ID: 1437130
Sample Name:
bUHMq54m6Q.exe
Cookbook: default.jbs
Time: 01:31:24
Date: 07/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

Table of Contents 2
Windows Analysis Report bUHMq54m6Q.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 5
Dropped Files 6
Memory Dumps 6
Sigma Signatures 6
System Summary 6
Snort Signatures 6
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
System Summary 7
Boot Survival 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
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 10
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 18
Public IPs 18
General Information 19
Warnings 19
Simulations 19
Behavior and APIs 19
Joe Sandbox View / Context 20
IPs 20
Domains 20
ASNs 20
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 20
C:\ProgramData\MPGPH131\MPGPH131.exe 20
C:\ProgramData\MPGPH131\MPGPH131.exe:Zone.Identifier 20
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_MPGPH131.exe_5ae7e4c267f7e8254d33e44a3aef75514fc3925e_0010bad0_310ee076-0e1e-4dc2-a821-22b2cb294147\Report.wer 21
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bUHMq54m6Q.exe_7f5678ff3d44ce164b9187a831663245298324_7fe652d7_b9d6888b-1509-4a56-aeb6-1b74ada72881\Report.wer 21
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp 21
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml 22
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3245.tmp.xml 22
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3C94.tmp.dmp 22
C:\ProgramData\Microsoft\Windows\WER\Temp\WER461A.tmp.WERInternalMetadata.xml 23
C:\ProgramData\Microsoft\Windows\WER\Temp\WER463A.tmp.xml 23
C:\Users\user\AppData\Local\RageMP131\RageMP131.exe 23
C:\Users\user\AppData\Local\RageMP131\RageMP131.exe:Zone.Identifier 24
C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip 24
C:\Users\user\AppData\Local\Temp\eK26yDxmyAbMrjg7CdmfOmj.zip 24
C:\Users\user\AppData\Local\Temp\rage131MP.tmp 25
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\02zdBXI47cvzcookies.sqlite 25
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\3b6N2Xdh3CYwplaces.sqlite 25
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\8aQjHf7utHnSHistory 25
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\9V16nhm0bFZXWeb Data 26
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\D87fZN3R3jFeplaces.sqlite 26
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\EvDoFjSc27w4History 26

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\FQEh_xU7vRTGWeb Data 27
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\JEr8lVONTEQKLogin Data 27
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\LmI4gt7uNt6lWeb Data 27
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\P8T1BgZgt5t1Cookies 28
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\RVFvq_w1ZQYbWeb Data 28
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\dn59MYeqcUJmWeb Data 28
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\lKkvrLBG06UiLogin Data For Account 28
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\nQVbv3R1YjF8Cookies 29
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\oVix2UaWI8VCHistory 29
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\q58jgT3UDnoOWeb Data 29
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\w07ebxHrMjWrHistory 30
C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\wib805ADjjQsLogin Data 30
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite 30
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\1oBLao5WFReeLogin Data For Account 31
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite 31
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Bs1Rik95T3UPWeb Data 31
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite 31
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\F27iDkUSbUX4History 32
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\GoTBCXWsNltoCookies 32
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\IuMVYmRLxIIELogin Data 32
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\KsIfLLPbfavZWeb Data 33
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\SrMOR5IqDZZTCookies 33
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\TQL0dLOETHSsHistory 33
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\W4StvYRvRm8RLogin Data 34
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\djGL4gOVacKhHistory 34
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\e0WJiscSE76mWeb Data 34
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uH4Klb1syK8iWeb Data 35
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uyAd3P89yfWTHistory 35
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\vCcKyxUjjGyAWeb Data 35
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\z81g9YDMLrJHWeb Data 35
C:\Users\user\AppData\Local\Temp\trixylgSFE9XfRUKm\Cookies\Chrome_Default.txt 36
C:\Users\user\AppData\Local\Temp\trixylgSFE9XfRUKm\information.txt 36
C:\Users\user\AppData\Local\Temp\trixylgSFE9XfRUKm\passwords.txt 36
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Cookies\Chrome_Default.txt 37
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt 37
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\passwords.txt 37
C:\Windows\appcompat\Programs\Amcache.hve 38
Static File Info 38
General 38
File Icon 38
Static PE Info 38
General 38
Entrypoint Preview 39
Data Directories 40
Sections 41
Resources 42
Imports 42
Possible Origin 42
Network Behavior 43
Snort IDS Alerts 43
Network Port Distribution 43
TCP Packets 43
UDP Packets 45
DNS Queries 45
DNS Answers 45
HTTP Request Dependency Graph 46
Statistics 46
Behavior 46
System Behavior 46
Analysis Process: bUHMq54m6Q.exePID: 6556, Parent PID: 4004 46
General 46
File Activities 47
Registry Activities 47
Analysis Process: schtasks.exePID: 3560, Parent PID: 6556 47
General 47
File Activities 47
Analysis Process: conhost.exePID: 3200, Parent PID: 3560 47
General 47
Analysis Process: schtasks.exePID: 5412, Parent PID: 6556 48
General 48
File Activities 48
Analysis Process: conhost.exePID: 4412, Parent PID: 5412 48
General 48
Analysis Process: MPGPH131.exePID: 4896, Parent PID: 1064 48
General 48
File Activities 49
File Created 49
File Deleted 53
File Written 53
File Read 65
Registry Activities 67
Analysis Process: MPGPH131.exePID: 2836, Parent PID: 1064 67
General 67
File Activities 68
File Created 68
File Deleted 68
File Written 68

File Read 70
Analysis Process: WerFault.exePID: 1836, Parent PID: 6556 70
General 70
File Activities 71
File Created 71
File Written 71
Analysis Process: WerFault.exePID: 5088, Parent PID: 4896 88
General 88
Analysis Process: RageMP131.exePID: 3604, Parent PID: 4004 89
General 89
Analysis Process: RageMP131.exePID: 5700, Parent PID: 4004 89
General 89
Disassembly 89

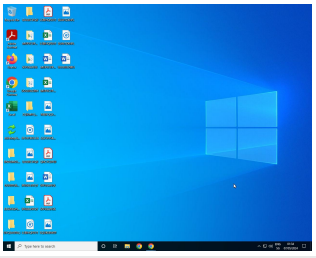
Windows Analysis Report

bUHMq54m6Q.exe

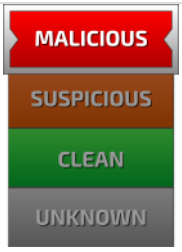
Overview

General Information

Sample name:	bUHMq54m6Q.exerenamed because original name is a hash value
Original sample name:	2cf4b5cf32775…
Analysis ID:	1437130
MD5:	2cf4b5cf32775…
SHA1:	020751e48f382..
SHA256:	a275c369ef53e..
Tags:	exe RisePro Stealer
Infos:	



Detection



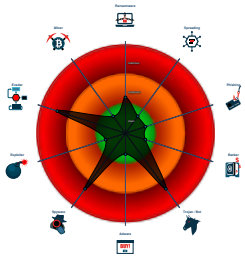
RisePro Stealer

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Yara detected RisePro Stealer
- Connects to many ports of the same…
- Contains functionality to inject threa…
- Found many strings related to Crypt…
- Found stalling execution ending in A…
- Machine Learning detection for drop…
- Machine Learning detection for sam…
- PE file contains section with specia…
- Query firmware table information (lik…

Classification



Process Tree

- **System is w10x64**
- bUHMq54m6Q.exe (PID: 6556 cmdline: "C:\Users\user\Desktop\bUHMq54m6Q.exe" MD5: 2CF4B5CF327757376E717AB5554B921B)
  - schtasks.exe (PID: 3560 cmdline: schtasks /create /f /RU "user" /tr "C:\ProgramData\MPGPH131\MPGPH131.exe" /tn "MPGPH131 HR" /sc HOURLY /rl HIGHEST MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 3200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - schtasks.exe (PID: 5412 cmdline: schtasks /create /f /RU "user" /tr "C:\ProgramData\MPGPH131\MPGPH131.exe" /tn "MPGPH131 LG" /sc ONLOGON /rl HIGHEST MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 4412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - WerFault.exe (PID: 1836 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6556 -s 1888 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- MPGPH131.exe (PID: 4896 cmdline: C:\ProgramData\MPGPH131\MPGPH131.exe MD5: 2CF4B5CF327757376E717AB5554B921B)
  - WerFault.exe (PID: 5088 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4896 -s 1148 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- MPGPH131.exe (PID: 2836 cmdline: C:\ProgramData\MPGPH131\MPGPH131.exe MD5: 2CF4B5CF327757376E717AB5554B921B)
- RageMP131.exe (PID: 3604 cmdline: "C:\Users\user\AppData\Local\RageMP131\RageMP131.exe" MD5: 2CF4B5CF327757376E717AB5554B921B)
- RageMP131.exe (PID: 5700 cmdline: "C:\Users\user\AppData\Local\RageMP131\RageMP131.exe" MD5: 2CF4B5CF327757376E717AB5554B921B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\eK26yDxmyAbMrjg7CdmfOmj.zip	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.2159759925.0000000005C56000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000000.00000002.2276746268.000000000122E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000000.00000002.2280792333.0000000005C5F000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000006.00000002.2282419782.0000000005A70000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000000.00000002.2280715188.0000000005C30000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	

Click to see the 7 entries

Sigma Signatures

System Summary

Sigma detected: CurrentVersion Autorun Keys Modification

Snort Signatures

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.6

Timestamp:	05/07/24-01:32:16.104894
SID:	2046266
Source Port:	58709
Destination Port:	49703
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.6

Timestamp:	05/07/24-01:32:30.432420
SID:	2046266
Source Port:	58709
Destination Port:	49720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.6

Timestamp:	05/07/24-01:32:13.660877
SID:	2046266
Source Port:	58709
Destination Port:	49699
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (External IP) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.6

Timestamp:	05/07/24-01:32:13.858546
SID:	2046267

Source Port:	58709
Destination Port:	49699
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.6	−
Timestamp:	05/07/24-01:32:16.124524
SID:	2046266
Source Port:	58709
Destination Port:	49702
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN RisePro TCP Heartbeat Packet - Source IP: 192.168.2.6 - Destination IP: 147.45.47.126	−
Timestamp:	05/07/24-01:32:13.477244
SID:	2049060
Source Port:	49699
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.6 - Destination IP: 147.45.47.126	−
Timestamp:	05/07/24-01:32:19.524067
SID:	2046269
Source Port:	49699
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.6	−
Timestamp:	05/07/24-01:32:39.555621
SID:	2046266
Source Port:	58709
Destination Port:	49724
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Connects to many ports of the same IP (likely port scanning)

System Summary

PE file contains section with special chars

Boot Survival

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

Malware Analysis System Evasion

Found stalling execution ending in API Sleep call

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

HIPS / PFW / Operating System Protection Evasion

Contains functionality to inject threads in other processes

Stealing of Sensitive Information

Yara detected RisePro Stealer

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

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

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

Remote Access Functionality

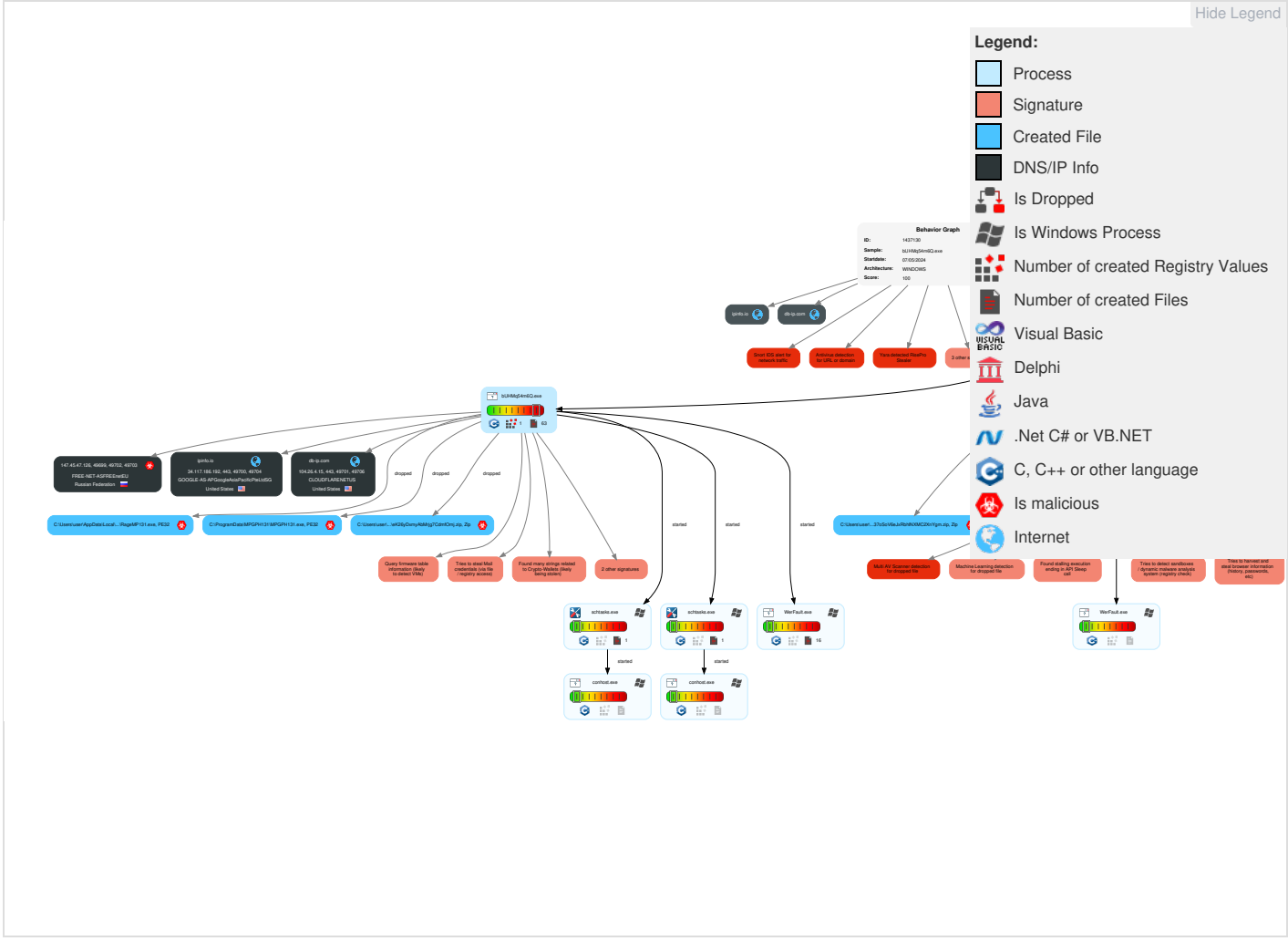
Yara detected RisePro Stealer

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	2 Command and Scripting Interpreter	1 Scheduled Task/Job	1 1 Process Injection	3 Obfuscated Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	2 Data from Local System	2 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	2 Software Packing	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	1 Non-Standard Port	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	NTDS	3 5 System Information Discovery	Distributed Component Object Model	1 Email Collection	2 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Query Registry	SSH	Keylogging	1 3 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 3 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 5 1 Security Software Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 1 Process Injection	DCSync	1 3 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	2 Process Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	HTML Smuggling	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	Dynamic API Resolution	Network Sniffing	1 System Network Configuration Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement

