
SID:	2851779
Source Port:	49715
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 149.154.167.220	
Timestamp:	192.168.2.3149.154.167.220497014432851779 03/20/23-18:31:36.462231
SID:	2851779
Source Port:	49701
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)
- May check the online IP address of the machine
- Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Installs a global keyboard hook
- Contains functionality to register a low level keyboard hook

Boot Survival

- Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection

- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

- 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

- Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

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 browser information (history, passwords, etc)

Remote Access Functionality

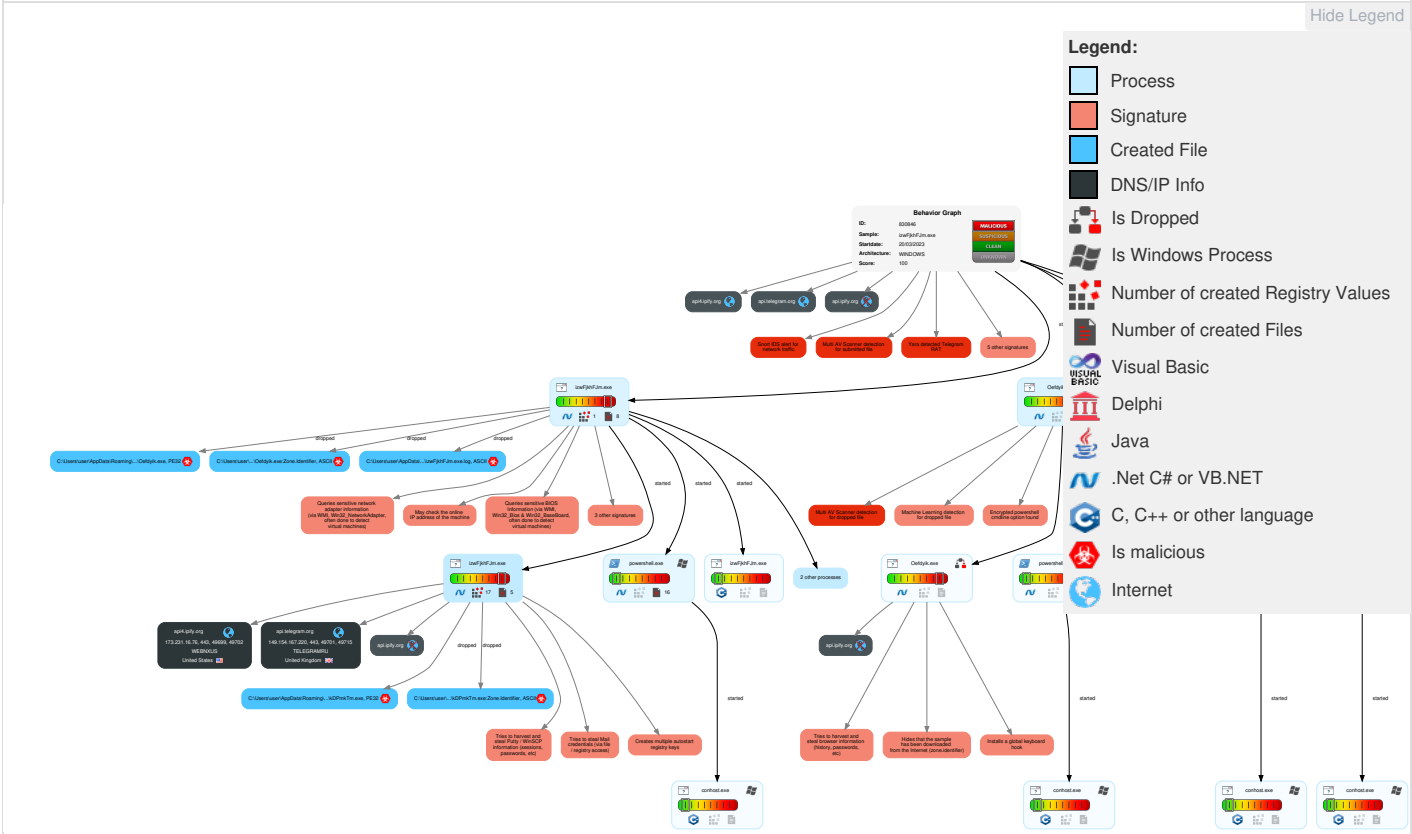
Yara detected Telegram RAT

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 1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 Account Discovery	Remote Services	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 PowerShell	Boot or Logon Initialization Scripts	1 1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	1 Credentials in Registry	1 1 4 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Virtualization/Sandbox Evasion	LSA Secrets	2 Process Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 2 Process Injection	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 Hidden Files and Directories	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Network Configuration Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