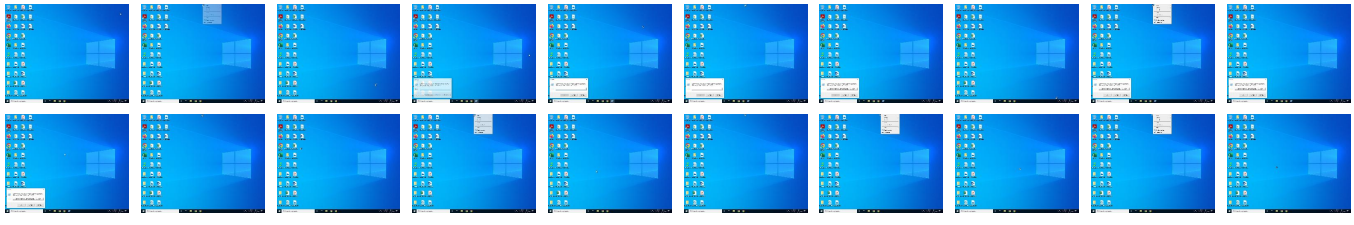
Behavior Graph

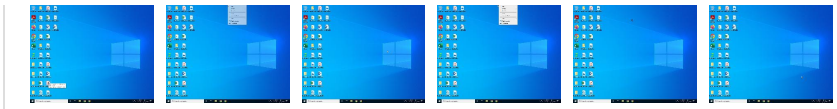


Screenshots

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
bUHMq54m6Q.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\RageMP131\RageMP131.exe	100%	Joe Sandbox ML		
C:\ProgramData\MPGPH131\MPGPH131.exe	100%	Joe Sandbox ML		
C:\ProgramData\MPGPH131\MPGPH131.exe	47%	ReversingLabs	Win32.Trojan.RiseProStealer	
C:\Users\user\AppData\Local\RageMP131\RageMP131.exe	47%	ReversingLabs	Win32.Trojan.RiseProStealer	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.micro	0%	URL Reputation	safe	
http://193.233.132.56/cost/go.exe207	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exe68.0	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exeaO	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/go.exeWOUl-	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/go.exeServer	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exe)=	0%	Avira URL Cloud	safe	
http://193.23	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exe	100%	Avira URL Cloud	malware	
http://193.233.132.56/cost/go.exeTerracoin=	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/go.exe	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/lenin.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ipinfo.io	34.117.186.192	true	false		high
db-ip.com	104.26.4.15	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://db-ip.com/demo/home.php?s=156.146.37.102	false		high
http://https://ipinfo.io/widget/demo/156.146.37.102	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	bUHMq54m6Q.exe, 00000000.00000003.2150265902.0000000005C6F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2152690333.0000000005C93000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2151263071.0000000005C92000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2181530040.0000000005EFD000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2179554394.0000000005EFB000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2180030463.0000000005F00000.00000004.00000020.00020000.00000000.sdmp, RVFvq_w1ZQYbWeb Data.0.dr, 9V16nhm0bFZXWeb Data.0.dr, LmI4gt7uNt6lWeb Data.0.dr, uH4Klb1syK8iWeb Data.6.dr, KslfLLPbfavZWeb Data.6.dr, e0WJiscSE76mWeb Data.6.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/ac/?q=	bUHMq54m6Q.exe, 00000000.00000003.2150265902.0000000005C6F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2152690333.0000000005C93000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2151263071.0000000005C92000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2181530040.0000000005EFD000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2179554394.0000000005EFB000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2180030463.0000000005F00000.00000004.00000020.00020000.00000000.sdmp, RVFvq_w1ZQYbWeb Data.0.dr, 9V16nhm0bFZXWeb Data.0.dr, Lml4gt7uNt6lWeb Data.0.dr, uH4Klb1syK8iWeb Data.6.dr, KslfLLPbfavZWeb Data.6.dr, e0WJiscSE76mWeb Data.6.dr	false		high
http://193.233.132.56/cost/go.exe207	bUHMq54m6Q.exe, 00000000.00000002.2276746268.00000000012BC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://db-ip.com/demo/home.php?s=156.146.37.102D	RageMP131.exe, 0000000E.00000002.2325536566.00000000010F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io/widget/demo/156.146.37.102p	MPGPH131.exe, 00000006.00000002.2275133356.0000000000D1B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://147.45.47.102:57893/hera/amadka.exe	bUHMq54m6Q.exe, 00000000.00000002.2276746268.00000000012BC000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2158606160.0000000005C71000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2159759925.0000000005C73000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2158405940.0000000005C71000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000002.2280792333.0000000005C73000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2158512133.0000000005C71000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000007.00000002.2174199079.0000000001CA7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://db-ip.com/	RageMP131.exe, 0000000E.00000002.2325536566.00000000010F0000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000012.00000002.2429829682.00000000011BC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORTBB~	bUHMq54m6Q.exe, 00000000.00000003.2159759925.0000000005C56000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000002.2280792333.0000000005C5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORTf	bUHMq54m6Q.exe, 00000000.00000002.2276746268.000000000122E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://147.45.47.102:57893/hera/amadka.exe68.0	MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	bUHMq54m6Q.exe, 00000000.00000003.2150265902.0000000005C6F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2152690333.0000000005C93000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2151263071.0000000005C92000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2181530040.0000000005EFD000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2179554394.0000000005EFB000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2180030463.0000000005F00000.00000004.00000020.00020000.00000000.sdmp, RVFvq_w1ZQYbWeb Data.0.dr, 9V16nhm0bFZXWeb Data.0.dr, Lml4gt7uNt6lWeb Data.0.dr, uH4Klb1syK8iWeb Data.6.dr, KslfLLPbfavZWeb Data.6.dr, e0WJiscSE76mWeb Data.6.dr	false		high
http://https://t.me/risepro_bot7.102	RageMP131.exe, 0000000E.00000002.2325536566.00000000010F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORTq3i	MPGPH131.exe, 00000006.00000002.2275133356.0000000000CBE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_botr5	RageMP131.exe, 00000012.00000002.2429829682.00000000011BC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io/widget/demo/156.146.37.102d	RageMP131.exe, 0000000E.00000002.2325536566.00000000010AC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io/x	MPGPH131.exe, 00000007.00000002.2174199079.0000000001C27000.00000004.00000020.00020000.00000000.sdmp	false		high
http://193.233.132.56/cost/go.exe	bUHMq54m6Q.exe, 00000000.00000002.2276746268.00000000012BC000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2158606160.0000000005C71000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2159759925.0000000005C73000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000002.2280792333.0000000005C73000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2158512133.0000000005C71000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000007.00000002.2174199079.0000000001CA7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://db-ip.com/demo/home.php?s=156.146.37.102_i	RageMP131.exe, 00000012.00000002.2429829682.00000000011BC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io/e7	bUHMq54m6Q.exe, 00000000.00000002.2276746268.000000000129C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io/o	RageMP131.exe, 0000000E.00000002.2325536566.00000000010C3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORTP	bUHMq54m6Q.exe, 00000000.00000002.2280715188.0000000005C30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	bUHMq54m6Q.exe, 00000000.00000003.2150265902.0000000005C6F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2152690333.0000000005C93000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2151263071.0000000005C92000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2181530040.0000000005EFD000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2179554394.0000000005EFB000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2180030463.0000000005F00000.00000004.00000020.00020000.00000000.sdmp, RVFvq_w1ZQYbWeb Data.0.dr, 9V16nhm0bFZXWeb Data.0.dr, Lml4gt7uNt6lWeb Data.0.dr, uH4Klb1syK8iWeb Data.6.dr, KslfLLPbfavZWeb Data.6.dr, e0WJiscSE76mWeb Data.6.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/t	MPGPH131.exe, 00000007.00000002.2174199079.0000000001C5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORTPROCESSOR_LEVEL=6PROCES	RageMP131.exe, 0000000E.00000002.2325536566.000000000105E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_botisepro_bot_Aj	MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_botrisepro	RageMP131.exe, 0000000E.00000002.2325536566.00000000010F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://193.233.132.56/cost/go.exeTerracoin=	bUHMq54m6Q.exe, 00000000.00000003.2158606160.0000000005C71000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2159759925.0000000005C73000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000002.2280792333.0000000005C73000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2158512133.0000000005C71000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://db-ip.com/demo/home.php?s=156.146.37.102LS	MPGPH131.exe, 00000007.00000002.2174199079.0000000001CA7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	bUHMq54m6Q.exe, 00000000.00000003.2150265902.0000000005C6F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2152690333.0000000005C93000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2151263071.0000000005C92000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2181530040.0000000005EFD000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2179554394.0000000005EFB000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2180030463.0000000005F00000.00000004.00000020.00020000.00000000.sdmp, RVFvq_w1ZQYbWeb Data.0.dr, 9V16nhm0bFZXWeb Data.0.dr, Lml4gt7uNt6lWeb Data.0.dr, uH4Klb1syK8iWeb Data.6.dr, KsIfLLPbfavZWeb Data.6.dr, e0WJiscSE76mWeb Data.6.dr	false		high
http://https://ipinfo.io/widget/demo/156.146.37.102=	MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORT2	RageMP131.exe, 00000012.00000002.2429829682.0000000001147000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_botPrim	MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_botrisep	RageMP131.exe, 00000012.00000002.2429829682.00000000011BC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORT=L	MPGPH131.exe, 00000006.00000002.2282419782.0000000005A70000.00000004.00000020.00020000.00000000.sdmp	false		high

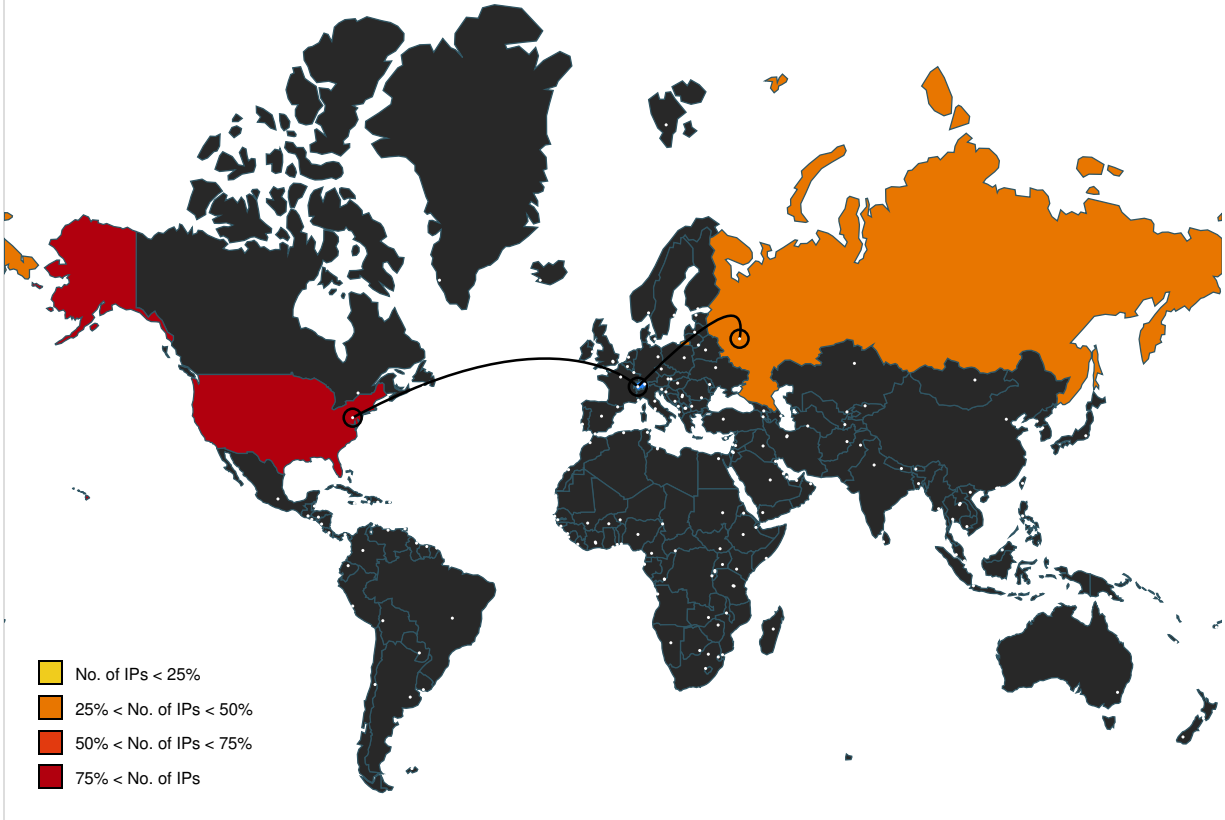
Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://ipinfo.io/https://www.maxmind.com/en/locate-my-ip-addressWs2_32.dll	bUHMq54m6Q.exe, 00000000.00000002.2272966412.000000000066D000.00000002.00000001.01000000.00000003.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2086040857.0000000001180000.00000004.00001000.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2114405302.0000000000C50000.00000004.00001000.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2277258884.0000000000105D000.00000002.00000001.01000000.00000004.sdmp, MPGPH131.exe, 00000007.00000002.2168458625.000000000105D000.00000002.00000001.01000000.00000004.sdmp, MPGPH131.exe, 00000007.00000003.2114630366.0000000001A50000.00000004.00001000.00020000.00000000.sdmp, RageMP131.exe, 0000000E.00000002.2324438250.00000000004BD000.00000002.00000001.01000000.00000008.sdmp, RageMP131.exe, 0000000E.00000003.2255008440.0000000002A30000.00000004.00001000.00020000.00000000.sdmp, RageMP131.exe, 00000012.00000002.2427181585.00000000004BD000.00000002.00000001.01000000.00000008.sdmp, RageMP131.exe, 00000012.00000003.2337606735.0000000002BE0000.00000004.00001000.00020000.00000000.sdmp	false		high
http:// https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	bUHMq54m6Q.exe, 00000000.00000003.2150265902.0000000005C6F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2152690333.0000000005C93000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2151263071.0000000005C92000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2181530040.0000000005EFD000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2179554394.0000000005EFB000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2180030463.0000000005F00000.00000004.00000020.00020000.00000000.sdmp, RVFvq_w1ZQYbWeb Data.0.dr, 9V16nhm0bFZXWeb Data.0.dr, Lml4gt7uNt6lWeb Data.0.dr, uH4Klb1syK8iWeb Data.6.dr, KsIfLLPbfavZWeb Data.6.dr, e0WJiscSE76mWeb Data.6.dr	false		high
http://upx.sf.net	Amcache.hve.10.dr	false		high
http://https://t.me/RiseProSUPPORT	bUHMq54m6Q.exe, 00000000.00000003.2159759925.0000000005C56000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000002.2276746268.00000000012E2E000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000002.2280792333.0000000005C5F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000002.2280715188.0000000005C30000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2275133356.0000000000CBE000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2282419782.0000000005A70000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000007.00000002.2174199079.0000000001C27000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 0000000E.00000002.2325536566.000000000105E000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000012.00000002.2429829682.0000000001147000.00000004.00000020.00020000.00000000.sdmp, NoSoV6eJxRbhlNXMC2XnYgm.zip.6.dr, eK26yDxmyAbMrjg7CdmfOmj.zip.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.ecosia.org/newtab/	bUHMq54m6Q.exe, 00000000.00000003.2150265902.0000000005C6F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2152690333.0000000005C93000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2151263071.0000000005C92000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2181530040.0000000005EFD000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2179554394.0000000005EFB000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2180030463.0000000005F00000.00000004.00000020.00020000.00000000.sdmp, RVFvq_w1ZQYbWeb Data.0.dr, 9V16nhm0bFZXWeb Data.0.dr, Lml4gt7uNt6lWeb Data.0.dr, uH4Klb1syK8iWeb Data.6.dr, KslfLLPbfavZWeb Data.6.dr, e0WJiscSE76mWeb Data.6.dr	false		high
http://https://ipinfo.io/Mozilla/5.0	bUHMq54m6Q.exe, 00000000.00000002.2276746268.00000000012A7000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000007.00000002.2174199079.0000000001C9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 0000000E.00000002.2325536566.00000000010D6000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000012.00000002.2429829682.00000000011BC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io:443/widget/demo/156.146.37.102	bUHMq54m6Q.exe, 00000000.00000002.2276746268.00000000012A7000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000007.00000002.2174199079.0000000001C9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 0000000E.00000002.2325536566.00000000010D6000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000012.00000002.2429829682.00000000011BC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	D87fZN3R3jFeplaces.sqlite.7.dr	false		high
http://193.233.132.56/cost/go.exeServer	MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://147.45.47.102:57893/hera/amadka.exe)=	bUHMq54m6Q.exe, 00000000.00000003.2158606160.0000000005C71000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2159759925.0000000005C73000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2158405940.0000000005C71000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000002.2280792333.0000000005C73000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2158512133.0000000005C71000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://db-ip.com:443/demo/home.php?s=156.146.37.102A	bUHMq54m6Q.exe, 00000000.00000002.2276746268.00000000012BC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://193.233.132.56/cost/go.exeWOUl-	MPGPH131.exe, 00000007.00000002.2174199079.0000000001CA7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	bUHMq54m6Q.exe, 00000000.00000003.2150265902.0000000005C6F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2152690333.0000000005C93000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2151263071.0000000005C92000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2181530040.0000000005EFD000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2179554394.0000000005EFB000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2180030463.0000000005F00000.00000004.00000020.00020000.00000000.sdmp, RVFvq_w1ZQYbWeb Data.0.dr, 9V16nhm0bFZXWeb Data.0.dr, Lml4gt7uNt6lWeb Data.0.dr, uH4Klb1syK8iWeb Data.6.dr, KslfLLPbfavZWeb Data.6.dr, e0WJiscSE76mWeb Data.6.dr	false		high
http://https://t.me/risepro_bot	RageMP131.exe, 00000012.00000002.2429829682.00000000011BC000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000012.00000002.2429829682.000000000121F000.00000004.00000020.00020000.00000000.sdmp, passwords.txt.0.dr, passwords.txt.6.dr	false		high
http://147.45.47.102:57893/hera/amadka.exeaO	MPGPH131.exe, 00000007.00000002.2174199079.0000000001CA7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.23	MPGPH131.exe, 00000007.00000002.2174199079.0000000001CA7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://crl.micro	MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ipinfo.io/	RageMP131.exe, 00000012.00000002.2429829682.0000000001180000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000012.00000002.2429829682.0000000001172000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.ZAnPVwXvBbYt	D87fZN3R3jFeplaces.sqlite.7.dr	false		high
http://https://www.maxmind.com/en/locate-my-ip-address	bUHMq54m6Q.exe, MPGPH131.exe	false		high
http://https://t.me/risepro_botz	bUHMq54m6Q.exe, 00000000.00000002.2276746268.00000000012BC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://193.233.132.56/cost/lenin.exe	MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000007.00000002.2174199079.0000000001CA7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.winimage.com/zLibDll	bUHMq54m6Q.exe, 00000000.00000002.2272966412.000000000066D000.00000002.00000001.01000000.00000003.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2086040857.0000000001180000.00000004.00001000.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2114405302.0000000000C50000.00000004.00001000.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2277258884.0000000000105D000.00000002.00000001.01000000.00000004.sdmp, MPGPH131.exe, 00000007.00000002.2168458625.000000000105D000.00000002.00000001.01000000.00000004.sdmp, MPGPH131.exe, 00000007.00000003.2114630366.0000000001A50000.00000004.00001000.00020000.00000000.sdmp, RageMP131.exe, 0000000E.00000002.2324438250.00000000004BD000.00000002.00000001.01000000.00000008.sdmp, RageMP131.exe, 0000000E.00000003.2255008440.0000000002A30000.00000004.00001000.00020000.00000000.sdmp, RageMP131.exe, 00000012.00000002.2427181585.00000000004BD000.00000002.00000001.01000000.00000008.sdmp, RageMP131.exe, 00000012.00000003.2337606735.0000000002BE0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org	D87fZN3R3jFeplaces.sqlite.7.dr	false		high
http://https://t.me/risepro_botrisepro;O	MPGPH131.exe, 00000007.00000002.2174199079.0000000001CA7000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://db-ip.com:443/demo/home.php?s=156.146.37.102	MPGPH131.exe, 00000006.00000002.2275133356.0000000000D36000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000007.00000002.2174199079.0000000001CA7000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 0000000E.00000002.2325536566.00000000010F0000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000012.00000002.2429829682.0000000011BC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io/$E	MPGPH131.exe, 00000006.00000002.2275133356.0000000000CF1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	bUHMq54m6Q.exe, 00000000.00000003.2150265902.0000000005C6F000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2152690333.0000000005C93000.00000004.00000020.00020000.00000000.sdmp, bUHMq54m6Q.exe, 00000000.00000003.2151263071.0000000005C92000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2181530040.0000000005EFD000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2179554394.0000000005EFB000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.2180030463.0000000005F00000.00000004.00000020.00020000.00000000.sdmp, RVFvq_w1ZQYbWeb Data.0.dr, 9V16nhm0bFZXWeb Data.0.dr, Lml4gt7uNt6lWeb Data.0.dr, uH4Klb1syK8iWeb Data.6.dr, KsIfLLPbfavZWeb Data.6.dr, e0WJiscSE76mWeb Data.6.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.117.186.192	ipinfo.io	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
147.45.47.126	unknown	Russian Federation		2895	FREE-NET-ASFREEnetEU	true
104.26.4.15	db-ip.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1437130
Start date and time:	2024-05-07 01:31:24 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 9m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	bUHMq54m6Q.exerenamed because original name is a hash value
Original Sample Name:	2cf4b5cf327757376e717ab5554b921b.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@13/58@3/3
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 67% • 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): dllhost.exe, WerFault.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.42.73.29
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, login.live.com, slscr.update.microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, ctldl.windowsupdate.com, umwatson.events.data.microsoft.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: bUHMq54m6Q.exe