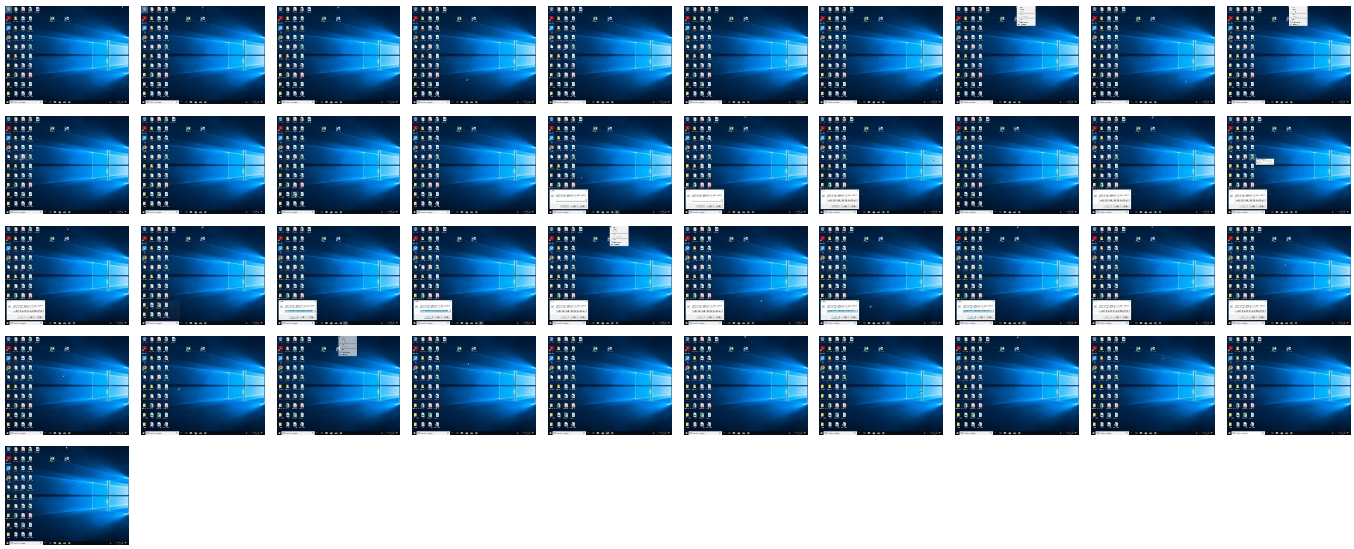
Behavior Graph



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
izwFjkhFJm.exe	33%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
izwFjkhFJm.exe	53%	Virustotal		Browse
izwFjkhFJm.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe	53%	Virustotal		Browse
C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe	33%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe	33%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
27.2.Oefdyik.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1215472		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://https://urn.to/r/sds_see	0%	URL Reputation	safe	
http://https://urn.to/r/sds_see	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api4.ipify.org	173.231.16.76	true	false		high
api.telegram.org	149.154.167.220	true	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