Simulations

Behavior and APIs

Time	Type	Description
01:32:12	Task Scheduler	Run new task: MPGPH131 HR path: C:\ProgramData\MPGPH131\MPGPH131.exe
01:32:13	Task Scheduler	Run new task: MPGPH131 LG path: C:\ProgramData\MPGPH131\MPGPH131.exe
01:32:15	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run RageMP131 C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
01:32:27	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run RageMP131 C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
01:32:28	API Interceptor	2x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\MPGPH131\MPGPH131.exe

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2298896
Entropy (8bit):	7.943949707127546
Encrypted:	false
SSDEEP:	49152:JZZ2yJFMXgNp/R21ABbgdThoxEN2lcHmNNQfwo:JZZF7N1ROABbgdThog24fwo
MD5:	2CF4B5CF327757376E717AB5554B921B
SHA1:	020751E48F382DBD25341228E0ACF66818428B12
SHA-256:	A275C369EF53EBA4655CA43244E230FD7B38E45DBF25FC0B614918A58B3D07A6
SHA-512:	CECCBEAF87660EA08D9BDC5804546C16A2ABEA4F73C8F80345E711CF5C4A8AB9330CA64022B890457187BDE83DE2687177CB50C1A4FC1BF9D49054510E2418FA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....j.....s...s...s.e.p.%.s.e.v...s.e.t./.s..y..*.s..yw.=.s..yp.4.s..yv.u.s.e.w.6.s.e.u./.s.e.r.5.s...r...s..zz.2.s..z../.s..../.s..zq./.s.Rich..s.....PE..L....96f.....'.....X`P.....@.....h.....#...@.....Q.....p.....h.....`.....6..@..... ....`  2~.....@..@  0I...P.....@.....r.....@..@  X....p...L...D.....@..B.vm_sec..@.....@.....@....idata.....P.....@....tls.....`.....rsrc.....p.....@..@.themida. 5..@.....`....boot....t...`P..t.....`..`.reloc.....h.....#.

C:\ProgramData\MPGPH131\MPGPH131.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309

SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_MPGPH131.exe_5ae7e4c267f7e8254d33e44a3aef75514fc3925e_0010bad0_310ee076-0e1e-4dc2-a821-22b2cb294147\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.0528304363184986
Encrypted:	false
SSDEEP:	192:QKlcZzR8D107ETl6E6jjyZrofxjPzuiFGZ24lO826t:t2ReW7ET4jLPzuiFGY4lO8p
MD5:	55FFA6AEB68627E18595895A40485121
SHA1:	AE5696883F3C06E49D31DAB177D1223C6B39CFC4
SHA-256:	859047D27DE298B2397FF427B2C29AF186EA31070DE9401F1C329CD172538B29
SHA-512:	2E80144AC3251CA2BB9172822638597460BF76D3AFD7EE184AFFC904EA3B6E3109113FB3A23DA9A9EB9575F6D1D3BA455A4FF6004464D654BE28A285BDFB11D8
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.5.9.5.1.1.9.4.4.6.4.0.4.1.8.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.5.9.5.1.1.9.4.7.3.7.4.7.9.2.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.1.0.e.e.0.7.6.-.0.e.1.e.-.4.d.c.2.-.a.8.2.1.-.2.2.b.2.c.b.2.9.4.1.4.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.1.5.d.0.5.d.5.-.3.0.6.1.-.4.1.2.9.-.b.2.8.3.-.c.d.1.2.b.c.0.3.2.a.6.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.M.P.G.P.H.1.3.1...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.r.o.s.s.D.e.v.i.c.e.S.e.t.t.i.n.g.s.H.o.s.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.2.0.-.0.0.0.1.-.0.0.1.5.-.1.c.2.f.-.5.e.9.f.0.d.a.0.d.a.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.6.7.a.b.c.f.8.d.6.c.2.5.2.9.7.e.d.9.7.2.3.e.f.1.6.c.3.8.f.3.6.0.0.0.0.0.9.1.0.!.0.0.0.0.0.2.0.7.5.1.e.4.8.f.3.8.2.d.b.d.2.5.3.4.1.2.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bUHMq54m6Q.exe_7f5678ff3d44ce164b9187a831663245298324_7fe652d7_b9d6888b-1509-4a56-aeb6-1b74ada72881\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.0564993166343377
Encrypted:	false
SSDEEP:	192:kz2FyGpe0AYvcjyZrosLZuzuiFGZ24lO8w:DFyGpFAYvcjyuzuiFGY4lO8w
MD5:	2496724ADC3F946A9EC4B66BA7F8E3AF
SHA1:	413DB74471545DB74251D665B0E2655A98368916
SHA-256:	1E7358379E3E413E7E0B108224F599DA60E1D0ED170F5589194853F8B52601B7
SHA-512:	24698623A0845B1E59CC4229900A1CABDE1FB8536D0D869AC4F2B36BB2129D2C945B4792966B41CFFEB6854C34193AA13EEEA0EEB9E4E0900225A9D41B80EC3F
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.5.9.5.1.1.9.4.1.3.6.0.7.6.5.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.5.9.5.1.1.9.4.2.2.2.0.1.4.4.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.9.d.6.8.8.8.b.-.1.5.0.9.-.4.a.5.6.-.a.e.b.6.-.1.b.7.4.a.d.a.7.2.8.8.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.5.f.d.3.c.5.f.-.9.2.a.3.-.4.a.c.1.-.9.2.8.f.-.3.f.d.9.c.e.1.f.1.b.7.c.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.b.U.H.M.q.5.4.m.6.Q...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.r.o.s.s.D.e.v.i.c.e.S.e.t.t.i.n.g.s.H.o.s.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.9.c.-.0.0.0.1.-.0.0.1.5.-.9.5.8.0.-.b.d.9.d.0.d.a.0.d.a.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.6.7.a.b.c.f.8.d.6.c.2.5.2.9.7.e.d.9.7.2.3.e.f.1.6.c.3.8.f.3.6.0.0.0.0.0.9.1.0.!.0.0.0.0.0.2.0.7.5.1.e.4.8.f.3.8.2.d.b.d.2.5.3.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 6 23:32:21 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	121480
Entropy (8bit):	1.855363340823153
Encrypted:	false
SSDEEP:	384:DD+AADAd0Ftvk7wkhOv0YASdEGG3qAJzlZl0BaQfK+rF9z2:DD+he0FtvcU0YASrobaE9z
MD5:	D265223288CCD39728494EDACC4D45CD
SHA1:	4EC0FD691CD4E11EAD031D358DCFBF6A5C1E79E1

SHA-256:	3A1EE8B072CC72BC32AEDC6A301DC67B033B20CB4F6E4606AF43E0611AA6027A
SHA-512:	19C823276AD1500C61CE121857EC766FED99485B43E0491417FAEDFEE9A8630BEEEDAF7C4AB0B3F2000ABAF116B28B34B5C0C1D724A8E9A339B268B7A07111 7F
Malicious:	false
Reputation:	low
Preview:	MDMP..a..... .....h9f.....(.....I...#.....O.....`.....8.....T.....HJ..@.....,$.....&.....eJ.....&.. ....GenuineIntel.....T.....zh9f.....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .S.u.m.m.e.r. . T.i.m.e.....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8396
Entropy (8bit):	3.708401782548626
Encrypted:	false
SSDEEP:	192:R6l7wVeJBM6GKrP56Y2DDSU/yAgmfsJlyprw89btOsfKEPm:R6lXJ66PP56YeSUqAgmfsJlKtNfK
MD5:	BFF72A7437A4CFE9B3A33B115D4942B4
SHA1:	8296D052352D269EADE7E733B3B1C6BE03531913
SHA-256:	AE160FD624E0970377AF57CA774FAFDFCBF04F5819A2538C99F29860D75D9418
SHA-512:	4A2CEDDC0AAEB1DEEE590F581DD15059DDC4CCDA200452DD43A4B87F3312B30FC318DB4ACF2614B0C086B50272B47CF640A544BBA6678163593815AE84D8D 67
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.5.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-. 1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c. t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.2.0.5.7.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i. d.>.6.5.5.6.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3245.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4728
Entropy (8bit):	4.5356433746061215
Encrypted:	false
SSDEEP:	48:cvIwWl8zshQJg77al9rCBWpW8VYAYm8M4JkNFN9z+q8Yf5+EQyffd:uljfsI74Q7VgJqzRPQynd
MD5:	D52E3C37BBCBDD516F70697AC8B54A96
SHA1:	975DE1864954B059C8D6F50837E9526627C2FCB3
SHA-256:	28435826EB843D3C8F5F29C60181A36224782383BCF8B26141C324E232324EC2
SHA-512:	5D1673CA7EE38D7C0EEC780AD44D501F8E467C611ED38B8AA202ECEC840F74607DC02E2EB70CE07E8C01FEFC058CD92208AC0B2961CE00C2F21C7166BEF8E 07A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg n m="geoid" val="223" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtyp e" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="311915" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.78 9.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3C94.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 6 23:32:25 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	110138
Entropy (8bit):	1.9059204889344317
Encrypted:	false
SSDEEP:	384:1Y+sf5xZhwFtvF6VlpZdoVq3VorSJgX16lUHtFB9F1FqEOUw8xNvtz+7kpU:1Y+sB/+FtvF6kZde1jz+e
MD5:	3A3C0CE18EF40D4E92E7C7EF400F0EE8
SHA1:	A7B1ADF42CA16E93E32D0164D91D91F749CF5634
SHA-256:	063504D6E121A76A6CA07CBDDC067EFB18EA8840028299F85A2D8E2592FE28E6

SHA-512:	6F7D883A74620053431694C42B4A5CB83340FA69760F374D1DFB84F8C4650E455AB3034574CCC12EE34BFF9925CEC612C0289E9FB0E48B9250BFA2811C9E3B0
Malicious:	false
Preview:	MDMP..a..... .....h9f.....I...`#.....I.....`.....8.....T.....I...d.....#.....%.....eJ.....P&.. ....GenuineIntel.....T..... ...|h9f.....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .S.u.m.m.e.r. .T.i.m.e... .....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER461A.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	6362
Entropy (8bit):	3.7263411812944227
Encrypted:	false
SSDEEP:	192:R6l7wVeJKuD6nYi5JlDRprq89bAnsfkAm:R6lXJH6nYSJlzAsfy
MD5:	6A14978891945B9E38AC53D5780B96EE
SHA1:	2DCDB9B3AE42ACAC20BA24F2708601D1234962AE
SHA-256:	61BF7B38559DD5F584E31F7344B0BA23A363C59A6280FB571C73A1C2013E2A1E
SHA-512:	C9A8545A9119AF1C63531F023D104ADF3098A75DDC4637295468C66C457A5C02EF0A4583F83BC06DF79BC84E3B0E507AF0546D76017F268708CE7FD03167AB27
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.5.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-. 1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c. t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.2.0.5.7.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i. d.>.4.8.9.6.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER463A.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4718
Entropy (8bit):	4.523696716084494
Encrypted:	false
SSDEEP:	48:cvIwWl8zshQJg77al9rCBWpW8VYmYm8M4JkteF6I+q80v0S5+71lwfd:uljfsI74Q7VyJ/VA1I+d
MD5:	5CFBE0ADA8596312330D36347D38BFC8
SHA1:	F5C3AEED32ADDD63E4FA0B1A87E8C00AC2EC7BE3
SHA-256:	164763BF3B7E5CACB0CB189AB3E7D8235E6B0CD97DE6985C03953D21127826D7
SHA-512:	0B666C4E159C55B786FC002D513756A672049EE3810FFF8ECC1B47244C0F3AF9CC68A42B05ED76ADBDF6A276599E0A4F1AC98A1676DF647DB79FEAB20B9B4B 4C
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg n m="geoid" val="223" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtyp e" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="311915" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.78 9.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\Users\user\AppData\Local\RageMP131\RageMP131.exe

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2298896
Entropy (8bit):	7.943949707127546
Encrypted:	false
SSDEEP:	49152:JZZ2yJFMXgNp/R21ABbgdThoxEN2lcHmNNQfwo:JZZF7N1ROABbgdThog24fwo
MD5:	2CF4B5CF327757376E717AB5554B921B
SHA1:	020751E48F382DBD25341228E0ACF66818428B12
SHA-256:	A275C369EF53EBA4655CA43244E230FD7B38E45DBF25FC0B614918A58B3D07A6
SHA-512:	CECCBEAF87660EA08D9BDC5804546C16A2ABEA4F73C8F80345E711CF5C4A8AB9330CA64022B890457187BDE83DE2687177CB50C1A4FC1BF9D49054510E2418 FA
Malicious:	**true**

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....j.....s...s...s.e.p.%.s.e.v...s.e.t./.s..y..*.s..yw.=.s..yp.4.s..yv.u.s. e.w.6.s.e.u./.s.e.r.5.s...r...s..zz.2.s..z../.s..../.s..zq./.s.Rich..s.....PE..L....96f.....'.....X`P.....@.....h.....#...@.....Q.... ...p.....h.....`.....6..@..... ....` 2~.....@..@ 0I...P.....@... .....r.....@..@ X....p...L...D.....@..B.vm_sec..@.....@.....@....idata.....P.....@....tls.....`.....rsrc.....p..... .....@..@.themida. 5..@.....`....boot....t...`P..t.....`..`.reloc.....h.....#.

C:\Users\user\AppData\Local\RageMP131\RageMP131.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	2860
Entropy (8bit):	7.739784447128016
Encrypted:	false
SSDEEP:	48:9raVXZV//QWGPvcpJVfMR7kl8QbBHy3Rrl735OS1hcj8xNnDyBZVYun3KJ67k0Oj:yZV//Q1vcGQdHA30MNIzYu3KJZ
MD5:	CC7DEAFED3A6A0D17C8B8648F48BBB28
SHA1:	F132D9ADBFC2BD3D5605BCC2E9E5C1B06CA0A800
SHA-256:	6E29C3B738F43B9F11E9ACA40DA25E96C0FB91C23C6370AE0E3BBE9EF5E8D28F
SHA-512:	B930BD3E8E8B96ECAF0A1C30617CDFE0DB25918E1586286FC672A975723ED5B7D42FACD7DBD5F4F8C29B51E1C5DF760E126816BEB41EC661844A9BF56E1CD 209
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip, Author: Joe Security
Preview:	PK.....X.....Cookies\..PK.....XA.`%.....Cookies\Chrome_Default.txt....@.....i.&h.Cn..L...\.FA@.~..v7..O...%!es.f..../S..a...@.,ek.%.H.....</<2..,..I..w... ...1q.f.F+PiM.=h.5..2....0....O..u_.~}Z.UM.....y...Rj..4H..D...xLY@....[.d.c&.....G_.....j%q%....Y.|.....P...u..u..85/..Z`...-..c...^A8n...Y.3.....j.G!....c.....AM@!._W.yQbs.@... ..h.y.-.....|J..i...r....c....M...E...GS...C....X..C.U..v.%.....C,.L0,.....5.=....6.....PK.....Xj.d.....k.....information.txt.Y.R.H.}w..."..b..K.....q7...m..Y*.M.W.....J6..M+. B.Je...*..4 K.$.V.b8.j.*-.1.....Qm..fc.4z&.'....sJ8.r0..47...$4L..G.....9...d>R.26..yB.pp:kt.....B.fq4b.Q..`.Pm...C-.7...Z.T...P.?..|.X.>Mh8.+..9op^F..L...e.,.....gL....l.pp[.....|.4Ly..^.G/.8. .o.j}_...y.N...<....c....'|.Q@.<S....I>.'...$....o...hS..4..1...4O..jLv..Q....V.?..I.ZojS..... B. .w._.>.^}.].J.~....9K.u..2U.mZD..t.(...E./7..>:.....e.....,...,Ok..Oi.L..!..Km 2r.6.

C:\Users\user\AppData\Local\Temp\eK26yDxmyAbMrjg7CdmfOmj.zip

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	modified
Size (bytes):	2860
Entropy (8bit):	7.720862667626285
Encrypted:	false
SSDEEP:	48:9BarXZV//QWGPvcUVwNupS38FlwH5uuErj7qL8V2jm49zieHkzuXYzS3M/dRn3K6:6ZV//Q1vcUOIpSRTUZA99HFIzVT3KJ4
MD5:	7BAAF6EFC43F0561B018A102B243D445
SHA1:	F4061F8E1B37F9954E0A59E17592485CABD22721
SHA-256:	F1C1160A830CE3BDB771D6707C576A3773E82D56E7A13453C3F40776D04E68B7
SHA-512:	8DBE7AA30E74E36DD64C1493DA4DA71FCE6D44CA3C378E2587326E734929654F6D906D7BA74994C37C09CAB7287B2868C70790B8A5BCDCB64E0022656A5805 0
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: C:\Users\user\AppData\Local\Temp\eK26yDxmyAbMrjg7CdmfOmj.zip, Author: Joe Security

Preview:	PK.....X.....Cookies\..PK.....XA.`%.....Cookies\Chrome_Default.txt....@.....i.&h.Cn..L...\.FA@.~..v7..O...%!es.f..../S..a...@.,ek.%.H.....</<2..,...I..w... ...1q.f.F+PiM.=h.5..2....0....O..u_.~}Z.UM.....y...Rj..4H..D...xLY@....[.d.c&.....G_.....j%q%....Y.|.....P...u..u..85/..Z`...-..c...^A8n...Y.3.....j.G!....c.....AM@!._W.yQbs.@... ..h.y.-.....|J..i...r....c....M...E...GS...C....X..C.U..v.%.....C,.L0,.....5.=....6.....PK.....X.....information.txt.Y.S.F.....Lk.%....@...qh.}...Q#.\I..N...Nv.9%.a....v....O7i ..Q.Ws..}TE..|.....~.mT.!..(4.....&CF..G.S..G.C....C.*..\.....q2.....<...{?.y....}..@.8.... .I0..Tra.C.....o.d.}AU..DI.X,..'8.....8'Q.0D....4..|i`....*?Wz}?.....|%...V.{.....E......_.8..o.j}_...9 [N.../.g..Z..d.....c.G.AR...g.....Qk...s...b..N6.^.YV.....I.D?.C....F.B.....{#.Zo*U._.....1....~..|..a61,5.....\g&b...ADh...%.9....&Z...y.w...:*./'..Y.....R..L.e.W...7..Gd.&.a.o

C:\Users\user\AppData\Local\Temp\rage131MP.tmp

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.6612262562697895
Encrypted:	false
SSDEEP:	3:LsXUW:wUW
MD5:	D0A75EBFF72FA9B67AA2874A9CEF49CB
SHA1:	1321F58A68CAAF00627A03FA4E1D2C274B115757
SHA-256:	1D30EA87A95BC86360BD27D6F5399E126E4B2B135AC5BF437AD2FD213CE807B9
SHA-512:	95E55D568E8C4561468BDEEBFA6295701D009796FF0BDF5F949A09499540E3788D3FF697FF256760A069FD7FD4FC5B8E7690CA5921BAB76DD52D8B2E002DA39
Malicious:	false
Preview:	1715044508013

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\02zdBXl47cvzcookies.sqlite

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cook ie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08235737944063153
Encrypted:	false
SSDEEP:	12:DQAsfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQAsff32mNVpP965Ra8KN0MG/lO
MD5:	369B6DD66F1CAD49D0952C40FEB9AD41
SHA1:	D05B2DE29433FB113EC4C558FF33087ED7481DD4
SHA-256:	14150D582B5321D91BDE0841066312AB3E6673CA51C982922BC293B82527220D
SHA-512:	771054845B27274054B6C73776204C235C46E0C742ECF3E2D9B650772BA5D259C8867B2FA92C3A9413D3E1AD35589D8431AC683DF84A53E13CDE361789045928
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....}..}.....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\3b6N2Xdh3CYwplaces.sqlite

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, user version 75, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, coo kie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	5242880
Entropy (8bit):	0.0357803477377646
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWwJU0VnQphI1mJ/8GJK:58r54w0VW3xWB0VaI4
MD5:	76D181A334D47872CD2E37135CC83F95
SHA1:	B563370B023073CE6E0F63671AA4AF169ABBF4E1
SHA-256:	52D831CC6F56C3A25EB9238AAF25348E1C4A3D361DFE7F99DB1D37D89A0057FD
SHA-512:	23E0D43E4785E5686868D5448628718720C5A8D9328EE814CB77807260F7CDA2D01C5DEE8F58B5713F4F09319E6CB7AB24725078C01322BAE04777418A49A9F7
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....K.....j.....-a>.~...|0{dz.z.z"y.y3x.xKw.v.u.uGt.t;sAs.q.p.q.p{o.ohn.nem.n,m9l.k.lPj.j.h.h.g.d.c.c6b.b.a.a>..

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\8aQjHf7utHnSHistory

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1

Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216
SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47A
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\9V16nhm0bFZXWeb Data

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136471148832945
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c1/k4:MnlyfnGtxnfVuSVumEH1s4
MD5:	37B1FC046E4B29468721F797A2BB968D
SHA1:	50055EF1C50E4C1A7CCF7D00620E95128E4C448B
SHA-256:	7BBD5DFC9026E0D477B027B9A2A3F022F2E72FC9B4E05E697461A00677AE8EFD
SHA-512:	1D8A0F0AE76E5A1CF131F6D2C5156EA4204449942210EF029D5B018464355DBF94E2D8ABD6A5A9CDFE4271DCD22703BF26ECE8FEE902E122184680F1BB001149
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....l.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\D87fZN3R3jFeplaces.sqlite

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, user version 75, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	5242880
Entropy (8bit):	0.0357803477377646
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWwJU0VnQphI1mJ/8GJK:58r54w0VW3xWB0VaI4
MD5:	76D181A334D47872CD2E37135CC83F95
SHA1:	B563370B023073CE6E0F63671AA4AF169ABBF4E1
SHA-256:	52D831CC6F56C3A25EB9238AAF25348E1C4A3D361DFE7F99DB1D37D89A0057FD
SHA-512:	23E0D43E4785E5686868D5448628718720C5A8D9328EE814CB77807260F7CDA2D01C5DEE8F58B5713F4F09319E6CB7AB24725078C01322BAE04777418A49A9F7
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....K.....j.....-a>.~...|0{dz.z.z"y.y3x.xKw.v.u.uGt.t;sAs.q.p.q.p{o.ohn.nem.n,m9l.k.lPj.j.h.h.g.d.c.c6b.b.a.a>.. ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\EvDoFjSc27w4History

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UlYysX0IxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+Ul3iN0RSV0k3qLyj9

MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4
SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC0
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j.....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\FQEh_xU7vRTGWeb Data

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x37, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1239949490932863
Encrypted:	false
SSDEEP:	384:g2qOB1nxCkvSA1LyKOMq+8iP5GDHP/0j:9q+n0E91LyKOMq+8iP5GLP/0
MD5:	271D5F995996735B01672CF227C81C17
SHA1:	7AEAACD66A59314D1CBF4016038D3A0A956BAF33
SHA-256:	9D772D093F99F296CD906B7B5483A41573E1C6BD4C91EF8DBACDA79CDF1436B4
SHA-512:	62F15B7636222CA89796FCC23FC5722657382FAAAFEDC937506CAB3286AA696609F2A5A8F479158574D9FB92D37C0AA74EA15F7A172EBF1F3D260EF6124CF8B5
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....7.....j.....W.....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\JEr8lVONTEQKLogin Data

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\LmI4gt7uNt6lWeb Data

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136471148832945
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c1/k4:MnlyfnGtxnfVuSVumEH1s4
MD5:	37B1FC046E4B29468721F797A2BB968D
SHA1:	50055EF1C50E4C1A7CCF7D00620E95128E4C448B
SHA-256:	7BBD5DFC9026E0D477B027B9A2A3F022F2E72FC9B4E05E697461A00677AE8EFD
SHA-512:	1D8A0F0AE76E5A1CF131F6D2C5156EA4204449942210EF029D5B018464355DBF94E2D8ABD6A5A9CDFE4271DCD22703BF26ECE8FEE902E122184680F1BB00114
Malicious:	false

Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\P8T1BgZgt5t1Cookies

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 7, database pages 5, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6732424250451717
Encrypted:	false
SSDEEP:	24:TLO1nKbXYFpFNYcoqT1kwE6UwpQ9YHVXxZ6HfB:Tq1KLopF+SawLUO1Xj8B
MD5:	CFFF4E2B77FC5A18AB6323AF9BF95339
SHA1:	3AA2C2115A8EB4516049600E8832E9BFFE0C2412
SHA-256:	EC8B67EF7331A87086A6CC085B085A6B7FFFD325E1B3C90BD3B9B1B119F696AE
SHA-512:	0BFDC8D28D09558AA97F4235728AD656FE9F6F2C61DDA2D09B416F89AB60038537B7513B070B907E57032A68B9717F03575DB6778B68386254C8157559A3F1BC
Malicious:	false
Preview:	SQLite format 3.....@ .....j...$.....g..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\RVFvq_w1ZQYbWeb Data

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136471148832945
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c1/k4:MnlyfnGtxnfVuSVumEH1s4
MD5:	37B1FC046E4B29468721F797A2BB968D
SHA1:	50055EF1C50E4C1A7CCF7D00620E95128E4C448B
SHA-256:	7BBD5DFC9026E0D477B027B9A2A3F022F2E72FC9B4E05E697461A00677AE8EFD
SHA-512:	1D8A0F0AE76E5A1CF131F6D2C5156EA4204449942210EF029D5B018464355DBF94E2D8ABD6A5A9CDFE4271DCD22703BF26ECE8FEE902E122184680F1BB00114 9
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\dn59MYeqcUJmWeb Data

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x37, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1239949490932863
Encrypted:	false
SSDEEP:	384:g2qOB1nxCkvSA1LyKOMq+8iP5GDHP/0j:9q+n0E91LyKOMq+8iP5GLP/0
MD5:	271D5F995996735B01672CF227C81C17
SHA1:	7AEAACD66A59314D1CBF4016038D3A0A956BAF33
SHA-256:	9D772D093F99F296CD906B7B5483A41573E1C6BD4C91EF8DBACDA79CDF1436B4
SHA-512:	62F15B7636222CA89796FCC23FC5722657382FAAAFEDC937506CAB3286AA696609F2A5A8F479158574D9FB92D37C0AA74EA15F7A172EBF1F3D260EF6124CF8B
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....7.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\lKkvrLBG06UiLogin Data For Account

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe

File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\nQVbv3R1YjF8Cookies

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 6, database pages 5, cookie 0x3, schema 4, UTF-8, version-valid-for 6
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.8508558324143882
Encrypted:	false
SSDEEP:	24:TLlF1kwNbXYFpFNYcw+6UwcQVXH5fBaJvWKC0ABndzGrW7swaE:TxFawNLopFgU10XJBaEKQxdgQsw
MD5:	933D6D14518371B212F36C3835794D75
SHA1:	92D056D912B3C0260D379330D3CC0359B57A322B
SHA-256:	55390EE61FB85370A8A7F51A8DD5374F7B1801D1D7DF09D6A90CDD74ED6E7D1E
SHA-512:	EAC706D8A579500EADA26FB9883E1F3CE9112A03F38EE78B11B393AB0A3285945F8E06EB406BFC17D1CB540F840E435E515FABFC265399CE6F5193980FDE3F2C
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\oVix2UaWI8VCHistory

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216
SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47A
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\q58jgT3UDnoOWeb Data

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x37, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1239949490932863
Encrypted:	false

SSDEEP:	384:g2qOB1nxCkvSA1LyKOMq+8iP5GDHP/0j:9q+n0E91LyKOMq+8iP5GLP/0
MD5:	271D5F995996735B01672CF227C81C17
SHA1:	7AEAACD66A59314D1CBF4016038D3A0A956BAF33
SHA-256:	9D772D093F99F296CD906B7B5483A41573E1C6BD4C91EF8DBACDA79CDF1436B4
SHA-512:	62F15B7636222CA89796FCC23FC5722657382FAAAFEDC937506CAB3286AA696609F2A5A8F479158574D9FB92D37C0AA74EA15F7A172EBF1F3D260EF6124CF8B
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....7.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\w07ebxHrMjWrHistory

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UIYysX0lxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+UI3iN0RSV0k3qLyj9
MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4
SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC0 0
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\spanlgSFE9XfRUKm\wib805ADjjQsLogin Data

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 2, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8745947603342119
Encrypted:	false
SSDEEP:	96:aZ8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:W8yLG7IwRWf4
MD5:	378391FDB591852E472D99DC4BF837DA
SHA1:	10CB2CDAD4EDCCACE0A7748005F52C5251F6F0E0
SHA-256:	513C63B0E44FFDE2B4E511A69436799A8B59585CB0EB5CCFDA7A9A8F06BA4808
SHA-512:	F099631BEC265A6E8E4F8808270B57FFF28D7CBF75CC6FA046BB516E8863F36E8506C7A38AD682132FCB1134D26326A58F5B588B9EC9604F09FD7155B2AEF2D
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08235737944063153
Encrypted:	false
SSDEEP:	12:DQAsfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQAsff32mNVpP965Ra8KN0MG/lO
MD5:	369B6DD66F1CAD49D0952C40FEB9AD41
SHA1:	D05B2DE29433FB113EC4C558FF33087ED7481DD4
SHA-256:	14150D582B5321D91BDE0841066312AB3E6673CA51C982922BC293B82527220D
SHA-512:	771054845B27274054B6C73776204C235C46E0C742ECF3E2D9B650772BA5D259C8867B2FA92C3A9413D3E1AD35589D8431AC683DF84A53E13CDE361789045928
Malicious:	false

Preview:	SQLite format 3.....@ .....j.....}..}.....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\1oBLao5WFReeLogin Data For Account

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, user version 75, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	5242880
Entropy (8bit):	0.0357803477377646
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWwJU0VnQphI1mJ/8GJK:58r54w0VW3xWB0VaI4
MD5:	76D181A334D47872CD2E37135CC83F95
SHA1:	B563370B023073CE6E0F63671AA4AF169ABBF4E1
SHA-256:	52D831CC6F56C3A25EB9238AAF25348E1C4A3D361DFE7F99DB1D37D89A0057FD
SHA-512:	23E0D43E4785E5686868D5448628718720C5A8D9328EE814CB77807260F7CDA2D01C5DEE8F58B5713F4F09319E6CB7AB24725078C01322BAE04777418A49A9F7
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....K.....j.....-a>.~...|0{dz.z.z"y.y3x.xKw.v.u.uGt.t;sAs.q.p.q.p{o.ohn.nem.n,m9l.k.lPj.j.h.h.g.d.c.c6b.b.a.a>..