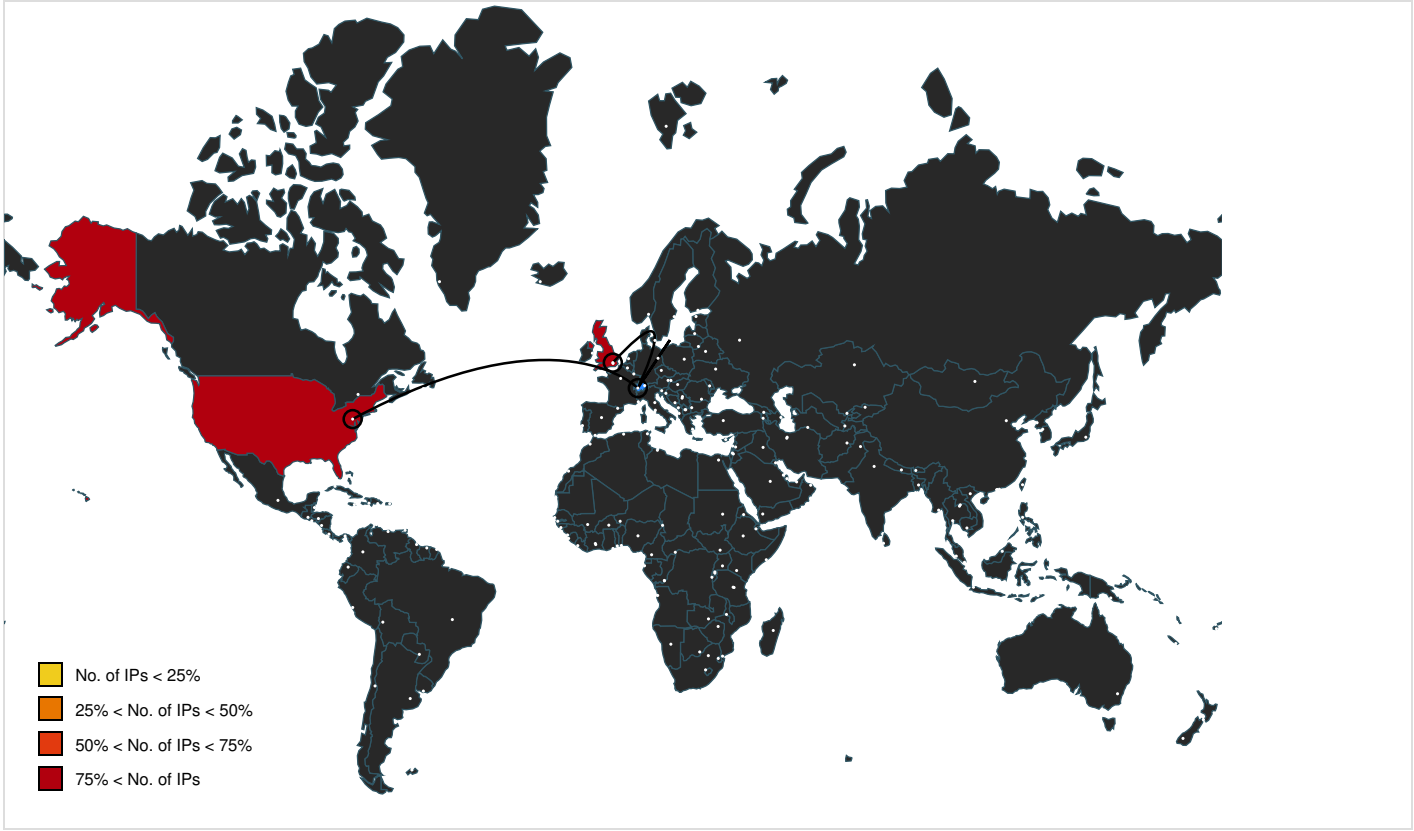
Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high
http://https://api.telegram.org/bot5687731944:AAEDpsUftmaHrKNSGkOlhq0UZLPEvIUd8Bo/sendDocument	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org	izwFjkhFJm.exe, 0000000F.00000002.530484456.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Oefdyik.exe, 0000001B.00000002.534154582.0000000002F31000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org4	izwFjkhFJm.exe, 0000000F.00000002.530484456.0000000003266000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org	izwFjkhFJm.exe, 0000000F.00000002.530484456.0000000003266000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.newtonsoft.com/jsonschema	kDPmkTm.exe, 00000015.00000002.536382964.00000000047F9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.newtonsoft.com/json	kDPmkTm.exe, 00000011.00000002.526973969.000000000301F000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000015.00000002.536382964.000000000489C000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000015.00000002.536382964.00000000047FC000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.nuget.org/packages/Newtonsoft.Json.Bson	izwFjkhFJm.exe, 00000000.00000002.338193275.0000000005CA0000.00000004.08000000.00040000.00000000.sdmp, izwFjkhFJm.exe, 00000000.00000002.331982609.000000000292A000.00000004.00000800.00020000.00000000.sdmp, Oefdyik.exe, 00000010.00000002.478092419.000000000330A000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000011.00000002.552309880.00000000046D9000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000011.00000002.526973969.000000000301F000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000015.00000002.536382964.00000000047F9000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://api.telegram.org/bot5687731944:AAEDpsUftmaHrKNSGkOlhq0UZLPEvIUd8Bo/	izwFjkhFJm.exe, 0000000F.00000002.530484456.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Oefdyik.exe, 0000001B.00000002.534154582.0000000002F31000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://urn.to/r/sds_see	izwFjkhFJm.exe, 00000000.00000002.336146048.0000000005440000.00000004.08000000.00040000.00000000.sdmp, Oefdyik.exe, 00000010.00000003.350241143.000000000472E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://api.telegram.org	izwFjkhFJm.exe, 0000000F.00000002.530484456.0000000003266000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/name	izwFjkhFJm.exe, 0000000F.00000002.530484456.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Oefdyik.exe, 0000001B.00000002.534154582.0000000002F31000.00000004.00000800.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	Oefdyik.exe, 00000010.00000002.478092419.000000000330A000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000011.00000002.552309880.00000000046D5000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000011.00000002.552309880.000000000462D000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000011.00000002.526973969.000000000301F000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000015.00000002.536382964.00000000047F5000.00000004.00000800.00020000.00000000.sdmp, kDPmkTm.exe, 00000015.00000002.536382964.000000000488D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • 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
173.231.16.76	api4.ipify.org	United States		18450	WEBNXUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830846
Start date and time:	2023-03-20 18:29:52 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, 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
Sample file name:	izwFjkhFJm.exe
Original Sample Name:	ae2a3b41292c66a9dd6f10c874c05293.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@29/16@8/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.126.32.137, 20.190.160.13, 40.126.32.69, 40.126.32.132, 20.190.160.15, 20.190.160.23, 40.126.32.67, 20.190.160.21, 13.89.179.12
- Excluded domains from analysis (whitelisted): prdv6a.aadg.msidentity.com, fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, www.tm.v6.a.prd.aadg.trafficmanager.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, onedsblobprdcus17.centralus.cloudapp.azure.com, login.msa.msidentity.com, www.tm.lg.prod.aadmsa.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
18:30:59	API Interceptor	90x Sleep call for process: powershell.exe modified
18:31:25	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Oefdyik "C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe"
18:31:31	API Interceptor	590x Sleep call for process: izwFjkhFJm.exe modified
18:31:33	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kDPmkTm C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe
18:31:44	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Oefdyik "C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe"
18:31:53	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kDPmkTm C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe
18:32:48	API Interceptor	17x Sleep call for process: Oefdyik.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\Oefdyik.exe.log	
Process:	C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1459
Entropy (8bit):	5.3420905847574325
Encrypted:	false
SSDEEP:	24:MLsmE4K5E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FayE4bE4KKE4KdEW:M4mHK5HKXwYHKhQnoPtHoxHhAHKzvFah
MD5:	FB4B7720101F874710FF986326F7980F
SHA1:	48F55B9470DB8CB42CF39FF5C8F5D6AAFB1BBD48
SHA-256:	94EF05B91B3B8D4F88102C7CEB77D5CAE9003A9534205ED0A15A5A227954D10D
SHA-512:	B08E09C4E5ADE86B5D0F9274FD1732F958DFAAA8F453BE55435B7504F4A51987180D13A5C35C759A27AE1000B8A624AE06CC2641A08A6C259C7F6C05B8F07D31
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Transactions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neut