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Bs1Rik95T3UPWeb Data

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x37, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1239949490932863
Encrypted:	false
SSDEEP:	384:g2qOB1nxCkvSA1LyKOMq+8iP5GDHP/0j:9q+n0E91LyKOMq+8iP5GLP/0
MD5:	271D5F995996735B01672CF227C81C17
SHA1:	7AEAACD66A59314D1CBF4016038D3A0A956BAF33
SHA-256:	9D772D093F99F296CD906B7B5483A41573E1C6BD4C91EF8DBACDA79CDF1436B4
SHA-512:	62F15B7636222CA89796FCC23FC5722657382FAAAFEDC937506CAB3286AA696609F2A5A8F479158574D9FB92D37C0AA74EA15F7A172EBF1F3D260EF6124CF8B
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....7.....j.....W.....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, user version 75, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	5242880
Entropy (8bit):	0.0357803477377646
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWwJU0VnQphI1mJ/8GJK:58r54w0VW3xWB0VaI4
MD5:	76D181A334D47872CD2E37135CC83F95
SHA1:	B563370B023073CE6E0F63671AA4AF169ABBF4E1
SHA-256:	52D831CC6F56C3A25EB9238AAF25348E1C4A3D361DFE7F99DB1D37D89A0057FD
SHA-512:	23E0D43E4785E5686868D5448628718720C5A8D9328EE814CB77807260F7CDA2D01C5DEE8F58B5713F4F09319E6CB7AB24725078C01322BAE04777418A49A9F7
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....K.....j.....-a>.~...|0{dz.z.z"y.y3x.xKw.v.u.uGt.t;sAs.q.p.q.p{o.ohn.nem.n,m9l.k.lPj.j.h.h.g.d.c.c6b.b.a.a>.. ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\F27iDkUSbUX4History

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216
SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47A
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\GoTBCXWsNltoCookies

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 6, database pages 5, cookie 0x3, schema 4, UTF-8, version-valid-for 6
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.8508558324143882
Encrypted:	false
SSDEEP:	24:TLlF1kwNbXYFpFNYcw+6UwcQVXH5fBaJvWKC0ABndzGrW7swaE:TxFawNLopFgU10XJBaEKQxdgQsw
MD5:	933D6D14518371B212F36C3835794D75
SHA1:	92D056D912B3C0260D379330D3CC0359B57A322B
SHA-256:	55390EE61FB85370A8A7F51A8DD5374F7B1801D1D7DF09D6A90CDD74ED6E7D1E
SHA-512:	EAC706D8A579500EADA26FB9883E1F3CE9112A03F38EE78B11B393AB0A3285945F8E06EB406BFC17D1CB540F840E435E515FABFC265399CE6F5193980FDE3F2C
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\IuMVYmRLxIIELogin Data

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782

Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\KsIfLLPbfavZWeb Data

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136471148832945
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c1/k4:MnlyfnGtxnfVuSVumEH1s4
MD5:	37B1FC046E4B29468721F797A2BB968D
SHA1:	50055EF1C50E4C1A7CCF7D00620E95128E4C448B
SHA-256:	7BBD5DFC9026E0D477B027B9A2A3F022F2E72FC9B4E05E697461A00677AE8EFD
SHA-512:	1D8A0F0AE76E5A1CF131F6D2C5156EA4204449942210EF029D5B018464355DBF94E2D8ABD6A5A9CDFE4271DCD22703BF26ECE8FEE902E122184680F1BB001149
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\SrMOR5IqDZZTCookies

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 7, database pages 5, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6732424250451717
Encrypted:	false
SSDEEP:	24:TLO1nKbXYFpFNYcoqT1kwE6UwpQ9YHVXxZ6HfB:Tq1KLopF+SawLUO1Xj8B
MD5:	CFFF4E2B77FC5A18AB6323AF9BF95339
SHA1:	3AA2C2115A8EB4516049600E8832E9BFFE0C2412
SHA-256:	EC8B67EF7331A87086A6CC085B085A6B7FFFD325E1B3C90BD3B9B1B119F696AE
SHA-512:	0BFDC8D28D09558AA97F4235728AD656FE9F6F2C61DDA2D09B416F89AB60038537B7513B070B907E57032A68B9717F03575DB6778B68386254C8157559A3F1BC
Malicious:	false
Preview:	SQLite format 3.....@ .....j...$.....g.....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\TQL0dLOETHSsHistory

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UIYysX0IxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+UI3iN0RSV0k3qLyj9
MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4

SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC0 0
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\W4StvYRvRm8RLogin Data

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 2, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8745947603342119
Encrypted:	false
SSDEEP:	96:aZ8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:W8yLG7lwRWf4
MD5:	378391FDB591852E472D99DC4BF837DA
SHA1:	10CB2CDAD4EDCCACE0A7748005F52C5251F6F0E0
SHA-256:	513C63B0E44FFDE2B4E511A69436799A8B59585CB0EB5CCFDA7A9A8F06BA4808
SHA-512:	F099631BEC265A6E8E4F8808270B57FFF28D7CBF75CC6FA046BB516E8863F36E8506C7A38AD682132FCB1134D26326A58F5B588B9EC9604F09FD7155B2AEF2D
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\djGL4gOVacKhHistory

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UIYysX0IxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+UI3iN0RSV0k3qLyj9
MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4
SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC0 0
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\e0WJiscSE76mWeb Data

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136471148832945
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c1/k4:MnlyfnGtxnfVuSVumEH1s4
MD5:	37B1FC046E4B29468721F797A2BB968D
SHA1:	50055EF1C50E4C1A7CCF7D00620E95128E4C448B
SHA-256:	7BBD5DFC9026E0D477B027B9A2A3F022F2E72FC9B4E05E697461A00677AE8EFD
SHA-512:	1D8A0F0AE76E5A1CF131F6D2C5156EA4204449942210EF029D5B018464355DBF94E2D8ABD6A5A9CDFE4271DCD22703BF26ECE8FEE902E122184680F1BB00114 9
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uH4Klb1syK8iWeb Data	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136471148832945
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c1/k4:MnlyfnGtxnfVuSVumEH1s4
MD5:	37B1FC046E4B29468721F797A2BB968D
SHA1:	50055EF1C50E4C1A7CCF7D00620E95128E4C448B
SHA-256:	7BBD5DFC9026E0D477B027B9A2A3F022F2E72FC9B4E05E697461A00677AE8EFD
SHA-512:	1D8A0F0AE76E5A1CF131F6D2C5156EA4204449942210EF029D5B018464355DBF94E2D8ABD6A5A9CDFE4271DCD22703BF26ECE8FEE902E122184680F1BB00114 9
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uyAd3P89yfWTHistory	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216
SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47 A
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\vCcKyxUjjGyAWeb Data	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x37, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1239949490932863
Encrypted:	false
SSDEEP:	384:g2qOB1nxCkvSA1LyKOMq+8iP5GDHP/0j:9q+n0E91LyKOMq+8iP5GLP/0
MD5:	271D5F995996735B01672CF227C81C17
SHA1:	7AEAACD66A59314D1CBF4016038D3A0A956BAF33
SHA-256:	9D772D093F99F296CD906B7B5483A41573E1C6BD4C91EF8DBACDA79CDF1436B4
SHA-512:	62F15B7636222CA89796FCC23FC5722657382FAAAFEDC937506CAB3286AA696609F2A5A8F479158574D9FB92D37C0AA74EA15F7A172EBF1F3D260EF6124CF8B
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....7.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\z81g9YDMLrJHWeb Data	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x37, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608

Entropy (8bit):	1.1239949490932863
Encrypted:	false
SSDEEP:	384:g2qOB1nxCkvSA1LyKOMq+8iP5GDHP/0j:9q+n0E91LyKOMq+8iP5GLP/0
MD5:	271D5F995996735B01672CF227C81C17
SHA1:	7AEAACD66A59314D1CBF4016038D3A0A956BAF33
SHA-256:	9D772D093F99F296CD906B7B5483A41573E1C6BD4C91EF8DBACDA79CDF1436B4
SHA-512:	62F15B7636222CA89796FCC23FC5722657382FAAAFEDC937506CAB3286AA696609F2A5A8F479158574D9FB92D37C0AA74EA15F7A172EBF1F3D260EF6124CF8B
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....7.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\trixylgSFE9XfRUKm\Cookies\Chrome_Default.txt

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	ASCII text, with very long lines (369), with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	6.005544722730675
Encrypted:	false
SSDEEP:	12:c7F2v4kMx/6UsMbf4/LJPhvkRj6a9kuEYTCRopYxOOVtouEYv:SCJyHXbfQJPh8RdkYiFoYv
MD5:	987FB1A1830B0EB5C0D306F8A2DE9981
SHA1:	8374E6320AD99C3FF177A9889F1AB75448F6EB19
SHA-256:	5EF24A6CE57CA3048431555909EC23CD5494DA76845F84271946442249DDA891
SHA-512:	9E2A48264084B79051FC275DD7780A5552B56220459A1CDDBE6F6A307FE0E5759AE20BC243D085D9734153879AC4E66233AB83F92551DD8092EABF85B16F2D15
Malicious:	false
Preview:	.google.com.TRUE./.TRUE.1712298002.NID.ENC893*_djEwx6CLkXLg8AuSZWCgylmAsMNnd1LSfbcL+lfCgMvX/m5IrzdSwxt6X6n5S6C7wCoUoWvuixZpzrMizGZ c5ohIpmsvlOrGTOhFkQ4+lCF6fVH0QNPBBb27o2nXM8em7EAYS1bYZC2LV04SqpgyxJmdfFA7UyWUoK8kFZQDRl0vdOzWdvAoumw2skuCCtJC2oG3z3OYbLT LDbM7wYvVmfDeqtnZRihAAt+ptql6cfY1a+KO9XP+4XkDSXW7JhsexYHBqzSSBmUisGZ7f9E=_DrTFYLsM7YVgEN6pCv/RXeb8Bq748EwHbsLCIGv1kEc=*...google.c om.FALSE./.TRUE.1699078840.1P_JAR.ENC893*_djEwZKzV9KAslchfQWnVTck71JHMVRC24lvAWgdl5WpYIXllNsbQSVWzkKU=_DrTFYLsM7YVgEN6pCv/RXeb8Bq7 48EwHbsLCIGv1kEc=*..

C:\Users\user\AppData\Local\Temp\trixylgSFE9XfRUKm\information.txt

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	6788
Entropy (8bit):	5.454511401811121
Encrypted:	false
SSDEEP:	96:xyONORzSJLcBC1IUlzhge+U8Acf99+KQeTw47OGhLfgAgkM4/DhPigy62/OA61Yg:xYRIL84IUlzhsB
MD5:	06FC6A2B56EABC4E7CDD6DE8AC35FB9F
SHA1:	88FE1D2F77ACBCCA7A7621611721CF6DD22CE3F9
SHA-256:	B0E5B51EE03901CB820B662ADB6337F863E4272A5A06DF904ECE22EA2443BD97
SHA-512:	1087D72E81BDC0017052B73839F034C9935AF7EC8545A9B61EA1927E17DFFABD555B1D2F5BE96D0084A5C2336416A0683C8B90C9FCCC22DA99B15BAB7ED782 5
Malicious:	false
Preview:	Build: combo..Version: 2.0....Date: Tue May 7 01:32:17 2024.MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06..GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6 963}..HWID: 904752e9437da3bfff870d09bb5572b2....Path: C:\Users\user\Desktop\bUHMq54m6Q.exe..Work Dir: C:\Users\user\AppData\Local\Temp\trixylgSFE9XfRU Km....IP: 156.146.37.102..Location: US, New York City..ZIP (Autofills): -..Windows: Windows 10 Pro [x64]..Computer Name: 390120 [WORKGROUP]..User Name: user..Display Resolution: 1280x1024..Display Language: en-CH..Keyboard Languages: English (United Kingdom) / English (United Kingdom)..Local Time: 7/5/2024 1: 32:17..TimeZone: UTC1....[Hardware]..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..CPU Count: 4..RAM: 8191 MB..VideoCard #0: Microsoft Basic Display Adapter....[Processes]..System [4]..Registry [92]..smss.exe [328]..csrss.exe [412]..wininit.exe [488]..csrss.exe [496]..winlogon.exe [560]..services.exe [632]..lsass.exe [652]..svchost.exe [752]..fontdrvhost.exe [780]..fontd

C:\Users\user\AppData\Local\Temp\trixylgSFE9XfRUKm\passwords.txt

Process:	C:\Users\user\Desktop\bUHMq54m6Q.exe
File Type:	Unicode text, UTF-8 text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	4897
Entropy (8bit):	2.518316437186352
Encrypted:	false
SSDEEP:	48:4MMMMMMMMMdMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMMMdMMMMMMMM3:q
MD5:	B3E9D0E1B8207AA74CB8812BAAF52EAE

SHA1:	A2DCE0FB6B0BBC955A1E72EF3D87CADCC6E3CC6B
SHA-256:	4993311FC913771ACB526BB5EF73682EDA69CD31AC14D25502E7BDA578FFA37C
SHA-512:	B17ADF4AA80CADC581A09C72800DA22F62E5FB32953123F2C513D2E88753C430CC996E82AAE7190C8CB3340FCF2D9E0D759D99D909D2461369275FBE5C68C2A
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Cookies\Chrome_Default.txt

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	ASCII text, with very long lines (369), with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	6.005544722730675
Encrypted:	false
SSDEEP:	12:c7F2v4kMx/6UsMbf4/LJPhvkRj6a9kuEYTCRopYxOOVtouEYv:SCJyHXbfQJPh8RdkYiFoYv
MD5:	987FB1A1830B0EB5C0D306F8A2DE9981
SHA1:	8374E6320AD99C3FF177A9889F1AB75448F6EB19
SHA-256:	5EF24A6CE57CA3048431555909EC23CD5494DA76845F84271946442249DDA891
SHA-512:	9E2A48264084B79051FC275DD7780A5552B56220459A1CDDBE6F6A307FE0E5759AE20BC243D085D9734153879AC4E66233AB83F92551DD8092EABF85B16F2D15
Malicious:	false
Preview:	.google.com.TRUE./.TRUE.1712298002.NID.ENC893*_djEwx6CLkXLg8AuSZWCgylmAsMNnd1LSfbcL+IfCgMvX/m5IrzdSwxt6X6n5S6C7wCoUoWvuixZpzrMizGZc5ohlpmsvlOrGTOhFkQ4+lCF6fVH0QNPBBb27o2nXM8em7EAYS1bYZC2LV04SqpgyxJmdfFA7UyWUoK8kFZQDRl0vdOzWdvAoumw2skuCCtJC2oG3z3OYbLTLDbM7wYvVmfDeqtnZRihAAt+ptql6cfY1a+KO9XP+4XkDSXW7JhsexYHBqzSSBmUisGZ7f9E=_DrTFYLsM7YVgEN6pCv/RXeb8Bq748EwHbsLCIGv1kEc=*...google.com.FALSE./.TRUE.1699078840.1P_JAR.ENC893*_djEwZKzV9KAslchfQWnVTck71JHMVRC24lvAWgdl5WpYIXIlNsbQSVWzkKU=_DrTFYLsM7YVgEN6pCv/RXeb8Bq748EwHbsLCIGv1kEc=*..

C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	6763
Entropy (8bit):	5.453486822202273
Encrypted:	false
SSDEEP:	96:xysBORzSLcBC1IUlzhge+U8Acf99+KQeTw47OGhLfgAgkM4/DhPigy62/OA61YLv:xWRW84IUlzhPB
MD5:	B8958E5F1DE6D63E8AC54C767F4BEF84
SHA1:	C4B15EDB99B71BA90A811636B2CAEC9EAC30EC90
SHA-256:	A07F9B147FBCC63536AFE4F3F3D7294E1BD64105A4EEBEB2663322F5C6882F61
SHA-512:	6BCB2BC14DA4740C943A3EFDF0286183C12A4AE7338281B4EFCCA8DC471C4CA633C0FA9945EB2B7F8E2AFB5EF9FEA032AD11E468C059DE1DD6A0897DABF83365
Malicious:	false
Preview:	Build: combo..Version: 2.0....Date: Tue May 7 01:32:20 2024.MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06..GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}..HWID: 904752e9437da3bfff870d09bb5572b2....Path: C:\ProgramData\MPGPH131\MPGPH131.exe..Work Dir: C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs....IP: 156.146.37.102..Location: US, New York City..ZIP (Autofills): -..Windows: Windows 10 Pro [x64]..Computer Name: 390120 [WORKGROUP]..User Name: user..Display Resolution: 1280x1024..Display Language: en-CH..Keyboard Languages: English (United Kingdom) / English (United Kingdom)..Local Time: 7/5/2024 1:32:20..TimeZone: UTC1....[Hardware]..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..CPU Count: 4..RAM: 8191 MB..VideoCard #0: Microsoft Basic Display Adapter....[Processes]..System [4]..Registry [92]..smss.exe [328]..csrss.exe [412]..wininit.exe [488]..csrss.exe [496]..winlogon.exe [560]..services.exe [632]..lsass.exe [652]..svchost.exe [752]..fontdrvhost.exe [780]..fontdrvho

C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\passwords.txt

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	Unicode text, UTF-8 text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	4897
Entropy (8bit):	2.518316437186352
Encrypted:	false
SSDEEP:	48:4MMMMMMMMMdMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMMMdMMMMMMMM3:q
MD5:	B3E9D0E1B8207AA74CB8812BAAF52EAE
SHA1:	A2DCE0FB6B0BBC955A1E72EF3D87CADCC6E3CC6B
SHA-256:	4993311FC913771ACB526BB5EF73682EDA69CD31AC14D25502E7BDA578FFA37C
SHA-512:	B17ADF4AA80CADC581A09C72800DA22F62E5FB32953123F2C513D2E88753C430CC996E82AAE7190C8CB3340FCF2D9E0D759D99D909D2461369275FBE5C68C2A
Malicious:	false