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\izwFjkhFJm.exe.log	
Process:	C:\Users\user\Desktop\izwFjkhFJm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1459
Entropy (8bit):	5.3420905847574325
Encrypted:	false
SSDEEP:	24:MLsmE4K5E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FayE4bE4KKE4KdEW:M4mHK5HKXwYHKhQnoPtHoxHhAHKzvFah
MD5:	FB4B7720101F874710FF986326F7980F
SHA1:	48F55B9470DB8CB42CF39FF5C8F5D6AAFB1BBD48
SHA-256:	94EF05B91B3B8D4F88102C7CEB77D5CAE9003A9534205ED0A15A5A227954D10D
SHA-512:	B08E09C4E5ADE86B5D0F9274FD1732F958DFAAA8F453BE55435B7504F4A51987180D13A5C35C759A27AE1000B8A624AE06CC2641A08A6C259C7F6C05B8F07D31
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Transactions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neut

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB3287
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	15672
Entropy (8bit):	5.542414046296337
Encrypted:	false
SSDEEP:	384:nte/AM1oA1uPqtIosSjn+ilr3bsFvMs48LP:OrAqtyo+ilrIRpP
MD5:	8AEBA6925AFDFB54DA529AC11C28736E
SHA1:	05C4C8EE5B22C660A33DCFFC4F0E35900AF7BC90
SHA-256:	14595BFD9842BA212582C416C1B2F4128E1AC203DB766B0F5359EB46BF1F6265
SHA-512:	3C1A1D0E2273E4E9DA27384EEE2CED1B22EEC63B102D4602903705C8D9EDA6BCF07053A2FCFE0007629EE641F4B93F2D9D06F276E06995C96529DECD51E02E5F
Malicious:	false
Preview:	@...e.....7.....$.....s.s.....H.....<@.^.L."My....'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_23uza2uz.txl.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_ch2n5eak.wf2.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_d5xdroaz.3qx.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_dsdp1x51.web.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_p4snmec2.2zw.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_rydz4q53.akc.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_txscot0j.aim.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_xu1bhbsk.zgm.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\Roaming\Ienlugq\Oefdyik.exe

Process:	C:\Users\user\Desktop\izwFjkhFJm.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1863168
Entropy (8bit):	5.309741607982687
Encrypted:	false
SSDEEP:	24576:MVlSKtu1Dze6HDpL1J4yMPdxjNbTCUeoTYoTVCo8HkZ3Y8j8W0kWiqMhX2HyQBEO:8NLZzslSQqY5TXKZhSlB
MD5:	AE2A3B41292C66A9DD6F10C874C05293
SHA1:	CAA30701C5487C2AECFB9B35B1D0E9EA6F3214B6
SHA-256:	65CC1EA27C733C270DD0497ED9C99896BAF50EEAFA5E1200889557985BFD87D5
SHA-512:	54606FCE1CE37CA0B4A25DD94ABC5CD47BE86A498204A0581DEF8A62F714EA101B817570A456FF7E054A4C8D3DE8F3D69A8CD823DFA87515C4690AE229BB63 15
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 53%, Browse • Antivirus: ReversingLabs, Detection: 33%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...|..d.....H...$.....f... .....@.. ....`.....f..W.....!..... ..... ..H.....text....F... ...H..... ..`.rsrc....!.....".....J.....@..@.reloc..... .....!.....@..B.....f.....H.....DJ..T.....U...h1.....0.....(.....-.+.(!...+.*..0.....s.....-.&+.....+.*..0..-.....(.....s%....-.&+.(....+.*...-.&&+. (....+.*....0..0.....(.....s?....-.&+.(....+.*....-.&&&+.(....+.*.0..#.....(.....,.s3....-.&+.(....+.*.(....&*..0..*.....(.....,.sV....-.&+.(....+.*..-.&+.(....+.*...0.,.....(.....,.sJ....-.&+.(....+.*...- .&&+.(....+.*.0..-.....(.....,...s6....-.&+.(....+.*...-.&&+.(....+.*....0..

C:\Users\user\AppData\Roaming\Ienlugq\Oefdyik.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\izwFjkhFJm.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\AppData\Roaming\kDPmkTm\kDPmkTm.exe

Process:	C:\Users\user\Desktop\izwFjkhFJm.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1863168
Entropy (8bit):	5.309741607982687
Encrypted:	false
SSDEEP:	24576:MVlSKtu1Dze6HDpL1J4yMPdxjNbTCUeoTYoTVCo8HkZ3Y8j8W0kWiqMhX2HyQBEO:8NLZzslSQqY5TXKZhSlB
MD5:	AE2A3B41292C66A9DD6F10C874C05293
SHA1:	CAA30701C5487C2AECFB9B35B1D0E9EA6F3214B6
SHA-256:	65CC1EA27C733C270DD0497ED9C99896BAF50EEAFA5E1200889557985BFD87D5
SHA-512:	54606FCE1CE37CA0B4A25DD94ABC5CD47BE86A498204A0581DEF8A62F714EA101B817570A456FF7E054A4C8D3DE8F3D69A8CD823DFA87515C4690AE229BB6315
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...|..d.....H...$.....f... .....@.. ....`.....f..W.....!..... ..... ..H.....text....F... ...H..... ..`.rsrc....!....."...J.....@..@.reloc..... .....!.....@..B.....f.....H.....DJ..T.....U...h1.....0.....(.....-.+.(!...+.*..0.....s.....-.&+.....+.*..0..-.....(.....s%....-.&+.(....+.*...-.&&+.(....+.*....0..0.....(....,....s?....-.&+.(....+.*....-.&&&+.(....+.*.0..#.....(....,..s3....-.&+.(....+.*.(....&*..0..*.....(....,..sV....-.&+.(....+.*..-.&+.(....+.*...0..,.....(.....,.sJ....-.&+.(....+.*..-.&&+.(....+.*.0..-.....(....,...s6....-.&+.(....+.*...-.&&+.(....+.*....0..