Preview:	....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1835008
Entropy (8bit):	4.47233161646703
Encrypted:	false
SSDEEP:	6144:kzZfpi6ceLPx9skLmb0fvZWSP3aJG8nAgeiJRMMhA2zX4WABluuNWjDH5S:KZHtvZWOKnMM6bFpMj4
MD5:	7089E7B13B3F7D5480AC10E9FC9BC7BD
SHA1:	B80DCAABFC25F3670FA3EF3D0892CCFB4687B462
SHA-256:	1440607BC822FC949BE90C3A333B2C52EF52E3F0ADFE88A9D28AD0FFC23F5272
SHA-512:	AE6085618880C9A12125CADB435C05F5ACF31739DE941DD330E040C0339730E2E37C61EAD3A41DEE36AED981B3A9078102D4EDF86B4F86A4AD5DE879E714313
Malicious:	false
Preview:	regfH...H....\.Z..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e....c...b...#.....c...b...#.....c...b...#.....rmtm..O..... ....99X..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.943949707127546
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:	bUHMq54m6Q.exe
File size:	2'298'896 bytes
MD5:	2cf4b5cf327757376e717ab5554b921b
SHA1:	020751e48f382dbd25341228e0acf66818428b12
SHA256:	a275c369ef53eba4655ca43244e230fd7b38e45dbf25fc0b614918a58b3d07a6
SHA512:	ceccbeaf87660ea08d9bdc5804546c16a2abea4f73c8f80345e711cf5c4a8ab9330ca64022b890457187bde83de2687177cb50c1a4fc1bf9d49054510e2418fa
SSDEEP:	49152:JZZ2yJFMXgNp/R21ABbgdThoxEN2lcHmNNQfwo:JZZF7N1ROABbgdThog24fwo
TLSH:	81B533E824E3CFADD275EBF22503911944606F61DFE24BC4B24F696DABE264D437031A
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....j.....s...s...s.e.p.%.s.e.v...s.e.t./.s..y..*.s..yw.=.s..yp.4.s..yv.u.s.e.w.6.s.e.u./.s.e.r.5.s...r...s..zz.2.s..z../.s...../.s

File Icon

Icon Hash:	1e637808c76c1d83

Static PE Info

General

Entrypoint:	0x906058
Entrypoint Section:	.boot
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, TERMINAL_SERVER_AWARE
Time Stamp:	0x663639CA [Sat May 4 13:36:10 2024 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:	63814aaf116ba6abb6496ce4bcad24c6

Entrypoint Preview

Instruction
call 00007FA7CD44E5F0h
push ebx
mov ebx, esp
push ebx
mov esi, dword ptr [ebx+08h]
mov edi, dword ptr [ebx+10h]
cld
mov dl, 80h
mov al, byte ptr [esi]
inc esi
mov byte ptr [edi], al
inc edi
mov ebx, 00000002h
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FA7CD44E48Ch
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FA7CD44E4F3h
xor eax, eax
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FA7CD44E587h
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl

Instruction
adc eax, eax
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
je 00007FA7CD44E4AAh
push edi
mov eax, eax
sub edi, eax
mov al, byte ptr [edi]
pop edi
mov byte ptr [edi], al
inc edi
mov ebx, 00000002h
jmp 00007FA7CD44E43Bh
mov eax, 00000001h
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jc 00007FA7CD44E48Ch
sub eax, ebx
mov ebx, 00000001h
jne 00007FA7CD44E4CAh
mov ecx, 00000001h
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc ecx, ecx
add dl, dl
jne 00007FA7CD44E4A7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jc 00007FA7CD44E48Ch
push esi
mov esi, edi
sub esi, ebp

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1a518b	0x184	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a7000	0xc8c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x68e000	0x10	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x1a6018	0x18	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x18369c	0x40	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x1000	0x15bae8	0x80000	71df898e3bb7791f76e12ed59326dcd2	False	1.000030517578125	data	7.99965539534534	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
	0x15d000	0x27e32	0xc600	d46b2925dda747e309f73efc7cfe5f72	False	0.9986979166666666	data	7.995213678819302	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x185000	0x4930	0x800	3418c8de7b7967df6bb6c2c10ed53efb	False	0.9267578125	data	7.434788372867102	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
	0x18a000	0xc8c0	0x7200	ab55f75c506de7bda0f6900ce3592598	False	0.9992461622807017	interLaced eXtensible Trace (LXT) file (Version 19394)	7.990156009217108	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x197000	0x9858	0x4c00	b115c4aeaf5dbd0a5ed6289fe244caf5	False	0.9952713815789473	OpenPGP Public Key	7.97673825198549	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.vm_sec	0x1a1000	0x4000	0x4000	260e2630b7c17aea8fcc14acc331fbdc	False	0.1627197265625	data	2.8943699511117487	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x1a5000	0x1000	0x400	c9c064d6bd76a21fe27ddabad4c1bad5	False	0.3994140625	data	3.405869808210115	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x1a6000	0x1000	0x200	e0820cafed729136bac879e4277031ad	False	0.056640625	data	0.18120187678200297	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x1a7000	0xca00	0xca00	128d0357f9cf8c6ae4deac65154bce26	False	0.6009243502475248	DIY-Thermocam raw data (Lepton 2.x), scale 0-0, spot sensor temperature 0.000000, unit celsius, color scheme 0, calibration: offset 0.000000, slope 479547022718174183989048246272 0.000000	5.557009435024348	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.themida	0x1b4000	0x352000	0x0	d41d8cd98f00b204e9800998ecf8427e	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.boot	0x506000	0x187400	0x187400	c1e1fc63d9c36264abf090352999e312	False	0.9858744758386582	data	7.954415800190369	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x68e000	0x1000	0x10	9a86cd9aad32621e9b3fc39ac1644b9c	False	1.5	GLS_BINARY_LSB_FIRST	2.474601752714581	IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x1a7280	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	Russian	Russia	0.31402439024390244
RT_ICON	0x1a78f8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	Russian	Russia	0.42338709677419356
RT_ICON	0x1a7bf0	0x1e8	Device independent bitmap graphic, 24 x 48 x 4, image size 288	Russian	Russia	0.5061475409836066
RT_ICON	0x1a7de8	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	Russian	Russia	0.5675675675675675
RT_ICON	0x1a7f20	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Russian	Russia	0.46961620469083154
RT_ICON	0x1a8dd8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Russian	Russia	0.4020758122743682
RT_ICON	0x1a9690	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Russian	Russia	0.45506912442396313
RT_ICON	0x1a9d68	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Russian	Russia	0.2904624277456647
RT_ICON	0x1aa2e0	0x4b55	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	Russian	Russia	0.9921182266009853
RT_ICON	0x1aee48	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Russian	Russia	0.316701244813278
RT_ICON	0x1b1400	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Russian	Russia	0.36186679174484054
RT_ICON	0x1b24b8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Russian	Russia	0.42418032786885246
RT_ICON	0x1b2e50	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Russian	Russia	0.5026595744680851
RT_GROUP_ICON	0x1b32c8	0xbc	data	Russian	Russia	0.6170212765957447
RT_VERSION	0x1b3394	0x398	OpenPGP Public Key	Russian	Russia	0.42282608695652174
RT_MANIFEST	0x1b373c	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States	0.5931758530183727

Imports

DLL	Import
kernel32.dll	GetModuleHandleA
USER32.dll	wsprintfA
GDI32.dll	CreateCompatibleBitmap
ADVAPI32.dll	RegQueryValueExA
SHELL32.dll	ShellExecuteA
ole32.dll	CoInitialize
WS2_32.dll	WSAStartup
CRYPT32.dll	CryptUnprotectData
SHLWAPI.dll	PathFindExtensionA
gdiplus.dll	GdipGetImageEncoders
SETUPAPI.dll	SetupDiEnumDeviceInfo
ntdll.dll	RtlUnicodeStringToAnsiString
RstrtMgr.DLL	RmStartSession

Possible Origin

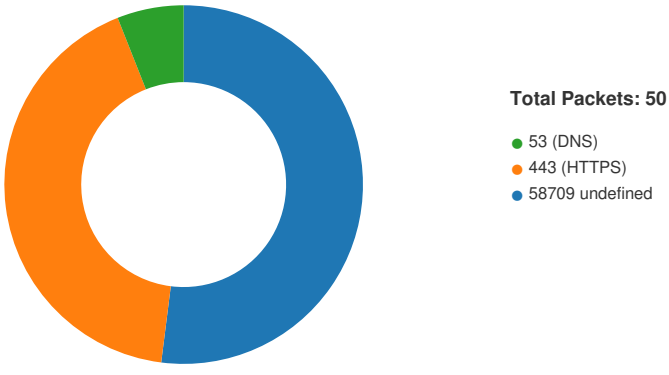
Language of compilation system	Country where language is spoken	Map
Russian	Russia	
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/07/24-01:32:16.104894	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49703	147.45.47.126	192.168.2.6
05/07/24-01:32:30.432420	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49720	147.45.47.126	192.168.2.6
05/07/24-01:32:13.660877	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49699	147.45.47.126	192.168.2.6
05/07/24-01:32:13.858546	TCP	2046267	ET TROJAN [ANY.RUN] RisePro TCP (External IP)	58709	49699	147.45.47.126	192.168.2.6
05/07/24-01:32:16.124524	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49702	147.45.47.126	192.168.2.6
05/07/24-01:32:13.477244	TCP	2049060	ET TROJAN RisePro TCP Heartbeat Packet	49699	58709	192.168.2.6	147.45.47.126
05/07/24-01:32:19.524067	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49699	58709	192.168.2.6	147.45.47.126
05/07/24-01:32:39.555621	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49724	147.45.47.126	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2024 01:32:13.278567076 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:13.469449043 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:13.469577074 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:13.477243900 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:13.660876989 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:13.667802095 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:13.667845964 CEST	49699	58709	192.168.2.6	147.45.47.126

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2024 01:32:13.783052921 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:13.858546019 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:13.907537937 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:14.020678043 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:14.139029026 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.139059067 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.139132977 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.142656088 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.142673969 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.329277992 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.329396009 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.333462000 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.333468914 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.334161997 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.376305103 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.421844959 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.468121052 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.540182114 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.540312052 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.540374994 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.542649031 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.542665005 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.542674065 CEST	49700	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:14.542680025 CEST	443	49700	34.117.186.192	192.168.2.6
May 7, 2024 01:32:14.632894993 CEST	49701	443	192.168.2.6	104.26.4.15
May 7, 2024 01:32:14.632950068 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:14.633013964 CEST	49701	443	192.168.2.6	104.26.4.15
May 7, 2024 01:32:14.633465052 CEST	49701	443	192.168.2.6	104.26.4.15
May 7, 2024 01:32:14.633486032 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:14.817739010 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:14.817826986 CEST	49701	443	192.168.2.6	104.26.4.15
May 7, 2024 01:32:14.820949078 CEST	49701	443	192.168.2.6	104.26.4.15
May 7, 2024 01:32:14.820969105 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:14.821257114 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:14.822922945 CEST	49701	443	192.168.2.6	104.26.4.15
May 7, 2024 01:32:14.864126921 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:15.073194981 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:15.073291063 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:15.073404074 CEST	49701	443	192.168.2.6	104.26.4.15
May 7, 2024 01:32:15.075107098 CEST	49701	443	192.168.2.6	104.26.4.15
May 7, 2024 01:32:15.075129032 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:15.075156927 CEST	49701	443	192.168.2.6	104.26.4.15
May 7, 2024 01:32:15.075164080 CEST	443	49701	104.26.4.15	192.168.2.6
May 7, 2024 01:32:15.075567961 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.303148031 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.315984011 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.526426077 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.532722950 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.723454952 CEST	49702	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.724183083 CEST	49703	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.733865023 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.733885050 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.733897924 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.733911037 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.733928919 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.733941078 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.733961105 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.733983040 CEST	58709	49699	147.45.47.126	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2024 01:32:15.733995914 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.734019995 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.734021902 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.734035015 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.734064102 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.734191895 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.913988113 CEST	58709	49702	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.914170027 CEST	49702	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.914343119 CEST	58709	49703	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.914413929 CEST	49703	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.924654007 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.924668074 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.924679041 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.924695015 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.924706936 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.924717903 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:15.924746037 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.924808025 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.930231094 CEST	49703	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.931149960 CEST	49702	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:15.970340967 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:16.104893923 CEST	58709	49703	147.45.47.126	192.168.2.6
May 7, 2024 01:32:16.124524117 CEST	58709	49702	147.45.47.126	192.168.2.6
May 7, 2024 01:32:16.157565117 CEST	49703	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:16.162386894 CEST	58709	49703	147.45.47.126	192.168.2.6
May 7, 2024 01:32:16.165083885 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:16.173194885 CEST	49702	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:16.188956976 CEST	49699	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:16.347762108 CEST	58709	49703	147.45.47.126	192.168.2.6
May 7, 2024 01:32:16.363729000 CEST	58709	49702	147.45.47.126	192.168.2.6
May 7, 2024 01:32:16.386547089 CEST	58709	49699	147.45.47.126	192.168.2.6
May 7, 2024 01:32:16.391907930 CEST	49703	58709	192.168.2.6	147.45.47.126
May 7, 2024 01:32:16.399765015 CEST	49704	443	192.168.2.6	34.117.186.192
May 7, 2024 01:32:16.399806023 CEST	443	49704	34.117.186.192	192.168.2.6
May 7, 2024 01:32:16.399882078 CEST	49704	443	192.168.2.6	34.117.186.192

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2024 01:32:14.047110081 CEST	57165	53	192.168.2.6	1.1.1.1
May 7, 2024 01:32:14.132601976 CEST	53	57165	1.1.1.1	192.168.2.6
May 7, 2024 01:32:14.544753075 CEST	55608	53	192.168.2.6	1.1.1.1
May 7, 2024 01:32:14.631848097 CEST	53	55608	1.1.1.1	192.168.2.6
May 7, 2024 01:32:40.073369980 CEST	64982	53	192.168.2.6	1.1.1.1
May 7, 2024 01:32:40.159960032 CEST	53	64982	1.1.1.1	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 7, 2024 01:32:14.047110081 CEST	192.168.2.6	1.1.1.1	0xee9b	Standard query (0)	ipinfo.io	A (IP address)	IN (0x0001)	false
May 7, 2024 01:32:14.544753075 CEST	192.168.2.6	1.1.1.1	0x3800	Standard query (0)	db-ip.com	A (IP address)	IN (0x0001)	false
May 7, 2024 01:32:40.073369980 CEST	192.168.2.6	1.1.1.1	0x7a90	Standard query (0)	ipinfo.io	A (IP address)	IN (0x0001)	false

DNS Answers

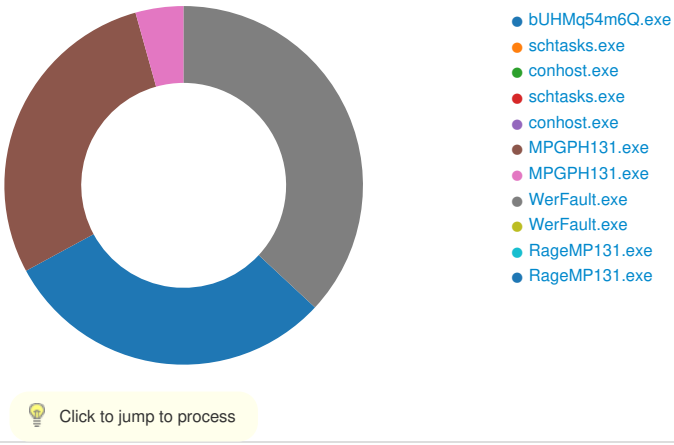
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 7, 2024 01:32:14.132601976 CEST	1.1.1.1	192.168.2.6	0xee9b	No error (0)	ipinfo.io		34.117.186.192	A (IP address)	IN (0x0001)	false
May 7, 2024 01:32:14.631848097 CEST	1.1.1.1	192.168.2.6	0x3800	No error (0)	db-ip.com		104.26.4.15	A (IP address)	IN (0x0001)	false
May 7, 2024 01:32:14.631848097 CEST	1.1.1.1	192.168.2.6	0x3800	No error (0)	db-ip.com		104.26.5.15	A (IP address)	IN (0x0001)	false
May 7, 2024 01:32:14.631848097 CEST	1.1.1.1	192.168.2.6	0x3800	No error (0)	db-ip.com		172.67.75.166	A (IP address)	IN (0x0001)	false
May 7, 2024 01:32:40.159960032 CEST	1.1.1.1	192.168.2.6	0x7a90	No error (0)	ipinfo.io		34.117.186.192	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- https:
  - ipinfo.io
- db-ip.com

Statistics

Behavior



System Behavior

Analysis Process: bUHMq54m6Q.exe PID: **6556**, Parent PID: **4004**

General

Target ID:	0
Start time:	01:32:10
Start date:	07/05/2024
Path:	C:\Users\user\Desktop\bUHMq54m6Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\bUHMq54m6Q.exe"
Imagebase:	0x510000

File size:	2'298'896 bytes
MD5 hash:	2CF4B5CF327757376E717AB5554B921B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000003.2159759925.0000000005C56000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000002.2276746268.000000000122E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000002.2280792333.0000000005C5F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000002.2280715188.0000000005C30000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

Registry Activities

Analysis Process: schtasks.exe PID: 3560, Parent PID: 6556

General

Target ID:	2
Start time:	01:32:12
Start date:	07/05/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /RU "user" /tr "C:\ProgramData\MPGPH131\MPGPH131.exe" /tn "MPGPH131 HR" /sc HOURLY /rl HIGHEST
Imagebase:	0x1e0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 3200, Parent PID: 3560

General

Target ID:	3
Start time:	01:32:12
Start date:	07/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff66e660000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: schtasks.exe PID: **5412**, Parent PID: **6556**

General	
Target ID:	4
Start time:	01:32:12
Start date:	07/05/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /RU "user" /tr "C:\ProgramData\MPGPH131\MPGPH131.exe" /tn "MPGPH131 LG" /sc ONLOGON /rl HIGHEST
Imagebase:	0x1e0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4412**, Parent PID: **5412**