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

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.309741607982687
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	izwFjkhFJm.exe
File size:	1863168
MD5:	ae2a3b41292c66a9dd6f10c874c05293
SHA1:	caa30701c5487c2aecfb9b35b1d0e9ea6f3214b6

SHA256:	65cc1ea27c733c270dd0497ed9c99896baf50eeafa5e1200889557985bfd87d5
SHA512:	54606fce1ce37ca0b4a25dd94abc5cd47be86a498204a0581def8a62f714ea101b817570a456ff7e054a4c8d3de8f3d69a8cd823dfa87515c4690ae229bb6315
SSDEEP:	24576:MVlSKtu1Dze6HDpL1J4yMPdxjNbTCUeoTYoTVCo8HkZ3Y8j8W0kWiqMhX2HyQBEO:8NLZzslSQqY5TXKZhSlB
TLSH:	0D854CF24193FEC4976F2D4481143A40DC101C6797BC9698FDC92AA793E9978EF9CAB0
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L...\|..d.................H...$.......f... ....@.. ....`.................................

File Icon

Icon Hash:	78b87c6c6c606880

Static PE Info

General

Entrypoint:	0x5c66f2
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:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6417E07C [Mon Mar 20 04:26:36 2023 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1c6698	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1c8000	0x21e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1cc000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c46f8	0x1c4800	False	0.4735319190262431	data	5.272126053067271	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x1c8000	0x21e8	0x2200	False	0.8832720588235294	data	7.595705097596992	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1cc000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1c8130	0x1c12	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x1c9d44	0x14	data		
RT_VERSION	0x1c9d58	0x2dc	data		
RT_MANIFEST	0x1ca034	0x1b4	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (433), with no line terminators		

Imports

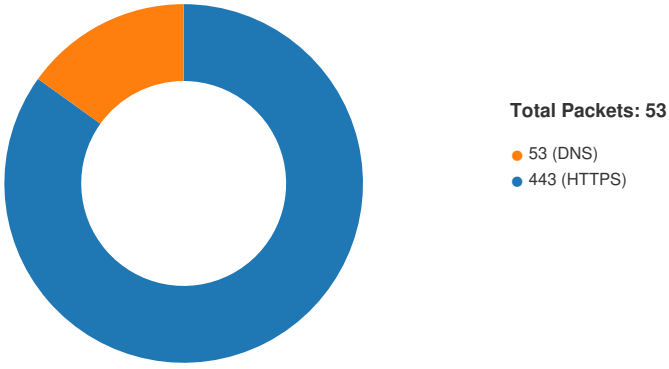
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3149.154.167.220497154432851779 03/20/23-18:33:24.869717	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49715	443	192.168.2.3	149.154.167.220
192.168.2.3149.154.167.220497014432851779 03/20/23-18:31:36.462231	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49701	443	192.168.2.3	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:31:27.699748039 CET	49699	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:31:27.699857950 CET	443	49699	173.231.16.76	192.168.2.3
Mar 20, 2023 18:31:27.699994087 CET	49699	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:31:27.733558893 CET	49699	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:31:27.733618975 CET	443	49699	173.231.16.76	192.168.2.3
Mar 20, 2023 18:31:28.379163980 CET	443	49699	173.231.16.76	192.168.2.3
Mar 20, 2023 18:31:28.379291058 CET	49699	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:31:28.382338047 CET	49699	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:31:28.382364035 CET	443	49699	173.231.16.76	192.168.2.3
Mar 20, 2023 18:31:28.382752895 CET	443	49699	173.231.16.76	192.168.2.3
Mar 20, 2023 18:31:28.586198092 CET	49699	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:31:28.648602009 CET	49699	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:31:28.648667097 CET	443	49699	173.231.16.76	192.168.2.3
Mar 20, 2023 18:31:28.803409100 CET	443	49699	173.231.16.76	192.168.2.3
Mar 20, 2023 18:31:28.803500891 CET	443	49699	173.231.16.76	192.168.2.3
Mar 20, 2023 18:31:28.803656101 CET	49699	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:31:28.804965973 CET	49699	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:31:36.293730974 CET	49701	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:31:36.293807983 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.293895960 CET	49701	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:31:36.294677019 CET	49701	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:31:36.294722080 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.361607075 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.361701012 CET	49701	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:31:36.367089987 CET	49701	443	192.168.2.3	149.154.167.220

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:31:36.367127895 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.367513895 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.428234100 CET	49701	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:31:36.428277969 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.455465078 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.462035894 CET	49701	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:31:36.462074995 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.567434072 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.567543983 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.568159103 CET	49701	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:31:36.568188906 CET	443	49701	149.154.167.220	192.168.2.3
Mar 20, 2023 18:31:36.568207979 CET	49701	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:31:36.568258047 CET	49701	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:32:35.641273975 CET	49702	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:32:35.641380072 CET	443	49702	173.231.16.76	192.168.2.3
Mar 20, 2023 18:32:35.641500950 CET	49702	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:32:35.658441067 CET	49702	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:32:35.658540964 CET	443	49702	173.231.16.76	192.168.2.3
Mar 20, 2023 18:32:36.303930998 CET	443	49702	173.231.16.76	192.168.2.3
Mar 20, 2023 18:32:36.304028988 CET	49702	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:32:36.306864977 CET	49702	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:32:36.306899071 CET	443	49702	173.231.16.76	192.168.2.3
Mar 20, 2023 18:32:36.307337046 CET	443	49702	173.231.16.76	192.168.2.3
Mar 20, 2023 18:32:36.514731884 CET	443	49702	173.231.16.76	192.168.2.3
Mar 20, 2023 18:32:36.514903069 CET	49702	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:32:36.752813101 CET	49702	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:32:36.752886057 CET	443	49702	173.231.16.76	192.168.2.3
Mar 20, 2023 18:32:37.603478909 CET	443	49702	173.231.16.76	192.168.2.3
Mar 20, 2023 18:32:37.603661060 CET	443	49702	173.231.16.76	192.168.2.3
Mar 20, 2023 18:32:37.603812933 CET	49702	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:32:37.608839989 CET	49702	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:33:23.255290031 CET	49714	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:33:23.255369902 CET	443	49714	173.231.16.76	192.168.2.3
Mar 20, 2023 18:33:23.255475044 CET	49714	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:33:23.258941889 CET	49714	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:33:23.259001017 CET	443	49714	173.231.16.76	192.168.2.3
Mar 20, 2023 18:33:23.901695013 CET	443	49714	173.231.16.76	192.168.2.3
Mar 20, 2023 18:33:23.901845932 CET	49714	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:33:23.904732943 CET	49714	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:33:23.904772043 CET	443	49714	173.231.16.76	192.168.2.3
Mar 20, 2023 18:33:23.905273914 CET	443	49714	173.231.16.76	192.168.2.3
Mar 20, 2023 18:33:23.941174984 CET	49714	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:33:23.941207886 CET	443	49714	173.231.16.76	192.168.2.3
Mar 20, 2023 18:33:24.256023884 CET	443	49714	173.231.16.76	192.168.2.3
Mar 20, 2023 18:33:24.256136894 CET	443	49714	173.231.16.76	192.168.2.3
Mar 20, 2023 18:33:24.256246090 CET	49714	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:33:24.257375956 CET	49714	443	192.168.2.3	173.231.16.76
Mar 20, 2023 18:33:24.753156900 CET	49715	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:33:24.753216028 CET	443	49715	149.154.167.220	192.168.2.3
Mar 20, 2023 18:33:24.753302097 CET	49715	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:33:24.753787041 CET	49715	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:33:24.753807068 CET	443	49715	149.154.167.220	192.168.2.3
Mar 20, 2023 18:33:24.817501068 CET	443	49715	149.154.167.220	192.168.2.3
Mar 20, 2023 18:33:24.817751884 CET	49715	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:33:24.820658922 CET	49715	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:33:24.820687056 CET	443	49715	149.154.167.220	192.168.2.3
Mar 20, 2023 18:33:24.821106911 CET	443	49715	149.154.167.220	192.168.2.3
Mar 20, 2023 18:33:24.823626995 CET	49715	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:33:24.823657036 CET	443	49715	149.154.167.220	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:33:24.869210958 CET	443	49715	149.154.167.220	192.168.2.3
Mar 20, 2023 18:33:24.869610071 CET	49715	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:33:24.869642973 CET	443	49715	149.154.167.220	192.168.2.3
Mar 20, 2023 18:33:24.982460022 CET	443	49715	149.154.167.220	192.168.2.3
Mar 20, 2023 18:33:24.982655048 CET	443	49715	149.154.167.220	192.168.2.3
Mar 20, 2023 18:33:24.982764006 CET	49715	443	192.168.2.3	149.154.167.220
Mar 20, 2023 18:33:24.983042955 CET	49715	443	192.168.2.3	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:31:27.614362001 CET	58921	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:31:27.633577108 CET	53	58921	8.8.8.8	192.168.2.3
Mar 20, 2023 18:31:27.642391920 CET	62704	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:31:27.665841103 CET	53	62704	8.8.8.8	192.168.2.3
Mar 20, 2023 18:31:36.269547939 CET	57840	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:31:36.289082050 CET	53	57840	8.8.8.8	192.168.2.3
Mar 20, 2023 18:32:35.568073988 CET	57990	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:32:35.586179972 CET	53	57990	8.8.8.8	192.168.2.3
Mar 20, 2023 18:32:35.607027054 CET	52387	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:32:35.627496004 CET	53	52387	8.8.8.8	192.168.2.3
Mar 20, 2023 18:33:23.202795029 CET	49302	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:33:23.222448111 CET	53	49302	8.8.8.8	192.168.2.3
Mar 20, 2023 18:33:23.229949951 CET	53975	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:33:23.249663115 CET	53	53975	8.8.8.8	192.168.2.3
Mar 20, 2023 18:33:24.733335972 CET	51139	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:33:24.752517939 CET	53	51139	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 18:31:27.614362001 CET	192.168.2.3	8.8.8.8	0x19fc	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:31:27.642391920 CET	192.168.2.3	8.8.8.8	0xa091	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:31:36.269547939 CET	192.168.2.3	8.8.8.8	0x71bc	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:32:35.568073988 CET	192.168.2.3	8.8.8.8	0x38bc	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:32:35.607027054 CET	192.168.2.3	8.8.8.8	0xc297	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:23.202795029 CET	192.168.2.3	8.8.8.8	0x7ad3	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:23.229949951 CET	192.168.2.3	8.8.8.8	0xf168	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:24.733335972 CET	192.168.2.3	8.8.8.8	0x2cfe	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 18:31:27.633577108 CET	8.8.8.8	192.168.2.3	0x19fc	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:31:27.633577108 CET	8.8.8.8	192.168.2.3	0x19fc	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:31:27.633577108 CET	8.8.8.8	192.168.2.3	0x19fc	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:31:27.633577108 CET	8.8.8.8	192.168.2.3	0x19fc	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false