General	
Target ID:	5
Start time:	01:32:12
Start date:	07/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff66e660000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: MPGPH131.exe PID: **4896**, Parent PID: **1064**

General	
Target ID:	6
Start time:	01:32:12
Start date:	07/05/2024
Path:	C:\ProgramData\MPGPH131\MPGPH131.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\MPGPH131\MPGPH131.exe
Imagebase:	0xf00000
File size:	2'298'896 bytes
MD5 hash:	2CF4B5CF327757376E717AB5554B921B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000006.00000002.2282419782.0000000005A70000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 47%, ReversingLabs
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F5A4D7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F5A4FD	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Ei8DrAmaYu9Ksignons.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\8ghN89CsjOW1signons.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD6CA7	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\IuMVYmRLxIIELogin Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\1oBLao5WFReeLogin Data For Account	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\KsIfLLPbfavZWeb Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\TQL0dLOETHSsHistory	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\e0WJiscSE76mWeb Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Dy_2BSqOm3HvCookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\GoTBCXWsNltoCookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\djGL4gOVacKhHistory	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uH4Klb1syK8iWeb Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\W4StvYRvRm8RLogin Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Eoy10p_mBubgLogin Data For Account	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\z81g9YDMLrJHWeb Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uyAd3P89yfWTHistory	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Bs1Rik95T3UPWeb Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\NUYRN8kYshuRCookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\SrMOR5IqDZZTCookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\F27iDkUSbUX4History	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\vCcKyxUjjGyAWeb Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\passwords.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F429AF	CreateFileW
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F429AF	CreateFileW
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	FE6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Cookies\Chrome_Default.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F429AF	CreateFileW
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Autofill	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	FE6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\FTP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0BA0A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\FTP\FileZilla	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0BAD4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Downloads	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	FE6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\FTP\TotalCommander	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0BD0A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Games	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0C0CE	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Games\Growtopia	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0C198	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Games\Minecraft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0C577	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Games\TLauncher	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0D29C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Games\FeatherClient	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0D6FA	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Games\LunarClient	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0DAD9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Games\Battle.net	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0DF3E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Games\Steam	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0E6FC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Messengers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0F45D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Messengers\Skype	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0F527	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Messengers\Element	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0F935	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Messengers\ICQ	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0FC57	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Messengers\Signal	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0FEF3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Messengers\Tox	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F10F14	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Messengers\Pidgin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F11906	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\VPN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F11E70	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\VPN\OpenVPN Connect	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F11FC0	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Plugins	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F5E1C4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Wallets	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F5E908	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\CC	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	FE6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\GoogleAccounts	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F65C36	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F429AF	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Ei8DrAmaYu9Ksignons.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\8ghN89CsjOW1signons.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\luMVYmRLxIIELogin Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\1oBLao5WFReeLogin Data For Account	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\KsIfLLPbfavZWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\TQL0dLOETHSsHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\e0WJiscSE76mWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Dy_2BSqOm3HvCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\GoTBCXWsNltoCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\djGL4gOVacKhHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uH4Klb1syK8iWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\W4StvYRvRm8RLogin Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Eoy10p_mBubgLogin Data For Account	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\z81g9YDMLrJHWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uyAd3P89yfWTHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Bs1Rik95T3UPWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\NUYRN8kYshuRCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\SrMOR5lqDZZTCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\F27iDkUSbUX4History	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\vCcKyxUjjGyAWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip	success or wait	1	FC7071	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rage131MP.tmp	0	13	31 37 31 35 30 34 34 35 30 38 30 31 33	1715044508013	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	0	524288	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 02 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 26 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 0d 7f fd 00 2d 61 3e 00 7e fd 7f fd 7c 30 7b 64 7a fd 7a fd 7a 22 79 fd 79 33 78 fd 78 4b 77 fd 76 fd 75 fd 75 47 74 fd 74 3b 73 41 73 fd 71 fd 70 fd 71 fd 70 7b 6f fd 6f 68 6e fd 6e 65 6d fd 6e 2c 6d 39 6c fd 6b fd 6c 50 6a fd 6a 01 68 fd 68 1f 67 fd 64 fd 63 fd 63 36 62 17 62 fd 61 fd 61 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAsqpqp{ooh nnemn,m9lklPjjhhgdcc6bbaa>	success or wait	10	FD6CA7	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j}}	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite	0	524288	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 02 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 26 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 0d 7f fd 00 2d 61 3e 00 7e fd 7f fd 7c 30 7b 64 7a fd 7a fd 7a 22 79 fd 79 33 78 fd 78 4b 77 fd 76 fd 75 fd 75 47 74 fd 74 3b 73 41 73 fd 71 fd 70 fd 71 fd 70 7b 6f fd 6f 68 6e fd 6e 65 6d fd 6e 2c 6d 39 6c fd 6b fd 6c 50 6a fd 6a 01 68 fd 68 1f 67 fd 64 fd 63 fd 63 36 62 17 62 fd 61 fd 61 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAs qpqp{ooh nnemn,m9lklPjjhhgdcc6b baa>	success or wait	10	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\luMVYmRLxIIELogin Data	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\1oBLao5WFReeLogin Data For Account	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\KsIfLLPbfavZWeb Data	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\TQL0dLOETHSsHistory	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ' .j	success or wait	2	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\e0WJiscSE76mWeb Data	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\GoTBCXWsNltoCookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 06 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 06 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\djGL4gOVacKhHistory	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ' .j	success or wait	2	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uH4Klb1syK8iWeb Data	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\W4StvYRvRm8RLogin Data	0	51200	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 02 00 2e 6a fd 05 00 00 00 02 07 fd 00 00 00 00 18 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\z81g9YDMLrJHWeb Data	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 08 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 37 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 08 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y7.jW	success or wait	2	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uyAd3P89yfWTHistory	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 26 00 00 00 00 00 00 00 00 00 00 00 1f 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ &.j	success or wait	2	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Bs1Rik95T3UPWeb Data	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 08 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 37 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 08 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y7.jW	success or wait	2	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\SrMOR5IqDZZTCookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 07 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 07 00 2e 6a fd 0d 0d 24 00 04 0a 0c 00 0f 67 0f fd 0a 0c 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j$g	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\F27iDkUSbUX4History	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 26 00 00 00 00 00 00 00 00 00 00 00 1f 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ &.j	success or wait	2	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\vCcKyxUjjGyAWeb Data	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 08 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 37 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 08 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y7.jW	success or wait	2	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Cookies\Chrome_Default.txt	0	530	2e 67 6f 6f 67 6c 65 2e 63 6f 6d 09 54 52 55 45 09 2f 09 54 52 55 45 09 31 37 31 32 32 39 38 30 30 32 09 4e 49 44 09 45 4e 43 38 39 33 2a 5f 64 6a 45 77 78 36 43 4c 6b 58 4c 67 38 41 75 53 5a 57 43 67 79 6c 6d 41 73 4d 4e 6e 64 31 4c 53 66 62 63 4c 2b 49 66 43 67 4d 76 58 2f 6d 35 49 72 7a 64 53 77 78 74 36 58 36 6e 35 53 36 43 37 77 43 6f 55 6f 57 76 75 69 78 5a 70 7a 72 4d 69 7a 47 5a 63 35 6f 68 49 70 6d 73 76 6c 4f 72 47 54 4f 68 46 6b 51 34 2b 6c 43 46 36 66 56 48 30 51 4e 50 42 42 62 32 37 6f 32 6e 58 4d 38 65 6d 37 45 41 59 53 31 62 59 5a 43 32 4c 56 30 34 53 71 70 67 79 78 4a 6d 64 66 46 41 37 55 79 57 55 6f 4b 38 6b 46 5a 51 44 52 6c 30 76 64 4f 7a 57 64 76 41 6f 75 6d 77 32 73 6b 75 43 43 74 4a 43 32 6f 47 33 7a 33 4f 59 62 4c 54 4c 44 62 4d 37	.google.comTRUE/TRUE1712298002NIDENC893*_djEwx6CLkXLg8AuSZWCgylmAsMNnd1LSfbcL+IfCgMvX/m5IrzdSwxt6X6n5S6C7wCoUoWvuixZpzrMizGZc5ohIpmsvlOrGTOhFkQ4+lCF6fVH0QNPBBb27o2nXM8em7EAYS1bYZC2LV04SqpgyxJmdfFA7UyWUoK8kFZQDRl0vdOzWdvAoumw2skuCCtJC2oG3z3OYbLTLDbM7	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\passwords.txt	0	4096	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\passwords.txt	4096	801	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd		success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt	0	4096	42 75 69 6c 64 3a 20 63 6f 6d 62 6f 0d 0a 56 65 72 73 69 6f 6e 3a 20 32 2e 30 0d 0a 0d 0a 44 61 74 65 3a 20 54 75 65 20 4d 61 79 20 20 37 20 30 31 3a 33 32 3a 32 30 20 32 30 32 34 0a 4d 61 63 68 69 6e 65 49 44 3a 20 39 65 31 34 36 62 65 39 2d 63 37 36 61 2d 34 37 32 30 2d 62 63 64 62 2d 35 33 30 31 31 62 38 37 62 64 30 36 0d 0a 47 55 49 44 3a 20 7b 61 33 33 63 37 33 34 30 2d 36 31 63 61 2d 31 31 65 65 2d 38 63 31 38 2d 38 30 36 65 36 66 36 65 36 39 36 33 7d 0d 0a 48 57 49 44 3a 20 39 30 34 37 35 32 65 39 34 33 37 64 61 33 62 66 66 66 38 37 30 64 30 39 62 62 35 35 37 32 62 32 0d 0a 0d 0a 50 61 74 68 3a 20 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 4d 50 47 50 48 31 33 31 5c 4d 50 47 50 48 31 33 31 2e 65 78 65 0d 0a 57 6f 72 6b 20 44 69 72 3a 20 43 3a 5c	Build: comboVersion: 2.0Date: Tue May 7 01:32:20 2024MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}HWID: 904752e9437da3bfff870d09bb5572b2Path: C:\ProgramData\MPGPH131\MPGPH131.exeWork Dir: C:\	success or wait	1	F49914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt	4096	2667	79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 31 34 32 38 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 39 30 34 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 39 32 38 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 39 38 30 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 37 37 36 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 37 38 38 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 34 39 30 30 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d	yLnLovZsnAh.exe [1428]KWOadjiLmvQUByLnLovZsnAh.exe [5904]KWOadjiLmvQUByLnLovZsnAh.exe [5928]KWOadjiLmvQUByLnLovZsnAh.exe [5980]KWOadjiLmvQUByLnLovZsnAh.exe [5776]KWOadjiLmvQUByLnLovZsnAh.exe [5788]KWOadjiLmvQUByLnLovZsnAh.exe [4900]KWOadjiLm	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt	0	4096	42 75 69 6c 64 3a 20 63 6f 6d 62 6f 0d 0a 56 65 72 73 69 6f 6e 3a 20 32 2e 30 0d 0a 0d 0a 44 61 74 65 3a 20 54 75 65 20 4d 61 79 20 20 37 20 30 31 3a 33 32 3a 32 30 20 32 30 32 34 0a 4d 61 63 68 69 6e 65 49 44 3a 20 39 65 31 34 36 62 65 39 2d 63 37 36 61 2d 34 37 32 30 2d 62 63 64 62 2d 35 33 30 31 31 62 38 37 62 64 30 36 0d 0a 47 55 49 44 3a 20 7b 61 33 33 63 37 33 34 30 2d 36 31 63 61 2d 31 31 65 65 2d 38 63 31 38 2d 38 30 36 65 36 66 36 65 36 39 36 33 7d 0d 0a 48 57 49 44 3a 20 39 30 34 37 35 32 65 39 34 33 37 64 61 33 62 66 66 66 38 37 30 64 30 39 62 62 35 35 37 32 62 32 0d 0a 0d 0a 50 61 74 68 3a 20 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 4d 50 47 50 48 31 33 31 5c 4d 50 47 50 48 31 33 31 2e 65 78 65 0d 0a 57 6f 72 6b 20 44 69 72 3a 20 43 3a 5c	Build: comboVersion: 2.0Date: Tue May 7 01:32:20 2024MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}HWID: 904752e9437da3bfff870d09bb5572b2Path: C:\ProgramData\MPGPH131\MPGPH131.exeWork Dir: C:\	success or wait	1	F49914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt	4096	2667	79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 31 34 32 38 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 39 30 34 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 39 32 38 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 39 38 30 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 37 37 36 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 35 37 38 38 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d 76 51 55 42 79 4c 6e 4c 6f 76 5a 73 6e 41 68 2e 65 78 65 20 5b 34 39 30 30 5d 0d 0a 4b 57 4f 61 64 6a 69 4c 6d	yLnLovZsnAh.exe [1428]KWOadjiLmvQUByLnLovZsnAh.exe [5904]KWOadjiLmvQUByLnLovZsnAh.exe [5928]KWOadjiLmvQUByLnLovZsnAh.exe [5980]KWOadjiLmvQUByLnLovZsnAh.exe [5776]KWOadjiLmvQUByLnLovZsnAh.exe [5788]KWOadjiLmvQUByLnLovZsnAh.exe [4900]KWOadjiLm	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip	0	40	50 4b 03 04 14 00 00 08 08 00 0a 0c fd 58 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 43 6f 6f 6b 69 65 73 5c 03 00	PKXCookies\	success or wait	4	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip	14	12	00 00 00 00 02 00 00 00 00 00 00 00		success or wait	4	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip	2546	314	50 4b 01 02 00 0b 14 00 00 08 08 00 0a 0c fd 58 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 6f 6f 6b 69 65 73 5c 50 4b 01 02 00 0b 14 00 00 08 08 00 0a 0c fd 58 41 fd 60 25 fd 01 00 00 12 02 00 00 1a 00 00 00 00 00 00 00 01 00 00 00 00 00 28 00 00 00 43 6f 6f 6b 69 65 73 5c 43 68 72 6f 6d 65 5f 44 65 66 61 75 6c 74 2e 74 78 74 50 4b 01 02 00 0b 14 00 00 08 08 00 0a 0c fd 58 6a fd 64 fd fd 06 00 00 6b 1a 00 00 0f 00 00 00 00 00 00 00 01 00 00 00 00 00 fd 01 00 00 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 74 78 74 50 4b 01 02 00 0b 14 00 00 08 08 00 0a 0c fd 58 fd 46 fd fd 01 01 00 00 21 13 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 00 00 fd 08 00 00 70 61 73 73 77 6f 72 64 73 2e 74 78 74 50 4b 05 06 00 00 00 00 04	PKXCookies\PKXA`%(Cookies\Chrome_Default.txtPKXjdkinformation.txtPKXF!passwords.txtPK	success or wait	1	F49914	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\MPGPH131\MPGPH131.exe	0	1998848	success or wait	1	F48BE4	ReadFile
C:\ProgramData\MPGPH131\MPGPH131.exe	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Ei8DrAmaYu9Ksignons.sqlite	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\8ghN89CsjOW1signons.sqlite	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	0	100	success or wait	1	1045968	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	0	16	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\luMVYmRLxIIELogin Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\luMVYmRLxIIELogin Data	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\1oBLao5WFReeLogin Data For Account	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\1oBLao5WFReeLogin Data For Account	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\KsIfLLPbfavZWeb Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\KsIfLLPbfavZWeb Data	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\TQL0dLOETHSsHistory	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\TQL0dLOETHSsHistory	0	4096	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\TQL0dLOETHSsHistory	0	4096	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\e0WJiscSE76mWeb Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\e0WJiscSE76mWeb Data	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Dy_2BSqOm3HvCookies	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\GoTBCXWsNltoCookies	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\GoTBCXWsNltoCookies	0	4096	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\djGL4gOVacKhHistory	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\djGL4gOVacKhHistory	0	4096	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uH4Klb1syK8iWeb Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	40960	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\W4StvYRvRm8RLogin Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	40960	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	40960	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Eoy10p_mBubgLogin Data For Account	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\z81g9YDMLrJHWeb Data	0	100	success or wait	1	1045968	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\uyAd3P89yfWTHistory	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	40960	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Bs1Rik95T3UPWeb Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Bs1Rik95T3UPWeb Data	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	40960	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	40960	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\NUYRN8kYshuRCookies	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	40960	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\SrMOR5lqDZZTCookies	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\F27iDkUSbUX4History	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	40960	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\vCcKyxUjjGyAWeb Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\vCcKyxUjjGyAWeb Data	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	40960	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Cookies\Chrome_Default.txt	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\Cookies\Chrome_Default.txt	0	4096	end of file	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt	0	4096	success or wait	2	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\information.txt	0	4096	end of file	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\passwords.txt	0	4096	success or wait	2	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs\passwords.txt	0	4096	end of file	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\NoSoV6eJxRbhlNXMC2XnYgm.zip	0	4096	success or wait	1	F48BE4	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: MPGPH131.exe PID: **2836**, Parent PID: **1064**

General

Target ID:	7
Start time:	01:32:13
Start date:	07/05/2024
Path:	C:\ProgramData\MPGPH131\MPGPH131.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\MPGPH131\MPGPH131.exe
Imagebase:	0xf00000
File size:	2'298'896 bytes
MD5 hash:	2CF4B5CF327757376E717AB5554B921B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyuNssG0kGarHs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F5A4D7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F5A4FD	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Ei8DrAmaYu9Ksignons.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\8ghN89CsjOW1signons.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	FD69A6	CopyFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Ei8DrAmaYu9Ksignons.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\8ghN89CsjOW1signons.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	success or wait	1	F4B9DE	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rage131MP.tmp	0	13	31 37 31 35 30 34 34 35 30 38 30 31 33	1715044508013	success or wait	1	F49914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	0	524288	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 02 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 26 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 0d 7f fd 00 2d 61 3e 00 7e fd 7f fd 7c 30 7b 64 7a fd 7a fd 7a 22 79 fd 79 33 78 fd 78 4b 77 fd 76 fd 75 fd 75 47 74 fd 74 3b 73 41 73 fd 71 fd 70 fd 71 fd 70 7b 6f fd 6f 68 6e fd 6e 65 6d fd 6e 2c 6d 39 6c fd 6b fd 6c 50 6a fd 6a 01 68 fd 68 1f 67 fd 64 fd 63 fd 63 36 62 17 62 fd 61 fd 61 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .&K.j-a>~|0{dzzz"yy3xxKwvuuGtt;sAsqpqp{oohnnemn,m9lklPjjhhgdcc6bbaa>	success or wait	10	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j}}	success or wait	1	FD69A6	CopyFileA

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite</td><td>0</td><td>524288</td><td>53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 02 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 26 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 0d 7f fd 00 2d 61 3e 00 7e fd 7f fd 7c 30 7b 64 7a fd 7a fd 7a 22 79 fd 79 33 78 fd 78 4b 77 fd 76 fd 75 fd 75 47 74 fd 74 3b 73 41 73 fd 71 fd 70 fd 71 fd 70 7b 6f fd 6f 68 6e fd 6e 65 6d fd 6e 2c 6d 39 6c fd 6b fd 6c 50 6a fd 6a 01 68 fd 68 1f 67 fd 64 fd 63 fd 63 36 62 17 62 fd 61 fd 61 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>SQLite format 3@ .&K.j-a>~|0{dzzz"yy3xxKwvuuGtt;sAsqpqp{oohnnemn,m9lklPjjhhgdcc6bbaa></td><td>success or wait</td><td>10</td><td>FD69A6</td><td>CopyFileA</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\MPGPH131\MPGPH131.exe	0	1998848	success or wait	1	F48BE4	ReadFile
C:\ProgramData\MPGPH131\MPGPH131.exe	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\Ei8DrAmaYu9Ksignons.sqlite	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\8ghN89CsjOW1signons.sqlite	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\D87fZN3R3jFeplaces.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\02zdBXl47cvzcookies.sqlite	0	16	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\spanuNssG0kGarHs\3b6N2Xdh3CYwplaces.sqlite	0	16	success or wait	1	1045968	ReadFile

Analysis Process: WerFault.exe

PID: **1836**, Parent PID: **6556**

General

Target ID:	10
Start time:	01:32:21
Start date:	07/05/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6556 -s 1888
Imagebase:	0x970000
File size:	483'680 bytes
MD5 hash:	C31336C1EFC2CCB44B4326EA793040F2
Has elevated privileges:	true

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\3e5f863b-f117-4412-96b2-5ca580be5846	delete | generic read | generic write	device	delete on close	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\c5f97f31-b48a-4bd6-9736-b5eff0de2748	delete | generic read | generic write	device	delete on close	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\811ef8a0-c1ec-4a3d-b4c1-b1076f54e2e9	delete | generic read | generic write	device	delete on close	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\fbeddbca-a215-40e0-b998-2d08ae692e26	delete | generic read | generic write	device	delete on close	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3245.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3245.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\d887ac29-8cd1-4b63-b1ef-2d8cde99167e	delete | generic read | generic write	device	delete on close	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bUHMq54m6Q.exe_7f5678ff3d44ce164b9187a831663245298324_7fe652d7_b9d6888b-1509-4a56-aeb6-1b74ada72881	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bUHMq54m6Q.exe_7f5678ff3d44ce164b9187a831663245298324_7fe652d7_b9d6888b-1509-4a56-aeb6-1b74ada72881\ed909821-f24f-40c5-bb08-657de0a62401	delete | generic read | generic write	device	delete on close	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bUHMq54m6Q.exe_7f5678ff3d44ce164b9187a831663245298324_7fe652d7_b9d6888b-1509-4a56-aeb6-1b74ada72881\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C806C4D	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 68 39 66 fd 05 12 00 00 00 00 00	MDMPa h9f	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	9904	6	00 00 00 00 00 00		success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	212	1420	00 00 06 00 08 fd 04 01 0a 00 00 00 00 00 00 00 65 4a 00 00 02 00 00 00 fd 26 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c fd 06 08 00 fd fd fd 0f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 19 00 00 7a 68 39 66 00 00 00 00 01 00 00 00 fd 07 00 00 fd 07 00 00 fd 07 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 75 00 6d 00 6d 00 65 00 72 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	eJ&GenuineIntelTzh9f02 W. Europe Standard TimeW. Europe Summer Time	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	11882	716	7f 00 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 65 23 01 02 00 00 00 00 00 00 00 60 39 43 77 38 fd fd 00 08 fd fd 00 18 fd fd 00 fd 70 3f 77 23 00 00 00 46 02 00 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++e#`9Cw8p?w#F+	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	1632	168	fd 16 00 00 00 00 00 00 74 03 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 fd 70 3f 77 00 00 00 00 01 00 00 00 00 00 00 00 60 39 43 77 00 00 00 00 fd 01 00 00 00 00 00 00 2c fd 22 01 00 00 00 00 11 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 00 00 00 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 11 00 00 00 00 00 00 00 40 fd fd 00 00 00 00 00 38 42 23 01 00 00 00 00 fd fd fd 00 00 00 00 00 00 fd 38 77 00 00 00 00 fd 2c fd 02 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 02 00 00 6a 2e 00 00	tp?w`9Cw,"@8B#8w,j.	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	20474	20	2d 00 00 00 00 fd fd 00 00 00 00 00 fd 04 00 00 fd 52 00 00	-R	success or wait	45	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	21198	1192	00 00 00 04 fd fd fd fd 00 00 51 00 fd 5d 43 77 fd 0a 22 01 00 00 00 00 00 00 22 01 40 5b 43 77 00 00 00 00 00 00 00 00 00 00 00 00 70 13 fd 76 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 30 5d 43 77 fd fd fd fd 03 00 00 00 00 00 fd 7f 00 00 00 00 50 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 03 00 00 00 10 00 00 00 40 48 43 77 00 00 00 00 00 00 00 00 00 00 00 00 fd 33 43 77 0a 00 00 00 00 00 00 00 65 4a 00 00 02 00 00 00 02 00 00 00 06 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Q]Cw""@[Cwpv0]CwP(Pm @HCw3CweJ	success or wait	44	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	90342	256	fd 74 2d 51 68 44 3b 33 77 6a 00 6a 65 fd 5b fd fd fd fd fd 10 fd 7d 08 00 74 15 fd 65 fd 00 fd fd 07 33 fd 40 cb 65 fd fd 45 fd fd fd fd fd fd 45 fd fd 45 fd 33 fd 40 fd 45 fd fd 65 fd 00 fd 45 fd 0c 39 77 fd 45 fd fd 45 fd fd 45 fd fd 4d fd fd 12 00 00 00 fd 4d fd 64 fd 0d 00 00 00 00 59 5f 5e 5b fd fd 04 00 6a 18 68 fd fd 41 77 fd 0d fd fd fd 65 fd 00 51 fd 2d 1c fd fd fd 33 fd 4d fd 01 fd 00 fd 45 09 4d fd 45 fd 6a 00 fd 45 fd fd 70 04 fd 45 fd fd 30 fd 38 fd fd fd 75 fd 6a fd fd 7f fd fd fd 33 fd 40 cb 65 fd fd 45 fd fd fd fd fd fd 4d fd 64 fd 0d 00 00 00 00 59 5f 5e 5b fd cd fd 00 fd fd fd 56 fd fd fd 12 77 0b fd fd fd fd fd fd fd fd 14 76 14 fd 00 00 00 fd fd 74 0f fd fd 58 fd fd fd fd fd 1a 77 04 fd 01 5e fd 32 fd	t-QhD;3wjje[}te3@eEEE3@EeE9wEEEMMdY_^[jhAweQ-3MEMEjEpE08uj3@eEMdY_^[VwvtXw^2	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	1800	4	0b 00 00 00		success or wait	11	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	12598	716	3f 00 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 60 39 43 77 38 fd fd 00 00 00 00 00 fd fd fd 00 4c 30 38 77 23 00 00 00 06 02 00 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++`9Cw8L08w#+	success or wait	11	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	2284	48	7c 0c 00 00 01 00 00 00 00 fd 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd fd 05 00 00 00 00 04 0a 00 00 2e 22 01 00 fd 02 00 00 2e 4d 00 00	|.".M	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	2344	4	3f 00 00 00	?	success or wait	63	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	9910	34	1c 00 00 00 62 00 55 00 48 00 4d 00 71 00 35 00 34 00 6d 00 36 00 51 00 2e 00 65 00 78 00 65 00 00 00	bUHMq54m6Q.exe	success or wait	63	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	9044	120	00 00 30 77 00 00 00 00 00 fd 00 00 fd fd 00 00 fd cb 37 fd 2d 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 fd 02 61 4a 00 00 0a 00 fd 02 61 4a 3f 00 00 00 00 00 00 00 04 00 04 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 04 00 00 00	0w7-aJaJ?	success or wait	4	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	11708	54	30 00 00 00 72 00 65 00 73 00 6f 00 75 00 72 00 63 00 65 00 70 00 6f 00 6c 00 69 00 63 00 79 00 63 00 6c 00 69 00 65 00 6e 00 74 00 2e 00 64 00 6c 00 6c 00 00 00	0resourcepolicyclient.dll	success or wait	4	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	9236	668	00 00 fd 6e 00 00 00 00 00 fd 0d 00 fd 58 0e 00 fd 6b 07 fd 4c 2e 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 0d fd 0f 00 02 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 55 05 00 00 00 00 00 fd fd 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 00 00 00 00 fd 27 06 00 00 00 00 00 40 fd 1f 00 00 00 00 00 18 fd 06 00 00 00 00 00 72 fd fd fd 00 00 00 00 62 fd 61 27 00 00 00 00 20 68 52 20 00 00 00 00 fd 30 fd 00 00 00 00 00 fd 7e 01 00 fd fd 01 00 0f fd 05 00 fd 35 09 00 fd 27 06 00 0d fd 1f 00 18 fd 06 00 7e fd 39 00 26 2f 01 00 fd 36 13 00 00 00 00 00 fd 42 23 00 6e fd 06	nXkL.ZbpU'@rba' hR 0~5'~9&/6B#n	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	90598	30882	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 00 00 00 00 01 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49	EventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketI	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC2.tmp.dmp	32	120	03 00 00 00 14 02 00 00 08 07 00 00 04 00 00 00 fd 1a 00 00 28 09 00 00 0e 00 00 00 6c 00 00 00 fd 23 00 00 05 00 00 00 fd 02 00 00 fd 4f 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 48 4a 00 00 40 fd 01 00 15 00 00 00 fd 01 00 00 2c 24 00 00 16 00 00 00 fd 00 00 00 18 26 00 00	(I#O`8THJ@,$&	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 39 00 30 00 34 00 35 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>19045</Build>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	478	138	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 39 00 30 00 34 00 31 00 2e 00 32 00 30 00 30 00 36 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 76 00 62 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 39 00 31 00 32 00 30 00 36 00 2d 00 31 00 34 00 30 00 36 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>19041.2006.amd64fre.vb_release.191206-1406</BuildString>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	624	50	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 32 00 30 00 30 00 36 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>2006</Revision>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	682	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>MultiprocessorFree</Flavor>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	762	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	834	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 32 00 30 00 35 00 37 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>2057</LCID>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	874	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	926	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6556</Pid>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1012	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 55 00 48 00 4d 00 71 00 35 00 34 00 6d 00 36 00 51 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>bUHMq54m6Q.exe</ImageName>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1086	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1090	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1094	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1184	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1188	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1192	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 37 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11770</Uptime>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1236	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1240	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1244	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1326	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1330	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1334	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1386	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1390	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1394	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1438	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1442	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1448	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 39 00 30 00 37 00 32 00 32 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>159072256</PeakVirtualSize>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1536	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1540	2	09 00		success or wait	3	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1546	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 38 00 39 00 38 00 37 00 39 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>148987904</VirtualSize>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1618	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1622	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1628	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 32 00 31 00 30 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>12105</PageFaultCount>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1704	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1708	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1714	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 34 00 36 00 34 00 39 00 37 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>24649728</PeakWorkingSetSize>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1822	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 33 00 37 00 36 00 34 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>22376448</WorkingSetSize>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1904	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1908	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	1914	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 35 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>225520</QuotaPeakPagedPoolUsage>	success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2028	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2032	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2038	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 33 00 30 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>223080</QuotaPagedPoolUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2136	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2140	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2146	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 39 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>89880</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2270	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2274	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2280	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 38 00 38 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>88872</QuotaNonPagedPoolUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2388	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2392	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2398	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 32 00 35 00 36 00 33 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>10256384</PagefileUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2476	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2480	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2486	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 34 00 39 00 36 00 38 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>12496896</PeakPagefileUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2580	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2584	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2590	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 32 00 35 00 36 00 33 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>10256384</PrivateUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2664	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2668	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2672	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2718	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2722	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2726	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2756	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2760	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2766	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2806	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2810	2	09 00		success or wait	4	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2818	30	3c 00 50 00 69 00 64 00 3e 00 34 00 30 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4004</Pid>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2848	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2852	2	09 00		success or wait	4	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2860	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2930	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2934	2	09 00		success or wait	4	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	2942	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3032	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3036	2	09 00		success or wait	4	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3044	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 33 00 36 00 38 00 38 00 32 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6368829</Uptime>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3092	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3096	2	09 00		success or wait	4	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3104	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3182	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3186	2	09 00		success or wait	4	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3194	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3246	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3250	2	09 00		success or wait	4	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3258	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3302	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3306	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3316	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3406	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3410	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3420	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3494	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3498	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3508	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 33 00 31 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>113176</PageFaultCount>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3586	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3590	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3600	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 32 00 30 00 35 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>132055040</PeakWorkingSetSize>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3700	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3704	2	09 00		success or wait	5	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3714	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 39 00 37 00 36 00 31 00 32 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>129761280</WorkingSetSize>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3798	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3802	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3812	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 31 00 32 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11126632</QuotaPeakPagedPoolUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3928	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3932	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	3942	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 30 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1010056</QuotaPagedPoolUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4042	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4046	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4056	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>87264</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4180	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4184	2	09 00		success or wait	5	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4194	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 33 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>83264</QuotaNonPagedPoolUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4302	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4306	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4316	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 34 00 39 00 34 00 38 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>44494848</PagefileUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4394	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4398	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4408	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 38 00 33 00 34 00 38 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>44834816</PeakPagefileUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4502	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4506	2	09 00		success or wait	5	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4516	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 34 00 39 00 34 00 38 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44494848</PrivateUsage>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4590	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4594	2	09 00		success or wait	4	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4602	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4648	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4652	2	09 00		success or wait	3	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4658	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4700	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4704	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4708	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4746	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4788	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4792	2	09 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4794	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4832	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4836	2	09 00		success or wait	2	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4840	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4902	4	0d 00 0a 00		success or wait	8	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4906	2	09 00		success or wait	16	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	4910	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 62 00 55 00 48 00 4d 00 71 00 35 00 34 00 6d 00 36 00 51 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>bUHMq54m6Q.exe</Parameter0>	success or wait	8	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	5580	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	5584	2	09 00		success or wait	1	6C806C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	5586	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	5626	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	5630	2	09 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	5632	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	5670	4	0d 00 0a 00		success or wait	6	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	5674	2	09 00		success or wait	12	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	5678	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 39 00 30 00 34 00 35 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.19045.2.0.0.256.48</Parameter1>	success or wait	6	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	6232	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	6236	2	09 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	6238	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	6278	4	0d 00 0a 00		success or wait	1	6C806C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3215.tmp.WERInternalMetadata.xml	6282	2	09 00		success or wait	1	6C806C4D	unknown

Analysis Process: WerFault.exe PID: **5088**, Parent PID: **4896**

General

Target ID:	13
Start time:	01:32:24
Start date:	07/05/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4896 -s 1148
Imagebase:	0x970000
File size:	483'680 bytes
MD5 hash:	C31336C1EFC2CCB44B4326EA793040F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: RageMP131.exe PID: **3604**, Parent PID: **4004**

General	
Target ID:	14
Start time:	01:32:25
Start date:	07/05/2024
Path:	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\RageMP131\RageMP131.exe"
Imagebase:	0x360000
File size:	2'298'896 bytes
MD5 hash:	2CF4B5CF327757376E717AB5554B921B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 47%, ReversingLabs
Reputation:	low
Has exited:	true

Analysis Process: RageMP131.exe PID: **5700**, Parent PID: **4004**

General	
Target ID:	18
Start time:	01:32:35
Start date:	07/05/2024
Path:	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\RageMP131\RageMP131.exe"
Imagebase:	0x360000
File size:	2'298'896 bytes
MD5 hash:	2CF4B5CF327757376E717AB5554B921B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Disassembly

No disassembly