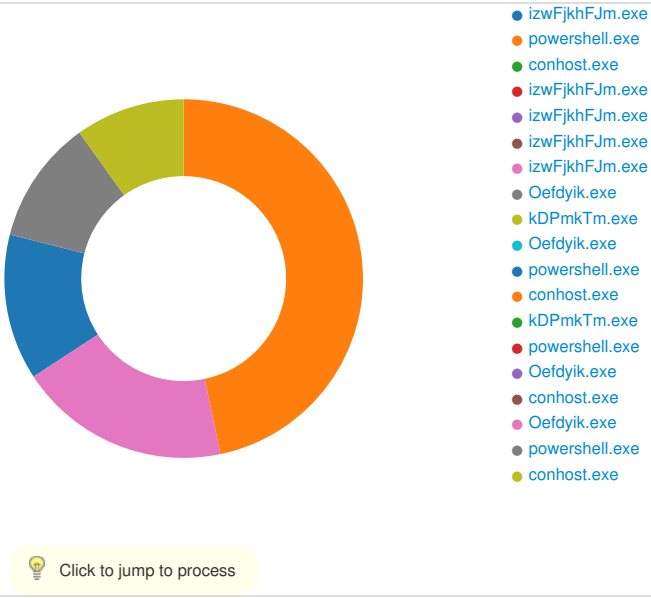
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 18:31:27.665841103 CET	8.8.8.8	192.168.2.3	0xa091	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:31:27.665841103 CET	8.8.8.8	192.168.2.3	0xa091	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:31:27.665841103 CET	8.8.8.8	192.168.2.3	0xa091	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:31:27.665841103 CET	8.8.8.8	192.168.2.3	0xa091	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:31:36.289082050 CET	8.8.8.8	192.168.2.3	0x71bc	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:32:35.586179972 CET	8.8.8.8	192.168.2.3	0x38bc	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:32:35.586179972 CET	8.8.8.8	192.168.2.3	0x38bc	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:32:35.586179972 CET	8.8.8.8	192.168.2.3	0x38bc	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:32:35.586179972 CET	8.8.8.8	192.168.2.3	0x38bc	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:32:35.627496004 CET	8.8.8.8	192.168.2.3	0xc297	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:32:35.627496004 CET	8.8.8.8	192.168.2.3	0xc297	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:32:35.627496004 CET	8.8.8.8	192.168.2.3	0xc297	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:32:35.627496004 CET	8.8.8.8	192.168.2.3	0xc297	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:23.222448111 CET	8.8.8.8	192.168.2.3	0x7ad3	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:33:23.222448111 CET	8.8.8.8	192.168.2.3	0x7ad3	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:23.222448111 CET	8.8.8.8	192.168.2.3	0x7ad3	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:23.222448111 CET	8.8.8.8	192.168.2.3	0x7ad3	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:23.249663115 CET	8.8.8.8	192.168.2.3	0xf168	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:33:23.249663115 CET	8.8.8.8	192.168.2.3	0xf168	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:23.249663115 CET	8.8.8.8	192.168.2.3	0xf168	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:23.249663115 CET	8.8.8.8	192.168.2.3	0xf168	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:33:24.752517939 CET	8.8.8.8	192.168.2.3	0x2cfe	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org
- api.telegram.org

Statistics

Behavior



System Behavior

Analysis Process: izwFjkhFJm.exe PID: **324**, Parent PID: **3452**

General

Target ID:	0
Start time:	18:30:47
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\izwFjkhFJm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\izwFjkhFJm.exe
Imagebase:	0x3d0000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000000.00000002.336146048.0000000005440000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CdFileMgr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
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	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Roaming\lenlugq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\izwFjkhFJm.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\izwFjkhFJm.exe.log	0	1459	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 54 72 61 6e 73 61 63 74 69 6f 6e 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 30	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Transactions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30	success or wait	1	72CAC907	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	728D03DE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Oefdyik	unicode	"C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe"	success or wait	1	717E646A	RegSetValueExW

Analysis Process: powershell.exe PID: **6076**, Parent PID: **324**

General

Target ID:	1
Start time:	18:30:57
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0x1350000
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\AppData\Local\Temp__PSscriptPolicyTest_p4snmec2.2zw.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_txscot0j.aim.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
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	7299CF06	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	7299CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p4snmec2.2zw.ps1	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_txscot0j.aim.psm1	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p4snmec2.2zw.ps1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_txscot0j.aim.psm1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOut-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOut-PrinteryH8IC:\Program Files (x86)\WindowsP	success or wait	1	717E1B4F	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 0f 00 00 00 37 0e 00 00 14 00 00 00 24 0e fd 05 fd 08 73 08 73 08 00 00 00 00 fd 00 14 00 01 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e7$ss	success or wait	1	72C676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	72C676FC	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	15	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 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 68 38 40 01 67 38 40 01 fd 53 40 01 fd 53 40 01 10 6f 40 01 1e 54 40 01 11 6f 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 05 0e fd 00 06 0e fd 00 04 0e fd 00 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 07 0c fd 00 38 4d 40 01 07 0e fd 00 3f 4d 40 01 08 0e fd 00 12 6f 40 01 2a 29 40 01 1f 29 40 01 4d 64 40 01 5d 64 40 01 4e 64 40 01 fd 29 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@h8@g8@S@S@o@T@o@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@o@*)@)@Md@]d@Nd@)@	success or wait	8	72C676FC	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	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72981F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7298203F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: conhost.exe PID: **6060**, Parent PID: **6076**

General	
Target ID:	2
Start time:	18:30:57
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: izwFjkhFJm.exe PID: **1784**, Parent PID: **324**

General	
Target ID:	12
Start time:	18:31:25
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\izwFjkhFJm.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\izwFjkhFJm.exe
Imagebase:	0x50000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: izwFjkhFJm.exe PID: **2108**, Parent PID: **324**

General	
Target ID:	13
Start time:	18:31:25
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\izwFjkhFJm.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\izwFjkhFJm.exe
Imagebase:	0xb0000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: izwFjkhFJm.exe PID: **2312**, Parent PID: **324**

General

Target ID:	14
Start time:	18:31:26
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\izwFjkhFJm.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\izwFjkhFJm.exe
Imagebase:	0x3d0000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: izwFjkhFJm.exe PID: **2948**, Parent PID: **324**

General

Target ID:	15
Start time:	18:31:26
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\izwFjkhFJm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\izwFjkhFJm.exe
Imagebase:	0xd60000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
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: 0000000F.00000002.530484456.0000000003248000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.530484456.0000000003248000.00000004.00000800.00020000.00000000.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	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Roaming\kDPmkTm	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.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	717EDD66	CopyFileW
C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	717EDD66	CopyFileW

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe:Zone.Identifier	success or wait	1	73E3A2A	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7c fd 17 64 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 48 1c 00 00 24 00 00 00 00 00 00 fd 66 1c 00 00 20 00 00 00 fd 1c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 1c 00 00 02 00 00 00 00 00 00 02 00 60 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.$PEL\|dH$f @ `	success or wait	8	717EDD66	CopyFileW
C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.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	717EDD66	CopyFileW

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	kDPmkTm	unicode	C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe	success or wait	1	717E646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	kDPmkTm	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	717EDE2E	RegSetValueExW

Analysis Process: Oefdyik.exe PID: **5104**, Parent PID: **3452**

General

Target ID:	16
Start time:	18:31:33
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe"
Imagebase:	0xcf0000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 53%, Virustotal, Browse • Detection: 33%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Oefdyik.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Oefdyik.exe.log	0	1459	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 54 72 61 6e 73 61 63 74 69 6f 6e 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 30	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Transactions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30	success or wait	1	72CAC907	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	728D03DE	ReadFile

Analysis Process: kDPmkTm.exe PID: **1952**, Parent PID: **3452**

General

Target ID:	17
Start time:	18:31:42
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe"
Imagebase:	0x7ff745070000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 33%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	728D03DE	ReadFile

Analysis Process: Oefdyik.exe PID: **4700**, Parent PID: **3452**

General

Target ID:	18
Start time:	18:31:53
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe"
Imagebase:	0xe00000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: powershell.exe PID: **5292**, Parent PID: **5104**

General	
Target ID:	19
Start time:	18:31:55
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0x1350000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **6072**, Parent PID: **5292**

General	
Target ID:	20
Start time:	18:31:55
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: kDPmkTm.exe PID: **6084**, Parent PID: **3452**

General	
Target ID:	21
Start time:	18:32:02
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kDPmkTm\kDPmkTm.exe"
Imagebase:	0x9f0000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: **4852**, Parent PID: **1952**

General	
Target ID:	24
Start time:	18:32:28

Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0x1350000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: Oefdyik.exe PID: **5344**, Parent PID: **5104**

General

Target ID:	25
Start time:	18:32:28
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe
Imagebase:	0x130000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3776**, Parent PID: **4852**

General

Target ID:	26
Start time:	18:32:28
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: Oefdyik.exe PID: **6036**, Parent PID: **5104**

General

Target ID:	27
Start time:	18:32:30
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\lenlugq\Oefdyik.exe
Imagebase:	0x950000
File size:	1863168 bytes
MD5 hash:	AE2A3B41292C66A9DD6F10C874C05293

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001B.00000002.534154582.0000000002F7F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: powershell.exe PID: **5444**, Parent PID: **4700**

General	
Target ID:	28
Start time:	18:32:50
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0x1350000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **5180**, Parent PID: **5444**

General	
Target ID:	29
Start time:	18:32:50
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff68f300000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly