ID: 1440164
Sample Name: file.exe
Cookbook: default.jbs
Time: 12:02:08
Date: 12/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

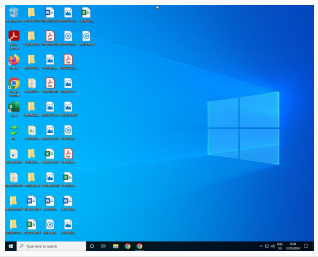
Windows Analysis Report

file.exe

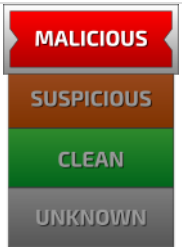
Overview

General Information

Sample name:	file.exe
Analysis ID:	1440164
MD5:	72007357beb7…
SHA1:	e37f50ace578f…
SHA256:	6a1bda6fa37b0..
Tags:	exe RisePro Stealer
Infos:	



Detection



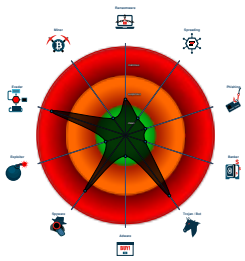
PrivateLoader, RisePro Stealer

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Yara detected PrivateLoader
- 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…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 744 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 72007357BEB74FEA20E7DAA285212B16)
  - schtasks.exe (PID: 1368 cmdline: schtasks /create /f /RU "user" /tr "C:\ProgramData\MPGPH131\MPGPH131.exe" /tn "MPGPH131 HR" /sc HOURLY /rl HIGHEST MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 1704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - schtasks.exe (PID: 3852 cmdline: schtasks /create /f /RU "user" /tr "C:\ProgramData\MPGPH131\MPGPH131.exe" /tn "MPGPH131 LG" /sc ONLOGON /rl HIGHEST MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 6880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - WerFault.exe (PID: 7448 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 744 -s 2028 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- MPGPH131.exe (PID: 1436 cmdline: C:\ProgramData\MPGPH131\MPGPH131.exe MD5: 72007357BEB74FEA20E7DAA285212B16)
  - WerFault.exe (PID: 7564 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1436 -s 1956 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- MPGPH131.exe (PID: 648 cmdline: C:\ProgramData\MPGPH131\MPGPH131.exe MD5: 72007357BEB74FEA20E7DAA285212B16)
  - WerFault.exe (PID: 7584 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 648 -s 1908 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- RageMP131.exe (PID: 7236 cmdline: "C:\Users\user\AppData\Local\RageMP131\RageMP131.exe" MD5: 72007357BEB74FEA20E7DAA285212B16)
- RageMP131.exe (PID: 7768 cmdline: "C:\Users\user\AppData\Local\RageMP131\RageMP131.exe" MD5: 72007357BEB74FEA20E7DAA285212B16)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
PrivateLoader	According to sekoia, PrivateLoader is a modular malware whose main capability is to download and execute one or several payloads. The loader implements anti-analysis techniques, fingerprints the compromised host and reports statistics to its C2 server.	No Attribution	**http://** https://any.run/cybersecurity-blog/crackedcantil-breakdown/https://any.run/cybersecurity-blog/privateloader-analyzing-the-encryption-and-decryption-of-a-modern-loader/https://bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadeyhttps://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.privateloader

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\OGKFocHES6dDgKTCWPSJdQR.zip	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\8klzCUsmQMVYazLTWo6KoKU.zip	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\ZeTvTkc8PqqpWi0gm5JPfdt.zip	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.2026410193.0000000000ABF000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.2017190533.00000000018FE000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000003.00000002.2025872612.00000000009AD000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.MPGPH131.exe.f00000.0.unpack	JoeSecurity_PrivateLoader	Yara detected PrivateLoader	Joe Security	
6.2.MPGPH131.exe.f00000.0.unpack	JoeSecurity_PrivateLoader	Yara detected PrivateLoader	Joe Security	
0.2.file.exe.bb0000.0.unpack	JoeSecurity_PrivateLoader	Yara detected PrivateLoader	Joe Security	
16.2.RageMP131.exe.b80000.0.unpack	JoeSecurity_PrivateLoader	Yara detected PrivateLoader	Joe Security	
7.2.RageMP131.exe.b80000.0.unpack	JoeSecurity_PrivateLoader	Yara detected PrivateLoader	Joe Security	

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: 192.168.2.4

Timestamp:	05/12/24-12:02:58.333893
SID:	2046266
Source Port:	58709
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.4

Timestamp:	05/12/24-12:02:56.237225
SID:	2046266
Source Port:	58709
Destination Port:	49730
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (External IP) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.4

Timestamp:	05/12/24-12:02:57.482973
SID:	2046267
Source Port:	58709
Destination Port:	49730
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (External IP) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.4

Timestamp:	05/12/24-12:02:58.992753
SID:	2046267
Source Port:	58709
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.4

Timestamp:	05/12/24-12:03:17.954872
SID:	2046266
Source Port:	58709
Destination Port:	49751
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.4 - Destination IP: 147.45.47.126

Timestamp:	05/12/24-12:03:05.358724
SID:	2046269
Source Port:	49730
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.4 - Destination IP: 147.45.47.126

Timestamp:	05/12/24-12:03:06.218564
SID:	2046269
Source Port:	49731
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.4 - Destination IP: 147.45.47.126

Timestamp:	05/12/24-12:03:11.796109
SID:	2046269
Source Port:	49739
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.4 - Destination IP: 147.45.47.126

Timestamp:	05/12/24-12:03:08.562034
SID:	2046269
Source Port:	49736
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (External IP) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.4

Timestamp:	05/12/24-12:03:00.933956
SID:	2046267
Source Port:	58709
Destination Port:	49736
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.4

Timestamp:	05/12/24-12:03:07.984400
SID:	2046266
Source Port:	58709
Destination Port:	49739
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.126 - Destination IP: 192.168.2.4

Timestamp:	05/12/24-12:03:00.497224
SID:	2046266
Source Port:	58709
Destination Port:	49736
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN RisePro TCP Heartbeat Packet - Source IP: 192.168.2.4 - Destination IP: 147.45.47.126

Timestamp:	05/12/24-12:02:55.911761
SID:	2049060
Source Port:	49730
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Spreading

Yara detected PrivateLoader

Networking

Snort IDS alert for network traffic

Yara detected PrivateLoader

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

System Summary

PE file has nameless sections

Data Obfuscation

Detected unpacking (changes PE section rights)

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

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

Contains functionality to inject threads in other processes

Stealing of Sensitive Information

Yara detected PrivateLoader

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)

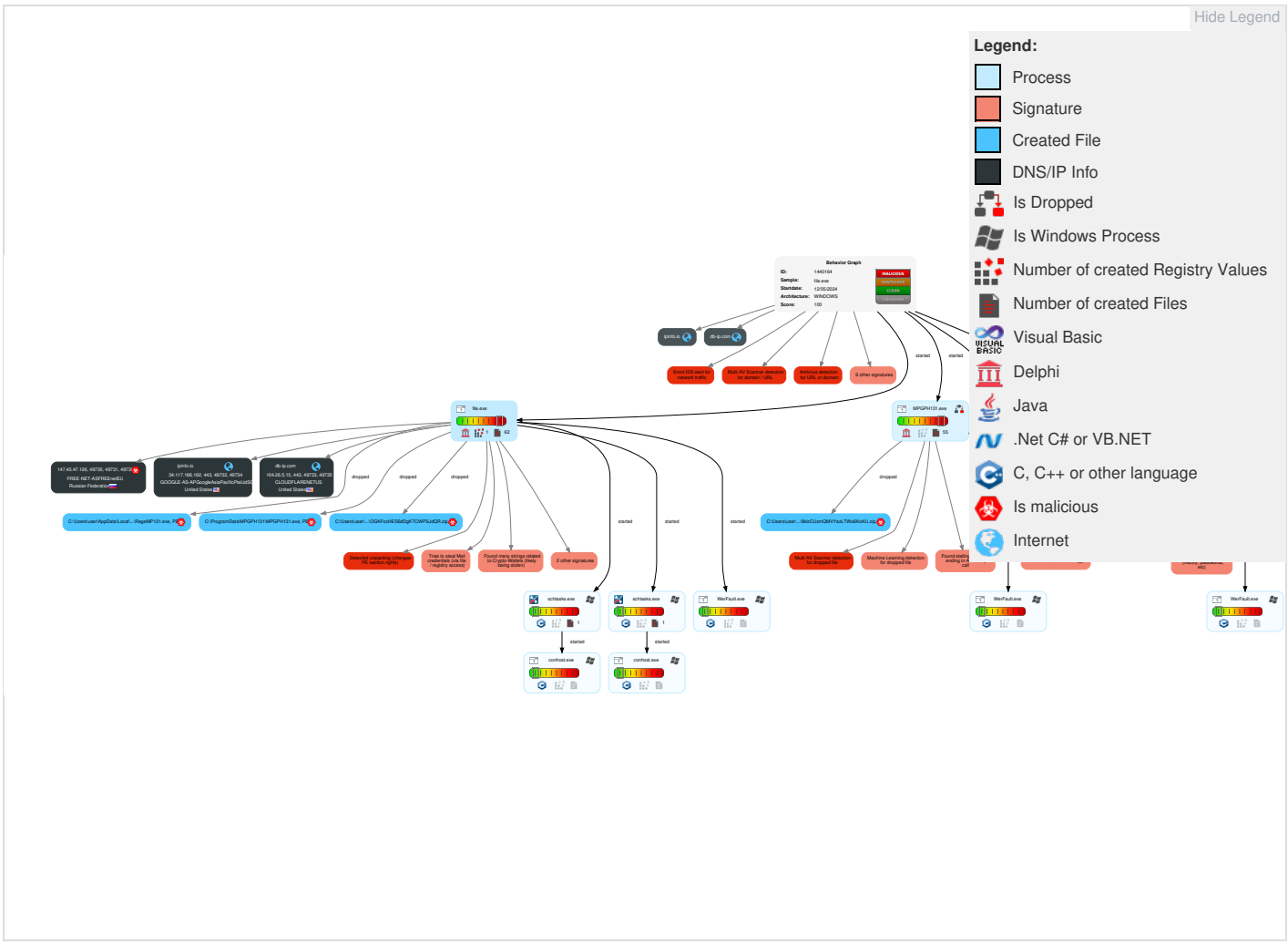
Remote Access Functionality

Yara detected PrivateLoader

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	3 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	1 2 Software Packing	Security Account Manager	3 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 2 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 4 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 2 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
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	HTML Smuggling	/etc/passwd and /etc/shadow	1 Application Window 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 Owner/User Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement
Network Security Appliances	Domains	Compromise Software Dependencies and Development Tools	AppleScript	Launchd	Launchd	Stripped Payloads	Input Capture	1 System Network Configuration Discovery	Software Deployment Tools	Remote Data Staging	Mail Protocols	Exfiltration Over Unencrypted Non-C2 Protocol	Firmware Corruption

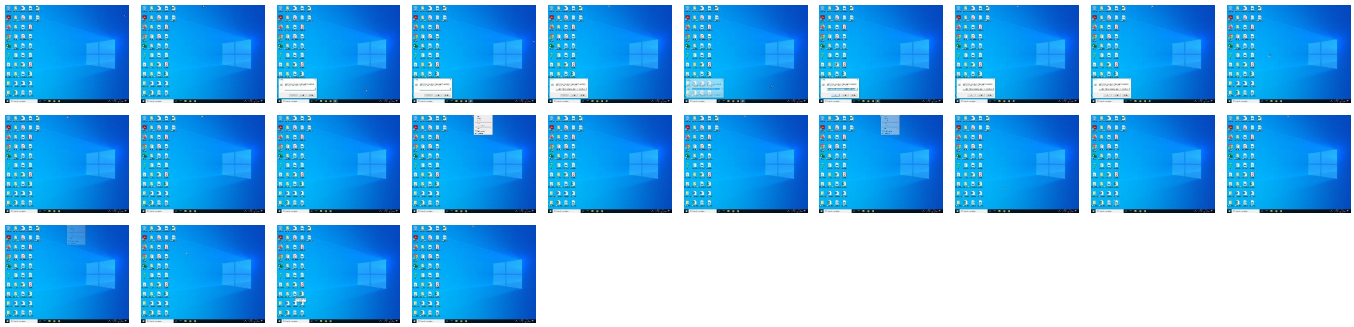
Behavior Graph



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
file.exe	47%	ReversingLabs	Win32.Trojan.Strictor	
file.exe	59%	Virustotal		Browse
file.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.Strictor	
C:\ProgramData\MPGPH131\MPGPH131.exe	59%	Virustotal		Browse
C:\Users\user\AppData\Local\RageMP131\RageMP131.exe	47%	ReversingLabs	Win32.Trojan.Strictor	
C:\Users\user\AppData\Local\RageMP131\RageMP131.exe	59%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://147.45.47.102:57893/hera/amadka.exe	0%	URL Reputation	safe	
http://pki-ocsp.symauth.com0	0%	URL Reputation	safe	
http://https://t.70	0%	Avira URL Cloud	safe	
http://5.42.96.7/cost/go.exe-Q	100%	Avira URL Cloud	phishing	
http://5.42.96.7/cost/lenin.exe9	100%	Avira URL Cloud	phishing	
http://5.42.96.7/cost/lenin.exe	100%	Avira URL Cloud	malware	
http://https://t.j	0%	Avira URL Cloud	safe	
http://5.42.96.7/cost/go.exeOw	100%	Avira URL Cloud	phishing	
http://5.42.96.7/cost/go.exe	100%	Avira URL Cloud	phishing	
http://147.45.47.102:57893/hera/amadka.exee	0%	Avira URL Cloud	safe	
http://5.42.96.7/cost/go.exe68v	100%	Avira URL Cloud	phishing	
http://https://t.=	0%	Avira URL Cloud	safe	
http://5.42.96.7/cost/go.exe	18%	Virustotal		Browse
http://5.42.96.7/cost/go.exec.vTK	100%	Avira URL Cloud	phishing	
http://147.45.47.102:57893/hera/amadka.exee	16%	Virustotal		Browse
http://5.42.96.7/cost/lenin.exe	20%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ipinfo.io	34.117.186.192	true	false		high
db-ip.com	104.26.5.15	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/widget/demo/81.181.60.11	false		high
http://https://db-ip.com/demo/home.php?s=81.181.60.11	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	file.exe, 00000000.00000003.1716313651.0 00000001988000.00000004.00000020.000200 00.00000000.sdmp, file.exe, 00000000.000 00003.1710776395.0000000001988000.000000 04.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710166201.000000000196900 0.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1728 367367.0000000000B44000.00000004.0000002 0.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1721151906.0000000000B 1E000.00000004.00000020.00020000.0000000 0.sdmp, MPGPH131.exe, 00000003.00000003. 1722946740.0000000000B3D000.00000004.000 00020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1743890646.0000000 0009A5000.00000004.00000020.00020000.000 00000.sdmp, MPGPH131.exe, 00000006.00000 003.1746218727.00000000009D6000.00000004 .00000020.00020000.00000000.sdmp, MPGPH1 31.exe, 00000006.00000003.1744801901.000 00000009D3000.00000004.00000020.00020000 .00000000.sdmp, 19u7ECnptzzlWeb Data.3.dr, sYcixjs lgY3sWeb Data.3.dr, v8KCsYORX8h7Web Data.6.dr, SBUYXJCvH4fCWeb Data.6.dr, M4EU2Y_AAhWdWeb Data.0.dr, ldCNLqBK5BIzWeb Data.0.dr, B0 87runuAKfxWeb Data.3.dr, fp5Zfw4ryWNTWeb Data.6.dr, ad9xHU1sHgxoWeb Data.0.dr	false		high
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.zvXrErQ5GYDF	D87fZN3R3jFeplaces.sqlite.3.dr	false		high
http://https://db-ip.com/$	MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORTv	file.exe, 00000000.00000002.2016612734.0 0000000017FE000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	file.exe, 00000000.00000003.1716313651.0 00000001988000.00000004.00000020.000200 00.00000000.sdmp, file.exe, 00000000.000 00003.1710776395.0000000001988000.000000 04.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710166201.000000000196900 0.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1728 367367.0000000000B44000.00000004.0000002 0.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1721151906.0000000000B 1E000.00000004.00000020.00020000.0000000 0.sdmp, MPGPH131.exe, 00000003.00000003. 1722946740.0000000000B3D000.00000004.000 00020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1743890646.0000000 0009A5000.00000004.00000020.00020000.000 00000.sdmp, MPGPH131.exe, 00000006.00000 003.1746218727.00000000009D6000.00000004 .00000020.00020000.00000000.sdmp, MPGPH1 31.exe, 00000006.00000003.1744801901.000 00000009D3000.00000004.00000020.00020000 .00000000.sdmp, 19u7ECnptzzlWeb Data.3.dr, sYcixjs lgY3sWeb Data.3.dr, v8KCsYORX8h7Web Data.6.dr, SBUYXJCvH4fCWeb Data.6.dr, M4EU2Y_AAhWdWeb Data.0.dr, ldCNLqBK5BIzWeb Data.0.dr, B0 87runuAKfxWeb Data.3.dr, fp5Zfw4ryWNTWeb Data.6.dr, ad9xHU1sHgxoWeb Data.0.dr	false		high
http://https://db-ip.com/demo/home.php?s=81.181.60.11G	file.exe, 00000000.00000002.2016612734.0 0000000018C4000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://https://t.j	MPGPH131.exe, 00000003.00000002.2025872612.0000000000A4C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ipinfo.io:443/widget/demo/81.181.60.11	file.exe, 00000000.00000002.2016612734.0 00000001880000.00000004.00000020.000200 00.00000000.sdmp, MPGPH131.exe, 00000003 .00000002.2025872612.0000000000A30000.00 000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.1860003 905.0000000001ADC000.00000004.00000020.0 0020000.00000000.sdmp, RageMP131.exe, 00 000010.00000002.1923638646.0000000001DB8 000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://147.45.47.102:57893/hera/amadka.exe	file.exe, 00000000.00000002.2016612734.0000000018C4000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000002.2025872612.0000000000A4C000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://pki-crl.symauth.com/ca_732b6ec148d290c0a071efd1dac8e288/LatestCRL.crl07	file.exe, RageMP131.exe.0.dr, MPGPH131.exe.0.dr	false		high
http://https://db-ip.com/	RageMP131.exe, 00000010.00000002.1923638646.0000000001E52000.00000004.00000020.00020000.00000000.sdmp	false		high
http://5.42.96.7/cost/go.exe-Q	MPGPH131.exe, 00000003.00000003.1732443446.0000000000B13000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://https://t.me/risepro_botlater60.11	RageMP131.exe, 00000010.00000002.1923638646.0000000001E52000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_botomaniaJ	MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://5.42.96.7/cost/lenin.exe9	MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://pki-crl.symauth.com/offlineca/TheInstituteofElectricalandElectronicsEngineersIncIEEERootCA.cr	file.exe, RageMP131.exe.0.dr, MPGPH131.exe.0.dr	false		high
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	file.exe, 00000000.00000003.1716313651.000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710776395.0000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710166201.0000000001969000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1728367367.0000000000B44000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1721151906.0000000000B1E000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1722946740.0000000000B3D000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1743890646.00000000009A5000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1746218727.00000000009D6000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1744801901.00000000009D3000.00000004.00000020.00020000.00000000.sdmp, 19u7ECnptzzlWeb Data.3.dr, sYcixjslgY3sWeb Data.3.dr, v8KCsYORX8h7Web Data.6.dr, SBUYXJCvH4fCWeb Data.6.dr, M4EU2Y_AAhWdWeb Data.0.dr, ldCNLqBK5BlzWeb Data.0.dr, B087runuAKfxWeb Data.3.dr, fp5Zfw4ryWNTWeb Data.6.dr, ad9xHU1sHgxoWeb Data.0.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	file.exe, 00000000.00000003.1714129104.0000000001976000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1745984308.00000000009C4000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1744541075.00000000009B2000.00000004.00000020.00020000.00000000.sdmp, ITZ0bicyJ58aHistory.6.dr, m78YdG3PG6psHistory.6.dr, 1_QlH4gDMSHgHistory.3.dr, 66rslgkYekRJHistory.3.dr, JRPAhKRZ9ZTqHistory.0.dr, rakgGBowKZnMHistory.0.dr	false		high
http://https://ipinfo.io/widget/demo/81.181.60.11m	MPGPH131.exe, 00000003.00000002.2025872612.00000000009E9000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://db-ip.com/demo/home.php?s=81.181.60.11Z	MPGPH131.exe, 00000003.00000002.2025872612.0000000000A4C000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://5.42.96.7/cost/lenin.exe	file.exe, 00000000.00000002.2016612734.0 0000000018C4000.00000004.00000020.000200 00.00000000.sdmp, MPGPH131.exe, 00000003 .00000002.2025872612.0000000000A97000.00 000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.17325089 63.0000000000B1E000.00000004.00000020.00 020000.00000000.sdmp, MPGPH131.exe, 0000 0006.00000002.2038444283.00000000008D700 0.00000004.00000020.00020000.00000000.sdmp	false	• 20%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://db-ip.com:443/demo/home.php?s=81.181.60.11	file.exe, 00000000.00000002.2016612734.0 0000000018C4000.00000004.00000020.000200 00.00000000.sdmp, MPGPH131.exe, 00000003 .00000002.2025872612.0000000000A4C000.00 000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.20384442 83.0000000000857000.00000004.00000020.00 020000.00000000.sdmp, RageMP131.exe, 000 00010.00000002.1923638646.0000000001DB80 00.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_bot(	RageMP131.exe, 00000007.00000002.1860003 905.0000000001B5F000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	ITZ0bicyJ58aHistory.6.dr, m78YdG3PG6psHistory.6.dr, 1_QlH4gDMSHgHistory.3.dr, 66rslgkYekRJHistory.3.dr, JRPAhKRZ9ZTqHistory.0.dr, rakgGBowKZnMHistory.0.dr	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	file.exe, 00000000.00000003.1716313651.0 000000001988000.00000004.00000020.000200 00.00000000.sdmp, file.exe, 00000000.000 00003.1710776395.0000000001988000.000000 04.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710166201.0000000001969000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1728 367367.0000000000B44000.00000004.0000002 0.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1721151906.0000000000B 1E000.00000004.00000020.00020000.0000000 0.sdmp, MPGPH131.exe, 00000003.00000003. 1722946740.0000000000B3D000.00000004.000 00020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1743890646.0000000 0009A5000.00000004.00000020.00020000.000 00000.sdmp, MPGPH131.exe, 00000006.00000 003.1746218727.00000000009D6000.00000004 .00000020.00020000.00000000.sdmp, MPGPH1 31.exe, 00000006.00000003.1744801901.000 00000009D3000.00000004.00000020.00020000 .00000000.sdmp, 19u7ECnptzzlWeb Data.3.dr, sYcixjslgY3sWeb Data.3.dr, v8KCsYORX8h7Web Data.6.dr, SBUYXJCvH4fCWeb Data.6.dr, M4EU2Y_AAhWdWeb Data.0.dr, ldCNLqBK5BIzWeb Data.0.dr, B087runuAKfxWeb Data.3.dr, fp5Zfw4ryWNTWeb Data.6.dr, ad9xHU1sHgxoWeb Data.0.dr	false		high
http://https://t.me/risepro_bot6	MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://db-ip.com/demo/home.php?s=81.181.60.11SRL	MPGPH131.exe, 00000003.00000002.2025872612.0000000000A4C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.70	RageMP131.exe, 00000007.00000002.1860003 905.0000000001B5F000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://db-ip.com/O	RageMP131.exe, 00000007.00000002.1860003 905.0000000001B5F000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORTB	MPGPH131.exe, 00000003.00000002.2025872612.00000000009AD000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_botrisepro	MPGPH131.exe, 00000003.00000002.2025872612.0000000000A4C000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 0000 0006.00000002.2038444283.00000000008D700 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORT9?	file.exe, 00000000.00000002.2017190533.0 0000000018FE000.00000004.00000020.000200 00.00000000.sdmp, file.exe, 00000000.000 00003.1754759356.00000000018FE000.000000 04.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://5.42.96.7/cost/go.exe	file.exe, 00000000.00000002.2016612734.0000000018C4000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000002.2025872612.0000000000A97000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1732443446.0000000000B13000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	false	• 18%, Virustotal, Browse • Avira URL Cloud: phishing	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	file.exe, 00000000.00000003.1716313651.0000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710776395.0000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710166201.0000000001969000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1728367367.0000000000B44000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1721151906.0000000000B1E000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1722946740.0000000000B3D000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1743890646.0000000009A5000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1746218727.00000000009D6000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1744801901.00000000009D3000.00000004.00000020.00020000.00000000.sdmp, 19u7ECnptzzlWeb Data.3.dr, sYcixjslgY3sWeb Data.3.dr, v8KCsYORX8h7Web Data.6.dr, SBUYXJCvH4fCWeb Data.6.dr, M4EU2Y_AAhWdWeb Data.0.dr, ldCNLqBK5BlzWeb Data.0.dr, B087runuAKfxWeb Data.3.dr, fp5Zfw4ryWNTWeb Data.6.dr, ad9xHU1sHgxoWeb Data.0.dr	false		high
http://https://db-ip.com:443/demo/home.php?s=81.181.60.11&OLa	RageMP131.exe, 00000007.00000002.1860003905.0000000001ADC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://5.42.96.7/cost/go.exeOw	file.exe, 00000000.00000002.2016612734.0000000018C4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://147.45.47.102:57893/hera/amadka.exee	MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	false	• 16%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ipinfo.io/https://www.maxmind.com/en/locate-my-ip-addressWs2_32.dll	file.exe, 00000000.00000002.2015608699.000000000BB1000.00000040.00000001.01000000.00000003.sdmp, MPGPH131.exe, 00000003.00000002.2026784616.0000000000F01000.00000040.00000001.01000000.00000004.sdmp, MPGPH131.exe, 00000006.00000002.2039072826.0000000000F01000.00000040.00000001.01000000.00000004.sdmp, RageMP131.exe, 00000007.00000002.1858273700.0000000000B81000.00000040.00000001.01000000.00000006.sdmp, RageMP131.exe, 00000010.00000002.1922715500.0000000000B81000.00000040.00000001.01000000.00000006.sdmp	false		high

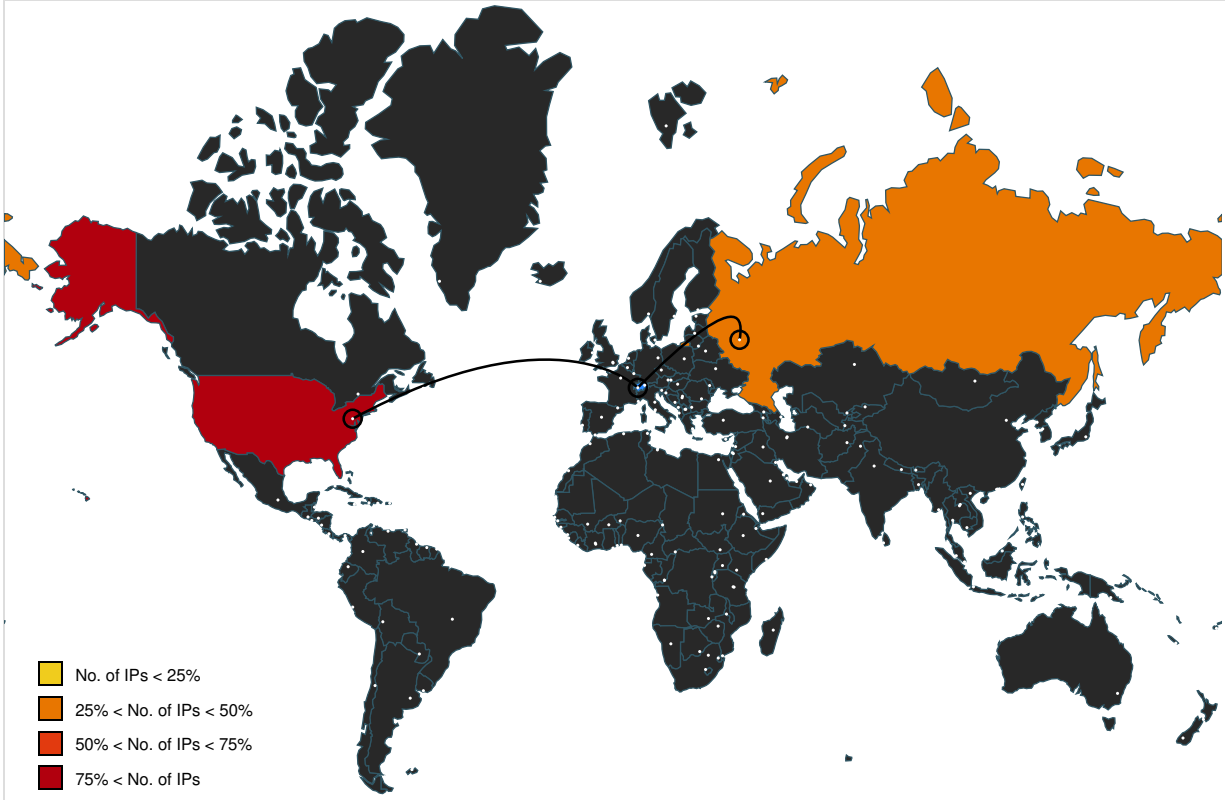
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	file.exe, 00000000.00000003.1716313651.000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710776395.0000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710166201.0000000001969000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1728367367.0000000000B44000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1721151906.0000000000B1E000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1722946740.0000000000B3D000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1743890646.0000000009A5000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1746218727.00000000009D6000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1744801901.00000000009D3000.00000004.00000020.00020000.00000000.sdmp, 19u7ECnptzzlWeb Data.3.dr, sYcixjslgY3sWeb Data.3.dr, v8KCsYORX8h7Web Data.6.dr, SBUYXJCvH4fCWeb Data.6.dr, M4EU2Y_AAhWdWeb Data.0.dr, ldCNLqBK5BIzWeb Data.0.dr, B087runuAKfxWeb Data.3.dr, fp5Zfw4ryWNTWeb Data.6.dr, ad9xHU1sHgxoWeb Data.0.dr	false		high
http://5.42.96.7/cost/go.exe68v	MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://upx.sf.net	Amcache.hve.10.dr	false		high
http://https://t.me/RiseProSUPPORT	MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1786714219.0000000000999000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2038444283.0000000000857000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.1860003905.0000000001AAE000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000010.00000002.1923638646.0000000001DB8000.00000004.00000020.00020000.00000000.sdmp, OGKFocHES6dDgKTCWPSJdQR.zip.0.dr, 8klzCUsmQMVYazLTWo6KoKU.zip.3.dr, ZeTvTkc8PqqpWi0gm5JPfdt.zip.6.dr	false		high
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	file.exe, 00000000.00000003.1714129104.000000001976000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1745984308.00000000009C4000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1744541075.00000000009B2000.00000004.00000020.00020000.00000000.sdmp, ITZ0bicyJ58aHistory.6.dr, m78YdG3PG6psHistory.6.dr, 1_QlH4gDMSHgHistory.3.dr, 66rslgkYekRJHistory.3.dr, JRPAhKRZ9ZTqHistory.0.dr, rakgGBowKZnMHistory.0.dr	false		high
http://https://db-ip.com/demo/home.php?s=81.181.60.1196	MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.ecosia.org/newtab/	file.exe, 00000000.00000003.1716313651.0000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710776395.0000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710166201.0000000001969000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1728367367.0000000000B44000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1721151906.0000000000B1E000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1722946740.0000000000B3D000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1743890646.0000000009A5000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1746218727.00000000009D6000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1744801901.00000000009D3000.00000004.00000020.00020000.00000000.sdmp, 19u7ECnptzzlWeb Data.3.dr, sYcixjslgY3sWeb Data.3.dr, v8KCsYORX8h7Web Data.6.dr, SBUYXJCvH4fCWeb Data.6.dr, M4EU2Y_AAhWdWeb Data.0.dr, ldCNLqBK5BIzWeb Data.0.dr, B087runuAKfxWeb Data.3.dr, fp5Zfw4ryWNTWeb Data.6.dr, ad9xHU1sHgxoWeb Data.0.dr	false		high
http://https://ipinfo.io/Mozilla/5.0	file.exe, 00000000.00000002.2016612734.0000000001880000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000002.2025872612.0000000000A30000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.1860003905.0000000001B3B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000010.00000002.1923638646.0000000001E37000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	D87fZN3R3jFeplaces.sqlite.3.dr	false		high
http://https://t.=	RageMP131.exe, 00000010.00000002.1923638646.0000000001E52000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://t.me/risepro0.11	RageMP131.exe, 00000007.00000002.1860003905.0000000001B5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io/wv~1	RageMP131.exe, 00000010.00000002.1923638646.0000000001DE7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io/widget/demo/81.181.60.11eG	file.exe, 00000000.00000002.2016612734.00000000183A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_botomania	file.exe, 00000000.00000002.2016612734.0000000018C4000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	file.exe, 00000000.00000003.1716313651.0 00000001988000.00000004.00000020.000200 00.00000000.sdmp, file.exe, 00000000.000 00003.1710776395.0000000001988000.000000 04.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710166201.000000000196900 0.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1728 367367.0000000000B44000.00000004.0000002 0.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1721151906.0000000000B 1E000.00000004.00000020.00020000.0000000 0.sdmp, MPGPH131.exe, 00000003.00000003. 1722946740.0000000000B3D000.00000004.000 00020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1743890646.0000000 0009A5000.00000004.00000020.00020000.000 00000.sdmp, MPGPH131.exe, 00000006.00000 003.1746218727.00000000009D6000.00000004 .00000020.00020000.00000000.sdmp, MPGPH1 31.exe, 00000006.00000003.1744801901.000 00000009D3000.00000004.00000020.00020000 .00000000.sdmp, 19u7ECnptzzlWeb Data.3.dr, sYcixjs lgY3sWeb Data.3.dr, v8KCsYORX8h7Web Data.6.dr, SBUYXJCvH4fCWeb Data.6.dr, M4EU2Y_AAhWdWeb Data.0.dr, ldCNLqBK5BIzWeb Data.0.dr, B0 87runuAKfxWeb Data.3.dr, fp5Zfw4ryWNTWeb Data.6.dr, ad9xHU1sHgxoWeb Data.0.dr	false		high
http://https://t.me/risepro_bot	RageMP131.exe, 00000010.00000002.1923638 646.0000000001E52000.00000004.00000020.0 0020000.00000000.sdmp, passwords.txt.0.dr, passwor ds.txt.3.dr, passwords.txt.6.dr	false		high
http://https://ipinfo.io/:	file.exe, 00000000.00000002.2016612734.0 00000000183F000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://https://t.me/risepro_botlater	file.exe, 00000000.00000002.2016612734.0 0000000018C4000.00000004.00000020.000200 00.00000000.sdmp, MPGPH131.exe, 00000003 .00000002.2025872612.0000000000A4C000.00 000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.1860003 905.0000000001B5F000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://https://db-ip.com/demo/home.php?s=81.181.60.111	RageMP131.exe, 00000007.00000002.1860003 905.0000000001B5F000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://https://ipinfo.io/	RageMP131.exe, 00000010.00000002.1923638 646.0000000001E19000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://pki-ocsp.symauth.com0	file.exe, RageMP131.exe.0.dr, MPGPH131.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://ipinfo.io:443/widget/demo/81.181.60.11o	MPGPH131.exe, 00000006.00000002.20384442 83.0000000000857000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://www.maxmind.com/en/locate-my-ip-address	MPGPH131.exe	false		high
http://www.winimage.com/zLibDll	file.exe, 00000000.00000002.2015608699.0 000000000BB1000.00000040.00000001.010000 00.00000003.sdmp, MPGPH131.exe, 00000003 .00000002.2026784616.0000000000F01000.00 000040.00000001.01000000.00000004.sdmp, MPGPH131.exe, 00000006.00000002.20390728 26.0000000000F01000.00000040.00000001.01 000000.00000004.sdmp, RageMP131.exe, 000 00007.00000002.1858273700.0000000000B810 00.00000040.00000001.01000000.00000006.sdmp, RageMP131.exe, 00000010.00000002.1922715500.0 000000000B81000.00000040.00000001.010000 00.00000006.sdmp	false		high
http://https://support.mozilla.org	D87fZN3R3jFeplaces.sqlite.3.dr	false		high
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	ITZ0bicyJ58aHistory.6.dr, m78YdG3PG6psHistory.6.dr , 1_QlH4gDMSHgHistory.3.dr, 66rslgkYekRJHistory.3. dr, JRPAhKRZ9ZTqHistory.0.dr, rakgGBowKZ nMHistory.0.dr	false		high
http://https://db-ip.com/demo/home.php?s=81.181.60.117	file.exe, 00000000.00000002.2016612734.0 0000000018C4000.00000004.00000020.000200 00.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	file.exe, 00000000.00000003.1716313651.000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710776395.0000000001988000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1710166201.0000000001969000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1728367367.0000000000B44000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1721151906.0000000000B1E000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000003.00000003.1722946740.0000000000B3D000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1743890646.0000000009A5000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1746218727.00000000009D6000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000003.1744801901.00000000009D3000.00000004.00000020.00020000.00000000.sdmp, 19u7ECnptzzlWeb Data.3.dr, sYcixjslgY3sWeb Data.3.dr, v8KCsYORX8h7Web Data.6.dr, SBUYXJCvH4fCWeb Data.6.dr, M4EU2Y_AAhWdWeb Data.0.dr, ldCNLqBK5BlzWeb Data.0.dr, B087runuAKfxWeb Data.3.dr, fp5Zfw4ryWNTWeb Data.6.dr, ad9xHU1sHgxoWeb Data.0.dr	false		high
http://https://ipinfo.io/widget/demo/81.181.60.11P	MPGPH131.exe, 00000006.00000002.2038444283.0000000008D7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://5.42.96.7/cost/go.exec.vTK	MPGPH131.exe, 00000003.00000002.2025872612.0000000000A97000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown

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
104.26.5.15	db-ip.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1440164
Start date and time:	2024-05-12 12:02:08 +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:	file.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@14/81@2/3
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 58% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, SIHClient.exe, conhost.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 NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:02:53	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run RageMP131 C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
11:02:54	Task Scheduler	Run new task: MPGPH131 HR path: C:\ProgramData\MPGPH131\MPGPH131.exe
11:02:56	Task Scheduler	Run new task: MPGPH131 LG path: C:\ProgramData\MPGPH131\MPGPH131.exe
11:03:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run RageMP131 C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
12:03:31	API Interceptor	3x 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\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3241984
Entropy (8bit):	7.9780906837515655
Encrypted:	false
SSDEEP:	98304:0y5rnbPr5he+zDgy3yQ7rDnI19mQxWaF67:0ADbPDQyCErDI19mQxvF6
MD5:	72007357BEB74FEA20E7DAA285212B16
SHA1:	E37F50ACE578FC3A69FB7A312A659D51491E32B0
SHA-256:	6A1BDA6FA37B02776B44C80FC1D8329BD7FBD49FF46EAF37346E5C436A52EC9E
SHA-512:	72A731A1F9DFA6E927665BB5649420A1114FECAAC6E7E30CCDA9028F37C1E6DE582E0F237F5A95CD012603B916C19AA31582729FCBC3D86DB4A2C4B96D6AC04E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47% • Antivirus: Virustotal, Detection: 59%, Browse
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...jR;f.....'.....C.....@.....`.....@... .. ..P.....p.....0.....<.....@.....@.....@.....P...P.....B.....@.....J.....@.....p...b...J.....@....rsrc.....@..@.....y.....(...v.....@....data.....".....".....@.....

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

Process:	C:\Users\user\Desktop\file.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_a2f39f18c7bab85a936641112cf4d8a65518de_de9be973_9436b2ab-098a-4a19-b205-1dc59dcf74a1\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):	1.0848730846464338
Encrypted:	false
SSDEEP:	192:2WCla+zq8Dz0N/76G6E6jjTZrlyLB+EzuiFeZ24IO826t:EvqegN/76ZjNEzuiFeY4IO8p
MD5:	6D1CA6FA7CC5E11C779DA8505F7044BD
SHA1:	DE94057A574DABD506916FBB4C49D5FCFF0018C6
SHA-256:	352D053BA30FCF1B708AA89BD0DD4FD34A7704E4F39C8ED778D1A443E530BE03
SHA-512:	A363F190E06828BE801742C6125DBFEF59F5FDC6C9414A6279779483BBC4861FC478B5335641F90FBAC785792137FB02C37D2446859088CA1B3EE061B10C2F34
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.=.1.3.3.5.9.9.8.1.7.9.0.8.0.8.2.9.9.5.....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.=.1.3.3.5.9.9.8.1.7.9.2.0.2.7.0.5.5.7.....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.=.9.4.3.6.b.2.a.b.-.0.9.8.a.-.4.a.1.9.-.b.2.0.5.-.1.d.c.5.9.d.c.f.7.4.a.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.=.7.1.d.3.0.9.3.3.-.0.8.1.c.-.4.f.a.3.-.a.4.c.3.-.9.c.0.b.8.3.d.8.5.3.2.8.....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.=.0.0.0.0.0.2.8.8.-.0.0.0.1.-.0.0.1.4.-.4.9.3.4.-.d.5.8.f.5.3.a.4.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.e.3.7.f.5.0.a.c.e.5.7.8.f.c.3.a.6.9.f.b.7.a.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_MPGPH131.exe_a2f39f18c7bab85a936641112cf4d8a65518de_de9be973_94773830-acbf-49ed-a888-c6bd52737c00\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):	1.0915295450278297
Encrypted:	false
SSDEEP:	192:Y0lS+zD8Dz0N/76G6E6jjYZrSruBF9zuiFeZ24IO826t:rXDegN/76ZjC9zuiFeY4IO8p
MD5:	A8D137DE10693B8D60435C79C4D1BE12
SHA1:	061332B6D6A678E83FCB112ED21AD2DA85333C4F
SHA-256:	9F7EC3A17FD18745DDB3663C88AC5E3A1B3678763F73266EABD27A608462A916
SHA-512:	1B8AAAF7CEEB792D3187FCCE4C2776DD7BDBF08439380D6F1726896BCD7CD255BDAB784BC2CFA25C0475D23AEA0D9727E400DAFFD3A5F9FD971E50FB3EE86D25
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.=.1.3.3.5.9.9.8.1.7.9.0.8.4.4.4.8.1.7.....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.=.1.3.3.5.9.9.8.1.7.9.2.1.5.6.9.8.4.3.....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.=.9.4.7.7.3.8.3.0.-.a.c.b.f.-.4.9.e.d.-.a.8.8.8.-.c.6.b.d.5.2.7.3.7.c.0.0.....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.c.2.5.4.b.9.5.-.6.3.5.5.-.4.2.3.2.-.a.a.f.1.-.1.2.c.8.7.5.b.7.d.2.7.9.....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.=.0.0.0.0.0.5.9.c.-.0.0.0.1.-.0.0.1.4.-.7.0.9.1.-.8.b.8.e.5.3.a.4.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.e.3.7.f.5.0.a.c.e.5.7.8.f.c.3.a.6.9.f.b.7.a.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_f72aa47e83387be13decffad958dd6df2948b_3ea92c58_dec5365b-211a-4509-a3ee-25eef0619427\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):	1.0841666276870021
Encrypted:	false
SSDEEP:	192:bvgvBKhvkgPXF07VDlIl3jYZrSruVzfzuiFeZ24IO8iB:Wakgvm7VDlBjAfzuiFeY4IO8S
MD5:	6A3C0263B0FE85DDC8D460E4041DF5F9
SHA1:	BE5C14905183120605A91410F6B4C31DDA4D60E9
SHA-256:	088908B7FAA974FA06F2E0410AE67A43B04DD1F3D061A879F557EF328DA98C6A
SHA-512:	B30A8EFB194BFEC3C20419079A95F9AD0C33C9C82D352C628E33193200D32D5474593CEF0BC75D5940793CB34E89618AC3824D2BB7330FB88D6C38790679A36

Malicious:	false
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.=.1.3.3.5.9.9.8.1.7.8.9.4.6.8.4.5.7.5.....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.=.1.3.3.5.9.9.8.1.7.9.1.2.6.5.3.3.1.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.e.c.5.3.6.5.b.-.2.1.1.a.-.4.5.0.9.-.a.3.e.e.-.2.5.e.e.f.0.6.1.9.4.2.7.....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.=.d.9.7.d.7.3.f.6.-.2.b.a.f.-.4.3.2.a.-.8.e.0.a.-.2.b.4.4.f.2.e.7.f.f.8.0.....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.=.f.i.l.e...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.=.0.0.0.0.0.2.e.8.-.0.0.0.1.-.0.0.1.4.-.5.f.f.4.-.2.b.8.d.5.3.a.4.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.3.6.0.0.0.0.0.0.9.1.0.!.0.0.0.0.e.3.7.f.5.0.a.c.e.5.7.8.f.c.3.a.6.9.f.b.7.a.3.1.2.a.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1C00.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun May 12 10:03:10 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	129498
Entropy (8bit):	1.857568066610471
Encrypted:	false
SSDEEP:	384:zJhmAX51ue6EYq0smQweS/B3fO8VRpDw+4sIG5/jJ2DmQbBKZB:z7XTue6xxNQ03hFD14vGNF2awBI
MD5:	78FDFD9D8DF6405323D119C96499AB31
SHA1:	24D77575C66015C624FC7ED0BE3C27A4AC1483EF
SHA-256:	9ED05429DB89E116C8DCE0AD108FFEC1CEB54A56C6E5C24BA641A01139155FB1
SHA-512:	CBB508564D8F845A86FA5CCDC36A52060259C7EE3DC9C9FA544E83252530292B2FF554E6CF6DDD93541623A1500DE89042B44B6E70C94D5383BEEB8CA72E81F
Malicious:	false
Preview:	MDMP..a..... .....@f.....D.....H...X.....I....%.....$....U.....`.....8.....T.....N.....&.....'.....eJ.....(....GenuineIntel.....T.....@f.....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\WER1F9B.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):	8372
Entropy (8bit):	3.6943459612633713
Encrypted:	false
SSDEEP:	192:R6l7wVeJFCy6T6Y9kSUS67gmfBhJJQprF89bjdsfBhm:R6lXJl6T6YOSUS67gmf3JJnjWfW
MD5:	7D9C49C01B0E7F6CD914C73C79C35E37
SHA1:	1F8AD420E11DF4B79406189ABB4895F4DE7592D2
SHA-256:	72F406A1B198CA18B745881F89AA535F766342AE5C3B2F73728A948CC11BD68F
SHA-512:	219B28B62618AED952260CA62A614EB451862DEBB033344EDA7A17A473D0E7667922BF3BD4695AEB633194127E152DC12F51C4E7DDCF34A06CFC8B2F69E87A1
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.>.7.4.4.<./.P.i.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2019.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4693
Entropy (8bit):	4.497637899098605
Encrypted:	false
SSDEEP:	48:cvIwWl8zsdJg77al9tCWpW8VYoYm8M4JGwhfFKz+q8khs+1qVyxoYafd:uljf3l7rD7VYJWzvggxoY8d
MD5:	4F6E15A022B6829FDA98E3475E2F8347
SHA1:	5426BF9ADD7A9C04BA4C86D3E4FE5FA7C9B64D2E
SHA-256:	EE4888A8318A68A61A49A26E10A2535CBCE6007BE4CA13ABB8F7FA4FE9306A7B
SHA-512:	34A801720D56EB0B8B0931BA8BF4776BF76EADD675DDEF571855D00D74AEED803A56C2554F58AA3AB30830247F3C9350DD10659C93D4C50E963DA35D9DA2D9C
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg nm="geoid" val="223" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="319745" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\ProgramData\Microsoft\Windows\WER\Temp\WER20C3.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun May 12 10:03:11 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	132270
Entropy (8bit):	1.8059476559714567
Encrypted:	false
SSDEEP:	384:9wJ2rVqyDXAXxLSe6iv0z9+P0pyFw5n63IT3hGc8nwLgNQF2y4HegkCahW0:9ZrV3QXZSe6FzXpT03IbBCNQF49aJ
MD5:	D433322A8EFE15733AD3C40B15A49753
SHA1:	6DC2992CAF5EB1DDCCFE000BD2335C64A063120A
SHA-256:	34D540EE2D778BA0BF0CA7075612055484AD8169F6F65622F2ADB6BB8CCE5F1E
SHA-512:	90EE2BA9F3BAF8A53608C48B5253AF34090FA588412781A0292E963909E95529A06CD8B5E5E9ED565D0748E93EA16A6E05BD4CB2338684E6F66EAEFDB442358F
Malicious:	false
Preview:	MDMP..a..... .....@f.....D.....X.....I...4%.....T.....`.....8.....T.....L.....%.....'.....eJ.....$(... ...GenuineIntel.....T.....@f.....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\WER214F.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun May 12 10:03:11 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	128110
Entropy (8bit):	1.8527198806427885
Encrypted:	false
SSDEEP:	384:iqaoTaHlue6e+Hte8WepRyu6UuAjdSAWsx3HkfvVM4:N/TUue6eEt/cOPGfdM4
MD5:	8BE259A42CE320284F547ECA648E06FD
SHA1:	861C2E3656EF90BB0B63F2E7E89F46F37D20B0E8
SHA-256:	218BE593563F4EF9AC005139175C0311519AE76C25A5753F508C744D898B1BC8
SHA-512:	E57497F3EDF663765B29E0DF4CF2812611C8CE96492B858E1DA0757AFDD2B968880934B0F7F476C7EF8CDC37791D2DAFB9F1794B631B9D62230DD728425783F
Malicious:	false
Preview:	MDMP..a..... .....@f.....D.....H...X.....I....%.....U.....`.....8.....T.....xL.....&.....'.....eJ.....(... ...GenuineIntel.....T.....@f.....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\WER21FC.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):	6368
Entropy (8bit):	3.727014031899765
Encrypted:	false
SSDEEP:	192:R6l7wVeJLuV6kcYizJJrpra89badsf+em:R6lXJo6kcYMJJ1aWf+
MD5:	8D59EA10F8F3A1A09476A275F0FD982F
SHA1:	2B5827F482A6766B2A8C4965EE22E624957F78C4
SHA-256:	388AD2B848669C50A82ED3E83774B706230E782EDF33F9F7FE0C56109474DD44
SHA-512:	3D302461CE04910E922F10A7896545D91A9C82FAD2ED082035AB7C51F44C5CB403CEAEDB15C3C060C292B58769F8CC56434C8397AAB06A5B5A45359B3FCF3C6
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.>.6.4.8.<./.P.i.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER226A.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):	6372
Entropy (8bit):	3.727914298468493
Encrypted:	false
SSDEEP:	192:R6l7wVeJJub6mjTYizJJrpr689baFsf5em:R6lXJk64YMJJVaefp
MD5:	9C9D0BDABF1B2755954555C269B8E11F
SHA1:	54D35F61D2DD9D8D712EB922D3813CFCF8783E72
SHA-256:	C038A9267EB41CC175285F498DC7ED5CDE931640AAE8FC21F18B7F340EA3CB66
SHA-512:	F4B4CE89D094554774839100A0D6E52D112CAFB46B31E05041292AEF766A3E8CBD328B1FEBD4337725EC7474DA9EA46B3DA2C4018DE504F8B49F1F4D8A3CF3 1
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.>.1.4.3.6.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER226B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4713
Entropy (8bit):	4.52370810854721
Encrypted:	false
SSDEEP:	48:cvIwWl8zsdJg77aI9tCWpW8VYwYm8M4Jy8zF3+q8fYAxVyaojrfd:uIjf3l7rD7V4JNJgZxgaojDd
MD5:	95699BB3B22E438924C763D6C79EC250
SHA1:	38B36CED2DB0A8743874741B253BA6DE65B18BFA
SHA-256:	5928ABDD4EFBD48B8B33D14556CA232F84F9DD13A1B0295477647EC736CCA18C
SHA-512:	9E038659D2ED848DE721A335F19D6A353B2CD92DF1E312621DAE47AFD4803DEBE2E78F423AEDDD5D0A6537A8E08F7A0DD2F201EBF9B8A31280823024B5582D F7
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="319745" />.. <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\WER22B9.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4713
Entropy (8bit):	4.524696941130901
Encrypted:	false
SSDEEP:	48:cvIwWl8zsdJg77aI9tCWpW8VYXYm8M4Jy8zFK+q8fYZ+Vyaoj/fd:uIjf3l7rD7V3JNogi+gaojHd
MD5:	40FBC326C8424DBCD784075A0FAFB469
SHA1:	FEAD49005144474507B777A5F5ABF4C14A611FE4
SHA-256:	F62F7B554F524977D1B7DF31820B4B4EDF0E85DA703727A92D8C4A0858F904FC
SHA-512:	DF6E823E8D2166CF2C58F3198A6DF3FD910BE1859CD41B0F0B87E2F675431CC48A64BC19C52CF6C858A02A275A73AFE257828DB42E7DB314032B43CF33C3C7 4
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="319745" />.. <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\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3241984
Entropy (8bit):	7.9780906837515655
Encrypted:	false
SSDEEP:	98304:0y5rnbPr5he+zDgy3yQ7rDnI19mQxWaF67:0ADbPDQyCErDI19mQxvF6
MD5:	72007357BEB74FEA20E7DAA285212B16
SHA1:	E37F50ACE578FC3A69FB7A312A659D51491E32B0
SHA-256:	6A1BDA6FA37B02776B44C80FC1D8329BD7FBD49FF46EAF37346E5C436A52EC9E
SHA-512:	72A731A1F9DFA6E927665BB5649420A1114FECAAC6E7E30CCDA9028F37C1E6DE582E0F237F5A95CD012603B916C19AA31582729FCBC3D86DB4A2C4B96D6AC04E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47% • Antivirus: Virustotal, Detection: 59%, Browse
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...jR;f.....'.....C.....@.....`.....@... .. ..P.....p.....0.....<.....@.....@.....@.....P...P.....B.....@.....J.....@.....p...b...J.....@....rsrc.....@..@.....y.....(...v.....@....data....."....."....@.....

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

Process:	C:\Users\user\Desktop\file.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
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\8klzCUsmQMVYazLTWo6KoKU.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):	5562
Entropy (8bit):	7.899388839027838
Encrypted:	false
SSDEEP:	96:9WGzqeAoMq+YK0KF8cAJiI2i+uVy611sFDgsmns0sq0/gL3KJd:RqASpF8wFmHMDgsIsq0/w6Jd
MD5:	72E1DF0B34942CC21E3D5AF1BBC42740
SHA1:	9117F1EDDD55D6E6646EB5B742920368F305FABE
SHA-256:	124FFEB118D235DE2CCDAC22BF23AEC7114033A17BC49183BFCE2E473A1E147B
SHA-512:	E1A33FFB7850B147F1AED4927CCD5470076EA37A3736ACA9091A6E78587DA7D58D46CA9C991416E1552BC50DA8BD8C5CBE08D532F1B6DA8B6706BD22DF7836C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: C:\Users\user\AppData\Local\Temp\8klzCUsmQMVYazLTWo6KoKU.zip, Author: Joe Security
Preview:	PK.....a`.X.....Cookies\..PK.....a`.XQn.+.....Cookies\Chrome_Default.txt.G..r...U.#.5C.....s$..-.D...7.\..$.G.)o....:....Z.C.f_..pm....."..t..t....}.k.@...a.2+P`.0.x.>....s..k%._..b..P..((.....B.....`.7..-m..JY..F....E.*.l.....l..&.....<J..M.....,V...)b.....Q..k.....M?.5L....h}.....X..'.0..tB.G...\;.a....4.....B4.....J.4.6.y:....4.-.UfE...3A*p.U5UX....Z.g:*e.j.C..Bw.....e..a^.vU:....$..U.....B..`._.e.....+...9.{u...7.e...H.]02...%yR".0...x...P<..N....R.}....{.G...;..c..x...kw.'S>.d|.....B..k.9.t.!>.rh...~n.[....s#/....`..!..Kb8%&.vZB`....O|.....>K.....L*...d0..03..t...T&.....`N.xp..".J.....Q.....c..5...).Z.91.6.j..G.....Wr...a.52!..(^.U.....6....dB.D.^...7..0H.\J9.H.$^`e"..d...\....B.8Z=.qeP.3Y.>..'W.X..T..>z...,..K.....g....%B.w4#...;.[]u|....v...3.;L..U?..b.....u..*..... .....F...P.a...|R*3.=.....r.:.64...#D..^..>.A..ZT.]E.....t...f...1..3....`...X.....C.]%...p.p.ym

C:\Users\user\AppData\Local\Temp\OGKFocHES6dDgKTCWPSJdQR.zip

Process:	C:\Users\user\Desktop\file.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	modified
Size (bytes):	5560
Entropy (8bit):	7.899805493655838
Encrypted:	false
SSDEEP:	96:9WGzqeAoMq+YK0KF8cAJiI2i+upx+xa+uOsp1UIOCrx6wmc03KJm:RqASpF8wFnuOsp86Jm
MD5:	333D01FF0C692D723E5170FDA912B5AF
SHA1:	07D4BEA07B71774D9D0F68EF748CB8741C63830C
SHA-256:	F09CDDEAD24F51F9AC512A6831006FBA2A6E55052B504DEDAA10F47547F17D55
SHA-512:	8143FE17258C37A44F9AC39103F91C88ADA65DADE80D63CDE979C43F9FC55E9EE60AB33C082FD3AD8E3B2E456ED28CDE1456840BDE513DDA624C496CA327E412
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: C:\Users\user\AppData\Local\Temp\OGKFocHES6dDgKTCWPSJdQR.zip, Author: Joe Security
Preview:	PK.....a`.X.....Cookies\..PK.....a`.XQn.+.....Cookies\Chrome_Default.txt.G..r...U.#.5C.....s$..-.D...7.\..$.G.)o....:....Z.C.f_..pm.....".t..t....}.k.@...a.2+ P`.0.x.>....s..k%.._..b..P..((.....B.....`.7..-m..JY..F....E.*.l.....I..&.....<J..M.....,V...)b.....Q..k.....M?.5L....h}.....X..'.0..tB.G...\;.a....4.....B4.....J.4.6.y:....4.-.UfE...3A*p.U5U X....Z.g:*e.j.C..Bw.....e..a^.vU:....$..U.....B..`._.e.....+...9.{u...7.e...H.]02...%yR".0...x...P<..N....R.}....{.G...;..c..x...kw.'S>.d|.....B..k.9.t.!>.rh...~n.[....s#/....`.!..Kb8% &.vZB`....O|.....>K.....L*...d0..03..t...T&.....`N.xp..".J.....Q.....c..5...).Z.91.6.j..G.....Wr...a.52!..(^.U.....6....dB.D.^...7..0H.\J9.H.$^`e"..d...\....B.8Z=.qeP.3Y.>..'W.X..T..>z ...,..K.....g....%B.w4#...;.[]u|....v...3.;L..U?..b.....u..*..... .....F...P.a...|R*3.=.....r.:.64...#D..^..>.A..ZT.]E.....t...f...1..3.....`...X.....C.]%...p.p.ym

C:\Users\user\AppData\Local\Temp\ZeTvTkc8PqqpWi0gm5JPfdt.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):	5564
Entropy (8bit):	7.903318556347248
Encrypted:	false
SSDEEP:	96:5WGzqeAoMq+YK0KF8cAJiI2i+u8/q9ajB5lfNlAyrEoq4y3KJ2:NqASpF8wF0alQqBy6J2
MD5:	045884CAC8190E44F7ABC2867D46807B
SHA1:	9B7FA398E1FE1FB3B5F027F094674BEA6B69F3BF
SHA-256:	24D8BBA77FD2B7E7E1FF88094B98394065B2E4C33AFE64FEC47329395DB8054F
SHA-512:	17E1E9DC4320F5872267390AF1DE2851614611DC62A75341798771A1F38BEDF0916D7727C57850194BA2EF15E9F5122CC8DC31AA395BE0B7ECBD4B7A66C6B5A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: C:\Users\user\AppData\Local\Temp\ZeTvTkc8PqqpWi0gm5JPfdt.zip, Author: Joe Security
Preview:	PK.....b`.X.....Cookies\..PK.....b`.XQn.+.....Cookies\Chrome_Default.txt.G..r...U.#.5C.....s$..-.D...7.\..$.G.)o....:....Z.C.f_..pm.....".t..t....}.k.@...a.2+ P`.0.x.>....s..k%.._..b..P..((.....B.....`.7..-m..JY..F....E.*.l.....I..&.....<J..M.....,V...)b.....Q..k.....M?.5L....h}.....X..'.0..tB.G...\;.a....4.....B4.....J.4.6.y:....4.-.UfE...3A*p.U5U X....Z.g:*e.j.C..Bw.....e..a^.vU:....$..U.....B..`._.e.....+...9.{u...7.e...H.]02...%yR".0...x...P<..N....R.}....{.G...;..c..x...kw.'S>.d|.....B..k.9.t.!>.rh...~n.[....s#/....`.!..Kb8% &.vZB`....O|.....>K.....L*...d0..03..t...T&.....`N.xp..".J.....Q.....c..5...).Z.91.6.j..G.....Wr...a.52!..(^.U.....6....dB.D.^...7..0H.\J9.H.$^`e"..d...\....B.8Z=.qeP.3Y.>..'W.X..T..>z ...,..K.....g....%B.w4#...;.[]u|....v...3.;L..U?..b.....u..*..... .....F...P.a...|R*3.=.....r.:.64...#D..^..>.A..ZT.]E.....t...f...1..3.....`...X.....C.]%...p.p.ym

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

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.7773627950641697
Encrypted:	false
SSDEEP:	3:LI8:Z8
MD5:	FDE07C3E6A4701AADF1451E07AC819DE
SHA1:	7C6F7BD99A9D5E7463A15CB16882F3D215352AEF
SHA-256:	5CD07F7CB46D77804C7AB2CC3036631E3340016D7978A913DEED0053587E1611
SHA-512:	BE51BE5F2DE955BEF34511538CE1E2FB2CDEDECD8DAB79582E28261827B00B8EA9ADD1DAF19597CBC148B039E96B082F2DA08EAB1A95DEB7C0517BD548A6B714
Malicious:	false
Preview:	1715514971206

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\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\span1kjtHrReFnXF\19u7ECnptzzlWeb 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):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\1_QlH4gDMSHgHistory

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UIYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+UI3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0
SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CBA
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\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):	0.037963276276857943
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWZWdgokBQNba9D3DO/JxW/QHI:58r54w0VW3xWZWdOBQFal3dQ
MD5:	C0FDF21AE11A6D1FA1201D502614B622

SHA1:	11724034A1CC915B061316A96E79E9DA6A00ADE8
SHA-256:	FD4EB46C81D27A9B3669C0D249DF5CE2B49E5F37B42F917CA38AB8831121ADAC
SHA-512:	A6147C196B033725018C7F28C1E75E20C2113A0C6D8172F5EABCB8FF334EA6CE10B758FFD1D22D50B4DB5A0A21BCC15294AC44E94D973F7A3EB9F8558F3176 B
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\span1kjtHrReFnXF\66rslgkYekRJHistory

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UIYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+UI3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0
SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\B087runuAKfxWeb 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):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3 EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\ByL8mAxGwSmaWeb Data

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false

Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\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):	0.037963276276857943
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWZWdgokBQNba9D3DO/JxW/QHI:58r54w0VW3xWZWdOBQFal3dQ
MD5:	C0FDF21AE11A6D1FA1201D502614B622
SHA1:	11724034A1CC915B061316A96E79E9DA6A00ADE8
SHA-256:	FD4EB46C81D27A9B3669C0D249DF5CE2B49E5F37B42F917CA38AB8831121ADAC
SHA-512:	A6147C196B033725018C7F28C1E75E20C2113A0C6D8172F5EABCB8FF334EA6CE10B758FFD1D22D50B4DB5A0A21BCC15294AC44E94D973F7A3EB9F8558F3176 B
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\span1kjtHrReFnXF\JhTxiIG1NfyxHistory

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE
SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F798 38
Malicious:	false
Preview:	SQLite format 3.....@ .....O}.....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\PJJYS_IpzF0mCookies

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 11, database pages 7, cookie 0x3, schema 4, UTF-8, version-valid-for 11
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.5793180405395284
Encrypted:	false
SSDEEP:	96:/xealJiylsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOI:/xGZR8wbtxq5uWRHKloIN7YItnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C278196210 3
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$.....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\azTbUSfG7fMXWeb Data	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\ctu1BJdlHpHIWeb Data	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\hxHjRwjYwPT3Login 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\span1kjtHrReFnXF\mHC5xGA2ZDf7Login 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\span1kjtHrReFnXF\otYgbid_VcgTLogin Data

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 1, database pages 24, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8180424350137764
Encrypted:	false
SSDEEP:	96:uRMKLyeymwxCn8MZyFlSynlbiXyKwt8hG:uRkxGOXnlbibhG
MD5:	349E6EB110E34A08924D92F6B334801D
SHA1:	BDFB289DAFF51890CC71697B6322AA4B35EC9169
SHA-256:	C9FD7BE4579E4AA942E8C2B44AB10115FA6C2FE6AFD0C584865413D9D53F3B2A
SHA-512:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC44574
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\rMqqLrP0489yHistory

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE
SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F79838
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\sYcixjslgY3sWeb 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):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622

SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....l.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\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\span7qiYjWFiJkre\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):	0.037963276276857943
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWZWdgokBQNba9D3DO/JxW/QHI:58r54w0VW3xWZWdOBQFal3dQ
MD5:	C0FDF21AE11A6D1FA1201D502614B622
SHA1:	11724034A1CC915B061316A96E79E9DA6A00ADE8
SHA-256:	FD4EB46C81D27A9B3669C0D249DF5CE2B49E5F37B42F917CA38AB8831121ADAC
SHA-512:	A6147C196B033725018C7F28C1E75E20C2113A0C6D8172F5EABCB8FF334EA6CE10B758FFD1D22D50B4DB5A0A21BCC15294AC44E94D973F7A3EB9F8558F3176B
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\span7qiYjWFiJkre\BdOSr6ULfsrrHistory

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE
SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F79838
Malicious:	false

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

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\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):	0.037963276276857943
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWZWdgokBQNba9D3DO/JxW/QHI:58r54w0VW3xWZWdOBQFal3dQ
MD5:	C0FDF21AE11A6D1FA1201D502614B622
SHA1:	11724034A1CC915B061316A96E79E9DA6A00ADE8
SHA-256:	FD4EB46C81D27A9B3669C0D249DF5CE2B49E5F37B42F917CA38AB8831121ADAC
SHA-512:	A6147C196B033725018C7F28C1E75E20C2113A0C6D8172F5EABCB8FF334EA6CE10B758FFD1D22D50B4DB5A0A21BCC15294AC44E94D973F7A3EB9F8558F3176 B
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\span7qiYjWFiJkre\HK3i7VEtGMBbWeb Data	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\ITZ0bicyJ58aHistory	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UlYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+UI3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0
SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j.....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\J0EAMZmTySltWeb Data	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4..... ....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\JsdnoRPI_10LHistory	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE
SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F798 38
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\SBUYXJCvH4fCWeb 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):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3 EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\TRbMB5IbyYCfLogin 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\span7qiYjWFiJkre_2Udgx0R4lC0Login 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\span7qiYjWFiJkre\fp5Zfw4ryWNTWeb 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):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\m78YdG3PG6psHistory

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UIYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+UI3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0

SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\rh5eReF6pk1JWeb Data	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4..... ....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\v8KCsYORX8h7Web 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):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3 EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\x6iuAgWaPHROLogin Data	
Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 1, database pages 24, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8180424350137764
Encrypted:	false
SSDEEP:	96:uRMKLyeymwxCn8MZyFlSynlbiXyKwt8hG:uRkxGOXnlbibhG
MD5:	349E6EB110E34A08924D92F6B334801D
SHA1:	BDFB289DAFF51890CC71697B6322AA4B35EC9169
SHA-256:	C9FD7BE4579E4AA942E8C2B44AB10115FA6C2FE6AFD0C584865413D9D53F3B2A
SHA-512:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4457 4
Malicious:	false

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

C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\zByDc7TM5G4BCookies

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 11, database pages 7, cookie 0x3, schema 4, UTF-8, version-valid-for 11
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.5793180405395284
Encrypted:	false
SSDEEP:	96:/xealJiylsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOI:/xGZR8wbtxq5uWRHKloIN7YItnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C278196213
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$.....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\02zdBXl47cvzcookies.sqlite

Process:	C:\Users\user\Desktop\file.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\spanr3JGE0E2FYa9\3b6N2Xdh3CYwplaces.sqlite

Process:	C:\Users\user\Desktop\file.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):	0.037963276276857943
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWZWdgokBQNba9D3DO/JxW/QHI:58r54w0VW3xWZWdOBQFal3dQ
MD5:	C0FDF21AE11A6D1FA1201D502614B622
SHA1:	11724034A1CC915B061316A96E79E9DA6A00ADE8
SHA-256:	FD4EB46C81D27A9B3669C0D249DF5CE2B49E5F37B42F917CA38AB8831121ADAC
SHA-512:	A6147C196B033725018C7F28C1E75E20C2113A0C6D8172F5EABCB8FF334EA6CE10B758FFD1D22D50B4DB5A0A21BCC15294AC44E94D973F7A3EB9F8558F31765B
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\spanr3JGE0E2FYa9\3vXQ9NJu865mWeb Data	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4..... ....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\4mK_R6tOoPGgWeb Data	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4..... ....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\C053a7OlzkOwHistory	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE
SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F798 38
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\D87fZN3R3jFeplaces.sqlite	
Process:	C:\Users\user\Desktop\file.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):	0.037963276276857943
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWZWdgokBQNba9D3DO/JxW/QHI:58r54w0VW3xWZWdOBQFal3dQ
MD5:	C0FDF21AE11A6D1FA1201D502614B622
SHA1:	11724034A1CC915B061316A96E79E9DA6A00ADE8
SHA-256:	FD4EB46C81D27A9B3669C0D249DF5CE2B49E5F37B42F917CA38AB8831121ADAC
SHA-512:	A6147C196B033725018C7F28C1E75E20C2113A0C6D8172F5EABCB8FF334EA6CE10B758FFD1D22D50B4DB5A0A21BCC15294AC44E94D973F7A3EB9F8558F3176 B
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\spanr3JGE0E2FYa9\DPh3g7VanZ0uLogin Data

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 1, database pages 24, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8180424350137764
Encrypted:	false
SSDEEP:	96:uRMKLyeymwxCn8MZyFlSynlbiXyKwt8hG:uRkxGOXnlbibhG
MD5:	349E6EB110E34A08924D92F6B334801D
SHA1:	BDFB289DAFF51890CC71697B6322AA4B35EC9169
SHA-256:	C9FD7BE4579E4AA942E8C2B44AB10115FA6C2FE6AFD0C584865413D9D53F3B2A
SHA-512:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4457 4
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\IdCNLqBK5BIzWeb Data

Process:	C:\Users\user\Desktop\file.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):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3 EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\JRPAhKRZ9ZTqHistory

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UIYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+UI3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0

SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\M4EU2Y_AAhWdWeb Data

Process:	C:\Users\user\Desktop\file.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):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3 EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\STqliTxIo5J7Login Data For Account

Process:	C:\Users\user\Desktop\file.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:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88 F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\ad9xHU1sHgxoWeb Data

Process:	C:\Users\user\Desktop\file.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):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3 EB
Malicious:	false

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

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\oUhaH1047Io5Login Data

Process:	C:\Users\user\Desktop\file.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\spanr3JGE0E2FYa9\opKyAgExHDMyCookies

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 11, database pages 7, cookie 0x3, schema 4, UTF-8, version-valid-for 11
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.5793180405395284
Encrypted:	false
SSDEEP:	96:/xealJiylsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOI:/xGZR8wbtxq5uWRHKloIN7Yltnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C2781962103
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$.....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\rakgGBowKZnMHistory

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UlYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+Ul3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0
SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CBA
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j.....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\sI5BW4MD5Iw7History

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE
SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F798 38
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Temp\spanr3JGE0E2FYa9\x7WOFKlgU8fPWeb Data

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4..... ....

C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\Cookies\Chrome_Default.txt

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	ASCII text, with very long lines (769), with CRLF line terminators
Category:	dropped
Size (bytes):	6085
Entropy (8bit):	6.038274200863744
Encrypted:	false
SSDEEP:	96:gxsumX/xKO2KbcRfbZJ5Jxjxcx1xcbza5BC126oxgxA26Fxr/CxbTxqCGYURxOeb:gWFXZQHRFJ5Pts7c3avC126Ygb6Lr/WY
MD5:	ACB5AD34236C58F9F7D219FB628E3B58
SHA1:	02E39404CA22F1368C46A7B8398F5F6001DB8F5C
SHA-256:	05E5013B848C2E619226F9E7A084DC7DCD1B3D68EE45108F552DB113D21B49D1
SHA-512:	5895F39765BA3CEDFD47D57203FD7E716347CD79277EDDCDC83A729A86E2E59F03F0E7B6B0D0E7C7A383755001EDACC82171052BE801E015E6BF7E6B959576 F
Malicious:	false
Preview:	.google.com.TRUE./.TRUE.1712145003.NID.ENC893*_djEw3+k+F2A/rK1XOX2BXUq6pY2LBCOzoXODiJnrrvDbDsPWiYwKZowg9PxHqkTm37HpwC52rXpnuUFrQMp V3iKtdSHegOm+XguZZ6tGaCY2hGVyR8JgIqQma1WLXyhCiWqjou7/c3qSeaKyNoUKHa4TULX4ZnNNtXFoCuZcBAAy4tYcz+0BF4j/0Pg+MgV+s7367kYcjO4q3zwc+Xorj Ss7PlgWlYrcc55rCJplhJ+H13M00HldLm+1t9PACck2xxSWX2DsA61sEDJCHEc=_b3i0u6LLcKCMUaF/UlQgEPSL9PtLZ21CuT1dJkfCzME=*..support.microsoft.c om.FALSE./.TRUE.1696413835..AspNetCore.AuthProvider.ENC893*_djEwVWJCCNyFkY3ZM/58ZZ/F/bz9H1yPvi6FOaroXC+KU8E=_b3i0u6LLcKCMUaF/UlQgE PSL9PtLZ21CuT1dJkfCzME=*..support.microsoft.com.TRUE./signin-oidc.TRUE.1696414135..AspNetCore.Correlation.mdRqPJxLbpyv7vX0eK9YkTR-xwcrW3VBLE 4Y3HEvxuU.ENC893*_djEwBAKLrkJs5PZ6BD7Beoa9N/bOSh5JtRch10gZT+E=_b3i0u6LLcKCMUaF/UlQgEPSL9PtLZ21CuT1dJkfCzME=*..support.microsoft.co m.TRUE./signin-oidc.TRUE.1696414135..AspNetCore.OpenIdConnect.Nonce.CfDJ8Kiuy_B5JgFMo7PeP95NLhqwcJ8koDy5pXkfoWsb5SbbU2hVCbsH2qt9GF _OVCqFkLEwhvzeADNQOF5RSmkDfh5RqfqlOkx5QWo4Lltvwb0CvwBFD8ujlm3BAglOeGca3ZatkLMUkH

C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\information.txt

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped

Size (bytes):	7024
Entropy (8bit):	5.405842873817507
Encrypted:	false
SSDEEP:	96:xfOCDCRencT4Aisph+9hcmYemgfhTme1LrXXZEAHRANUbg3x:xgwnvAtphWhcmLmgVJN6B
MD5:	ED318C125F614E4E075ADC28243FF285
SHA1:	DA53435D381FECB8236D3832C8E67A97117CCDB5
SHA-256:	F4B24F83A05A26FD0D263D50B116B6F9F45257AD3F859B2DB1C1799BB821ACEA
SHA-512:	DC202FBB60479376BE95D2617979EF51703BBD29738111E27B20708BABAFC6497F6DA539CAAEE9F9B705E3D93AEAAA0AD0E79BF12538E4832A9BF7E0C7B04FAB
Malicious:	false
Preview:	Build: tanos..Version: 2.0....Date: Sun May 12 12:03:03 2024.MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06..GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}..HWID: ee1dfe812e79685eafc5926398018eff....Path: C:\ProgramData\MPGPH131\MPGPH131.exe..Work Dir: C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF....IP: 81.181.60.11..Location: US, Seattle..ZIP (Autofills): -..Windows: Windows 10 Pro [x64]..Computer Name: 116938 [WORKGROUP]..User Name: user..Display Resolution: 1280x1024..Display Language: en-CH..Keyboard Languages: English (United Kingdom) / English (United Kingdom)..Local Time: 12/5/2024 12:3:3..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 [324]..csrss.exe [408]..wininit.exe [484]..csrss.exe [492]..winlogon.exe [552]..services.exe [620]..lsass.exe [628]..svchost.exe [752]..fontdrvhost.exe [776]..fontdrvhost.exe [784]..

C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\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:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\Cookies\Chrome_Default.txt

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	ASCII text, with very long lines (769), with CRLF line terminators
Category:	dropped
Size (bytes):	6085
Entropy (8bit):	6.038274200863744
Encrypted:	false
SSDEEP:	96:gxsumX/xKO2KbcRfbZJ5Jxjxcx1xcbza5BC126oxgxA26Fxr/CxbTxqCGYURxOeb:gWFXZQHRFJ5Pts7c3avC126Ygb6Lr/WY
MD5:	ACB5AD34236C58F9F7D219FB628E3B58
SHA1:	02E39404CA22F1368C46A7B8398F5F6001DB8F5C
SHA-256:	05E5013B848C2E619226F9E7A084DC7DCD1B3D68EE45108F552DB113D21B49D1
SHA-512:	5895F39765BA3CEDFD47D57203FD7E716347CD79277EDDCDC83A729A86E2E59F03F0E7B6B0D0E7C7A383755001EDACC82171052BE801E015E6BF7E6B959576F
Malicious:	false
Preview:	.google.com.TRUE./.TRUE.1712145003.NID.ENC893*_djEw3+k+F2A/rK1XOX2BXUq6pY2LBCOzoXODiJnrrvDbDsPWiYwKZowg9PxHqkTm37HpwC52rXpnuUFrQMpV3iKtdSHegOm+XguZZ6tGaCY2hGVyR8JgIqQma1WLXyhCiWqjou7/c3qSeaKyNoUKHa4TULX4ZnNNtXFoCuZcBAAy4tYcz+0BF4j/0Pg+MgV+s7367kYcjO4q3zwc+XorjSs7PlgWlYrcc55rCJplhJ+H13M00HldLm+1t9PACck2xxSWX2DsA61sEDJCHEc=_b3i0u6LLcKCMUaF/UlQgEPSL9PtLZ21CuT1dJkfCzME=*..support.microsoft.com.FALSE./.TRUE.1696413835..AspNetCore.AuthProvider.ENC893*_djEwVWJCCNyFkY3ZM/58ZZ/F/bz9H1yPvi6FOaroXC+KU8E=_b3i0u6LLcKCMUaF/UlQgEPSL9PtLZ21CuT1dJkfCzME=*..support.microsoft.com.TRUE./signin-oidc.TRUE.1696414135..AspNetCore.Correlation.mdRqPJxLbpyv7vX0eK9YkTR-xwcrW3VBLE4Y3HEvxuU.ENC893*_djEwBAKLrkJs5PZ6BD7Beoa9N/bOSh5JtRch10gZT+E=_b3i0u6LLcKCMUaF/UlQgEPSL9PtLZ21CuT1dJkfCzME=*..support.microsoft.com.TRUE./signin-oidc.TRUE.1696414135..AspNetCore.OpenIdConnect.Nonce.CfDJ8Kiuy_B5JgFMo7PeP95NLhqwcJ8koDy5pXkfoWsb5SbbU2hVCbsH2qt9GF_OVCqFkLEwhvzeADNQOF5RSmkDfh5RqfqlOkx5QWo4Lltvwb0CvwBFD8ujlm3BAglOeGca3ZatkLMUkH

C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\information.txt

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	7024
Entropy (8bit):	5.405300259476804

Encrypted:	false
SSDEEP:	96:xfO80lCReRcT4Aisph+9hcmYemgfhTme1LrXXZEAHRANUbg3x:xNwRvAtphWhcmLmgVJN6B
MD5:	B25F5DE46F5AFB6B4504680091AFC1A4
SHA1:	618E393F5DCEF7CB9DE6F0F642D24861AF86D0CC
SHA-256:	DEC8266FB7C00518CEBEFDE634EE3171A4E05EC1558203648EABD4301BD0BEC3
SHA-512:	6BCC657EDE9BE50AF34D0D3988EB9E77F332BFD63899578F0A8E95F1BDABA19CDFA6BF391366FDA49FEF36C2B0FED2AE46C27058DA66D4E6A8CE5CA009EF3B81
Malicious:	false
Preview:	Build: tanos..Version: 2.0....Date: Sun May 12 12:03:05 2024.MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06..GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}..HWID: ee1dfe812e79685eafc5926398018eff....Path: C:\ProgramData\MPGPH131\MPGPH131.exe..Work Dir: C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre....IP: 81.181.60.11..Location: US, Seattle..ZIP (Autofills): -..Windows: Windows 10 Pro [x64]..Computer Name: 116938 [WORKGROUP]..User Name: user..Display Resolution: 1280x1024..Display Language: en-CH..Keyboard Languages: English (United Kingdom) / English (United Kingdom)..Local Time: 12/5/2024 12:3:5..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 [324]..csrss.exe [408]..wininit.exe [484]..csrss.exe [492]..winlogon.exe [552]..services.exe [620]..lsass.exe [628]..svchost.exe [752]..fontdrvhost.exe [776]..fontdrvhost.exe [784]..

C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\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:\Users\user\AppData\Local\Temp\trixyr3JGE0E2FYa9\Cookies\Chrome_Default.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with very long lines (769), with CRLF line terminators
Category:	dropped
Size (bytes):	6085
Entropy (8bit):	6.038274200863744
Encrypted:	false
SSDEEP:	96:gxsumX/xKO2KbcRfbZJ5Jxjxcx1xcbza5BC126oxgxA26Fxr/CxbTxqCGYURxOeb:gWFXZQHRFJ5Pts7c3avC126Ygb6Lr/WY
MD5:	ACB5AD34236C58F9F7D219FB628E3B58
SHA1:	02E39404CA22F1368C46A7B8398F5F6001DB8F5C
SHA-256:	05E5013B848C2E619226F9E7A084DC7DCD1B3D68EE45108F552DB113D21B49D1
SHA-512:	5895F39765BA3CEDFD47D57203FD7E716347CD79277EDDCDC83A729A86E2E59F03F0E7B6B0D0E7C7A383755001EDACC82171052BE801E015E6BF7E6B959576F
Malicious:	false
Preview:	.google.com.TRUE./.TRUE.1712145003.NID.ENC893*_djEw3+k+F2A/rK1XOX2BXUq6pY2LBCOzoXODiJnrrvDbDsPWiYwKZowg9PxHqkTm37HpwC52rXpnuUFrQMpV3iKtdSHegOm+XguZZ6tGaCY2hGVyR8JgIqQma1WLXyhCiWqjou7/c3qSeaKyNoUKHa4TULX4ZnNNtXFoCuZcBAAy4tYcz+0BF4j/0Pg+MgV+s7367kYcjO4q3zwc+XorjSs7PlgWlYrcc55rCJplhJ+H13M00HIdLm+1t9PACck2xxSWX2DsA61sEDJCHEc=_b3i0u6LLcKCMUaF/UlQgEPSL9PtLZ21CuT1dJkfCzME=*..support.microsoft.com.FALSE./.TRUE.1696413835..AspNetCore.AuthProvider.ENC893*_djEwVWJCCNyFkY3ZM/58ZZ/F/bz9H1yPvi6FOaroXC+KU8E=_b3i0u6LLcKCMUaF/UlQgEPSL9PtLZ21CuT1dJkfCzME=*..support.microsoft.com.TRUE./signin-oidc.TRUE.1696414135..AspNetCore.Correlation.mdRqPJxLbpyv7vX0eK9YkTR-xwcrW3VBLE4Y3HEvxuU.ENC893*_djEwBAKLrkJs5PZ6BD7Beoa9N/bOSh5JtRch10gZT+E=_b3i0u6LLcKCMUaF/UlQgEPSL9PtLZ21CuT1dJkfCzME=*..support.microsoft.com.TRUE./signin-oidc.TRUE.1696414135..AspNetCore.OpenIdConnect.Nonce.CfDJ8Kiuy_B5JgFMo7PeP95NLhqwcJ8koDy5pXkfoWsb5SbbU2hVCbsH2qt9GF_OVCqFkLEwhvzeADNQOF5RSmkDfh5RqfqlOkx5QWo4Lltvwb0CvwBFD8ujlm3BAglOeGca3ZatkLMUkH

C:\Users\user\AppData\Local\Temp\trixyr3JGE0E2FYa9\information.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	7019
Entropy (8bit):	5.398038801982099
Encrypted:	false
SSDEEP:	96:xfOaGVOCRe6cT4Aisph+9hcmYemgfhTme1LrXXZEAHRANUbg3x:xjmw6vAtphWhcmLmgVJN6B

MD5:	64E3C5506DC469A135FFD609CB2756FF
SHA1:	60844CBA7C9DD72837A6A76114E037E4ED209A11
SHA-256:	12A961781BA5C671E31DE2E7D12E8958989F94E377ADB047A8554D5477A9CD34
SHA-512:	622C9EA60B194A0A84F55A8D2830CCA375BFFF65A98D0A63FCF577BA4774228F7C085056BB3CD361DB40F72B479CDDC6046A3C975E652F8AA2E0F7AB3C8707F
Malicious:	false
Preview:	Build: tanos..Version: 2.0....Date: Sun May 12 12:03:02 2024.MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06..GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}..HWID: ee1dfe812e79685eafc5926398018eff....Path: C:\Users\user\Desktop\file.exe..Work Dir: C:\Users\user\AppData\Local\Temp\trixyr3JGE0E2FYa9....IP: 81.181.60.11..Location: US, Seattle..ZIP (Autofills): -..Windows: Windows 10 Pro [x64]..Computer Name: 116938 [WORKGROUP]..User Name: user..Display Resolution: 1280x1024..Display Language: en-CH..Keyboard Languages: English (United Kingdom) / English (United Kingdom)..Local Time: 12/5/2024 12:3:2..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 [324]..csrss.exe [408]..wininit.exe [484]..csrss.exe [492]..winlogon.exe [552]..services.exe [620]..lsass.exe [628]..svchost.exe [752]..fontdrvhost.exe [776]..fontdrvhost.exe [784]..svcho

C:\Users\user\AppData\Local\Temp\trixyr3JGE0E2FYa9\passwords.txt	
Process:	C:\Users\user\Desktop\file.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:	48:4MMMMMMMMMMdMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMMMdMMMMMMMM3: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):	4.46902234255053
Encrypted:	false
SSDEEP:	6144:aIXfpi67eLPU9skLmb0b4fWSPKaJG8nAgejZMMhA2gX4WABl0uN2dwBCswSba:vXD94fWILZMM6YFHU+a
MD5:	ED2CDB80556696E79FEA0B0476130ECF
SHA1:	DB571940C5DE335ADFED1583AD02F21196061878
SHA-256:	4804864D288172513D87F51A6F54E4DA20BDB24ABDFCA550A8FBB8FB0F7B211D
SHA-512:	44CBF02759361376E20C408A0AA833CF28E28E958BBE3480DE41B8A7741DF9FC3B441E04974F8DCE4E4B01BF2C8630E12F715DA56AAE29816987D0850AC4FCCA
Malicious:	false
Preview:	regf6...6....\.Z..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e....c...b...#.....c...b...#.....c...b...#.....rmtm..K.S..... .....s\.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.9780906837515655
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:	file.exe
File size:	3'241'984 bytes
MD5:	72007357beb74fea20e7daa285212b16

SHA1:	e37f50ace578fc3a69fb7a312a659d51491e32b0
SHA256:	6a1bda6fa37b02776b44c80fc1d8329bd7fbd49ff46eaf37346e5c436a52ec9e
SHA512:	72a731a1f9dfa6e927665bb5649420a1114fecaac6e7e30ccda9028f37c1e6de582e0f237f5a95cd012603b916c19aa31582729fcbc3d86db4a2c4b96d6acc4e
SSDEEP:	98304:0y5rnbPr5he+zDgy3yQ7rDnI19mQxWaF67:0ADbPDQyCErDI19mQxvF6
TLSH:	1AE533A9C30694BAD74EDEFFDA6094BF043FDDE87AC0E443660128875C75A94383A479
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:	0xf743b0
Entrypoint Section:	.data
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, TERMINAL_SERVER_AWARE
Time Stamp:	0x663B526A [Wed May 8 10:22:34 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:	272279f18f704f637aa129691266b291

Entrypoint Preview

Instruction
jmp 00007F1AE8EA10CAh
add byte ptr [esi+0000000Eh], bl
add byte ptr [eax], al
pushad
call 00007F1AE8EA10C5h
pop ebp
sub ebp, 00000010h
sub ebp, 00B743B0h
jmp 00007F1AE8EA10C9h
mov esi, B809D96Dh
mov al, 43h
mov bh, 00h
add eax, ebp
add eax, 0000004Ch
mov ecx, 000005A7h
mov edx, 6FC513ACh
xor byte ptr [eax], dl
inc eax
dec ecx
jne 00007F1AE8EA10BCh
jmp 00007F1AE8EA10C9h
pop ss
or al, 61h

Instruction
pop ds
daa
popad
daa
and eax, ACACAC90h
sub eax, ACAC546Dh
lodsb
scasd
popad
adc al, AAh
lodsb
lodsb
lodsb
push ss
test byte ptr [esp+ebp*4-50B1A454h], ch
daa
sub eax, ACACACA0h
scasd
imul edi, esp, A3B8C4FCh
mov gs, word ptr [esp+eax*8-53C667D0h]
lodsd
or byte ptr [eax+4D08BDC4h], 00000003h
inc esp
test eax, 45ACACACh
call far 88C8h : 21ACACACh
push eax
and eax, C0218880h
mov byte ptr [edi-53535BD7h], ch
lodsb
daa
cmp dword ptr [eax+27ACACACh], esp
and dword ptr [esp+ebp*4+456DACACh], edi
scasb
popfd
scasb
das
outsb
test al, E5h
mov dword ptr [53535829h], eax
push ebx
daa
or byte ptr [eax-577737DFh], 0000006Eh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x94b050	0xe1e	.data
IMAGE_DIRECTORY_ENTRY_IMPORT	0x94be70	0x3b0	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a1000	0xc8bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x94b030	0x10	.data
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x94b000	0x18	.data
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	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x15c000	0x93c00	fb91b7bd755d7edf5f38440588fdf254	False	0.9999917380499154	data	7.999642093451103	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
	0x15d000	0x28000	0x10200	9a2d1dbb2ecdca4d0d0e514e8aea6c29	False	0.9983345445736435	data	7.99632844124323	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
	0x185000	0x5000	0x800	ed435fb29d4a6ca60e5cf9de6ea89b30	False	0.99658203125	data	7.827423983071036	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
	0x18a000	0xd000	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
	0x197000	0xa000	0x6200	753317f0f9bdce2beaa1559920682af2	False	0.9880022321428571	OpenPGP Public Key	7.973813310249681	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x1a1000	0xd000	0xca00	6e46563fc615b7272cc3ab7b669e3874	False	0.6000541460396039	data	5.556770173829542	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x1ae000	0x79a000	0x32800	8a2ee6a3dca387fe01edde34bddc02b2	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.data	0x948000	0x22e000	0x22da00	d062e04b8091a4fdaa89a7bd870c306a	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x1a1370	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	Russian	Russia	0.31402439024390244
RT_ICON	0x1a19d8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	Russian	Russia	0.42338709677419356
RT_ICON	0x1a1cc0	0x1e8	Device independent bitmap graphic, 24 x 48 x 4, image size 288	Russian	Russia	0.5061475409836066
RT_ICON	0x1a1ea8	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	Russian	Russia	0.5675675675675675

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x1a1fd0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Russian	Russia	0.46961620469083154
RT_ICON	0x1a2e78	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Russian	Russia	0.4020758122743682
RT_ICON	0x1a3720	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Russian	Russia	0.45506912442396313
RT_ICON	0x1a3de8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Russian	Russia	0.2904624277456647
RT_ICON	0x1a4350	0x4b55	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	Russian	Russia	0.9921182266009853
RT_ICON	0x1a8ea8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Russian	Russia	0.316701244813278
RT_ICON	0x1ab450	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Russian	Russia	0.36186679174484054
RT_ICON	0x1ac4f8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Russian	Russia	0.42418032786885246
RT_ICON	0x1ace80	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Russian	Russia	0.5026595744680851
RT_GROUP_ICON	0x1ad2e8	0xbc	data	Russian	Russia	0.6170212765957447
RT_VERSION	0x1ad3a4	0x398	OpenPGP Public Key	Russian	Russia	0.42282608695652174
RT_MANIFEST	0x1ad73c	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States	0.5931758530183727

Imports

DLL	Import
kernel32.dll	GetModuleHandleA, GetProcAddress, ExitProcess, LoadLibraryA
user32.dll	MessageBoxA
advapi32.dll	RegCloseKey
oleaut32.dll	SysFreeString
gdi32.dll	CreateFontA
shell32.dll	ShellExecuteA
version.dll	GetFileVersionInfoA
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

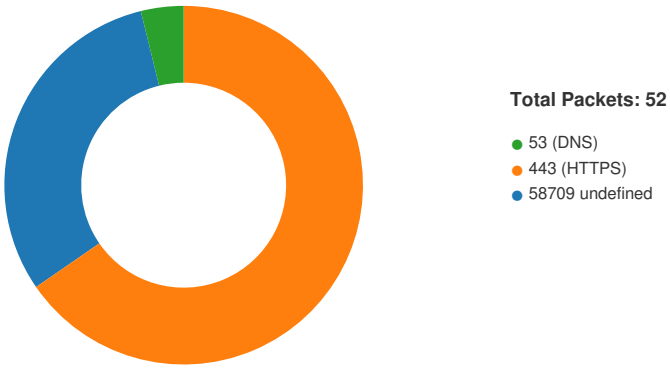
Language of compilation system	Country where language is spoken	Map
Russian	Russia	
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/24-12:02:58.333893	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49731	147.45.47.126	192.168.2.4
05/12/24-12:02:56.237225	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49730	147.45.47.126	192.168.2.4
05/12/24-12:02:57.482973	TCP	2046267	ET TROJAN [ANY.RUN] RisePro TCP (External IP)	58709	49730	147.45.47.126	192.168.2.4
05/12/24-12:02:58.992753	TCP	2046267	ET TROJAN [ANY.RUN] RisePro TCP (External IP)	58709	49731	147.45.47.126	192.168.2.4
05/12/24-12:03:17.954872	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49751	147.45.47.126	192.168.2.4
05/12/24-12:03:05.358724	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49730	58709	192.168.2.4	147.45.47.126
05/12/24-12:03:06.218564	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49731	58709	192.168.2.4	147.45.47.126
05/12/24-12:03:11.796109	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49739	58709	192.168.2.4	147.45.47.126
05/12/24-12:03:08.562034	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49736	58709	192.168.2.4	147.45.47.126
05/12/24-12:03:00.933956	TCP	2046267	ET TROJAN [ANY.RUN] RisePro TCP (External IP)	58709	49736	147.45.47.126	192.168.2.4
05/12/24-12:03:07.984400	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49739	147.45.47.126	192.168.2.4
05/12/24-12:03:00.497224	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49736	147.45.47.126	192.168.2.4
05/12/24-12:02:55.911761	TCP	2049060	ET TROJAN RisePro TCP Heartbeat Packet	49730	58709	192.168.2.4	147.45.47.126

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2024 12:02:55.567120075 CEST	49730	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:55.901746035 CEST	58709	49730	147.45.47.126	192.168.2.4
May 12, 2024 12:02:55.901832104 CEST	49730	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:55.911761045 CEST	49730	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:56.237225056 CEST	58709	49730	147.45.47.126	192.168.2.4
May 12, 2024 12:02:56.280395985 CEST	49730	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:56.297790051 CEST	58709	49730	147.45.47.126	192.168.2.4
May 12, 2024 12:02:57.482973099 CEST	58709	49730	147.45.47.126	192.168.2.4
May 12, 2024 12:02:57.530386925 CEST	49730	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:57.664839983 CEST	49731	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:57.792654991 CEST	49732	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:57.792689085 CEST	443	49732	34.117.186.192	192.168.2.4
May 12, 2024 12:02:57.792752028 CEST	49732	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:57.796406031 CEST	49732	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:57.796420097 CEST	443	49732	34.117.186.192	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2024 12:02:57.865272999 CEST	58709	49730	147.45.47.126	192.168.2.4
May 12, 2024 12:02:57.865392923 CEST	49730	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:57.999320030 CEST	58709	49731	147.45.47.126	192.168.2.4
May 12, 2024 12:02:57.999427080 CEST	49731	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:58.020725012 CEST	49731	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:58.132184029 CEST	443	49732	34.117.186.192	192.168.2.4
May 12, 2024 12:02:58.132307053 CEST	49732	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:58.134747982 CEST	49732	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:58.134756088 CEST	443	49732	34.117.186.192	192.168.2.4
May 12, 2024 12:02:58.134980917 CEST	443	49732	34.117.186.192	192.168.2.4
May 12, 2024 12:02:58.182138920 CEST	49732	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:58.228116989 CEST	443	49732	34.117.186.192	192.168.2.4
May 12, 2024 12:02:58.250719070 CEST	58709	49730	147.45.47.126	192.168.2.4
May 12, 2024 12:02:58.333893061 CEST	58709	49731	147.45.47.126	192.168.2.4
May 12, 2024 12:02:58.374147892 CEST	49731	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:58.407111883 CEST	58709	49731	147.45.47.126	192.168.2.4
May 12, 2024 12:02:58.516396046 CEST	443	49732	34.117.186.192	192.168.2.4
May 12, 2024 12:02:58.516508102 CEST	443	49732	34.117.186.192	192.168.2.4
May 12, 2024 12:02:58.516649961 CEST	49732	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:58.519298077 CEST	49732	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:58.519311905 CEST	443	49732	34.117.186.192	192.168.2.4
May 12, 2024 12:02:58.519323111 CEST	49732	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:58.519328117 CEST	443	49732	34.117.186.192	192.168.2.4
May 12, 2024 12:02:58.687388897 CEST	49733	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:58.687406063 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:58.687486887 CEST	49733	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:58.687800884 CEST	49733	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:58.687812090 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:58.992753029 CEST	58709	49731	147.45.47.126	192.168.2.4
May 12, 2024 12:02:59.024753094 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.024858952 CEST	49733	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:59.027000904 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.027028084 CEST	443	49734	34.117.186.192	192.168.2.4
May 12, 2024 12:02:59.027089119 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.027559996 CEST	49733	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:59.027569056 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.027791023 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.028342962 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.028353930 CEST	443	49734	34.117.186.192	192.168.2.4
May 12, 2024 12:02:59.028790951 CEST	49733	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:59.046000957 CEST	49731	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:59.076117992 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.359721899 CEST	443	49734	34.117.186.192	192.168.2.4
May 12, 2024 12:02:59.359857082 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.361188889 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.361196995 CEST	443	49734	34.117.186.192	192.168.2.4
May 12, 2024 12:02:59.361430883 CEST	443	49734	34.117.186.192	192.168.2.4
May 12, 2024 12:02:59.405425072 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.406560898 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.452124119 CEST	443	49734	34.117.186.192	192.168.2.4
May 12, 2024 12:02:59.471086025 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.471167088 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.471221924 CEST	49733	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:59.471395969 CEST	49733	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:59.471414089 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.471421957 CEST	49733	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:59.471431017 CEST	443	49733	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.477407932 CEST	49730	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:59.737987995 CEST	443	49734	34.117.186.192	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2024 12:02:59.738090992 CEST	443	49734	34.117.186.192	192.168.2.4
May 12, 2024 12:02:59.738152027 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.738424063 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.738440037 CEST	443	49734	34.117.186.192	192.168.2.4
May 12, 2024 12:02:59.738456964 CEST	49734	443	192.168.2.4	34.117.186.192
May 12, 2024 12:02:59.738464117 CEST	443	49734	34.117.186.192	192.168.2.4
May 12, 2024 12:02:59.758518934 CEST	49735	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:59.758541107 CEST	443	49735	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.758618116 CEST	49735	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:59.758980036 CEST	49735	443	192.168.2.4	104.26.5.15
May 12, 2024 12:02:59.758991003 CEST	443	49735	104.26.5.15	192.168.2.4
May 12, 2024 12:02:59.826524019 CEST	49736	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:02:59.860637903 CEST	58709	49730	147.45.47.126	192.168.2.4
May 12, 2024 12:02:59.913671970 CEST	58709	49730	147.45.47.126	192.168.2.4
May 12, 2024 12:02:59.946177006 CEST	49730	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:03:00.048217058 CEST	58709	49731	147.45.47.126	192.168.2.4
May 12, 2024 12:03:00.048409939 CEST	49731	58709	192.168.2.4	147.45.47.126
May 12, 2024 12:03:00.091185093 CEST	443	49735	104.26.5.15	192.168.2.4
May 12, 2024 12:03:00.091243982 CEST	49735	443	192.168.2.4	104.26.5.15
May 12, 2024 12:03:00.092709064 CEST	49735	443	192.168.2.4	104.26.5.15
May 12, 2024 12:03:00.092717886 CEST	443	49735	104.26.5.15	192.168.2.4
May 12, 2024 12:03:00.092943907 CEST	443	49735	104.26.5.15	192.168.2.4
May 12, 2024 12:03:00.094624996 CEST	49735	443	192.168.2.4	104.26.5.15
May 12, 2024 12:03:00.136125088 CEST	443	49735	104.26.5.15	192.168.2.4
May 12, 2024 12:03:00.161361933 CEST	58709	49736	147.45.47.126	192.168.2.4
May 12, 2024 12:03:00.161461115 CEST	49736	58709	192.168.2.4	147.45.47.126

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2024 12:02:57.623099089 CEST	58839	53	192.168.2.4	1.1.1.1
May 12, 2024 12:02:57.786385059 CEST	53	58839	1.1.1.1	192.168.2.4
May 12, 2024 12:02:58.521739006 CEST	58316	53	192.168.2.4	1.1.1.1
May 12, 2024 12:02:58.686448097 CEST	53	58316	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 12, 2024 12:02:57.623099089 CEST	192.168.2.4	1.1.1.1	0xb47	Standard query (0)	ipinfo.io	A (IP address)	IN (0x0001)	false
May 12, 2024 12:02:58.521739006 CEST	192.168.2.4	1.1.1.1	0x257c	Standard query (0)	db-ip.com	A (IP address)	IN (0x0001)	false

DNS Answers

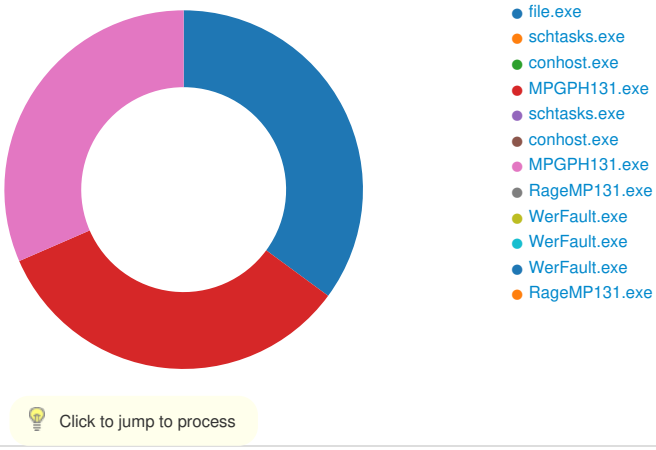
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 12, 2024 12:02:57.786385059 CEST	1.1.1.1	192.168.2.4	0xb47	No error (0)	ipinfo.io		34.117.186.192	A (IP address)	IN (0x0001)	false
May 12, 2024 12:02:58.686448097 CEST	1.1.1.1	192.168.2.4	0x257c	No error (0)	db-ip.com		104.26.5.15	A (IP address)	IN (0x0001)	false
May 12, 2024 12:02:58.686448097 CEST	1.1.1.1	192.168.2.4	0x257c	No error (0)	db-ip.com		172.67.75.166	A (IP address)	IN (0x0001)	false
May 12, 2024 12:02:58.686448097 CEST	1.1.1.1	192.168.2.4	0x257c	No error (0)	db-ip.com		104.26.4.15	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **744**, Parent PID: **2580**

General

Target ID:	0
Start time:	12:02:51
Start date:	12/05/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0xbb0000
File size:	3'241'984 bytes
MD5 hash:	72007357BEB74FEA20E7DAA285212B16
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000002.2017190533.00000000018FE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PrivateLoader, Description: Yara detected PrivateLoader, Source: 00000000.00000002.2015608699.0000000000BB1000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.2016612734.00000000018C4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000003.1754759356.00000000018FE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	RageMP131	unicode	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe	success or wait	1	C7FEDF	RegSetValueExA

Analysis Process: schtasks.exe PID: **1368**, Parent PID: **744**

General

Target ID:	1
Start time:	12:02:54
Start date:	12/05/2024
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:	0x510000
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: **1704**, Parent PID: **1368**

General

Target ID:	2
Start time:	12:02:54
Start date:	12/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: MPGPH131.exe PID: **1436**, Parent PID: **1044**

General

Target ID:	3
Start time:	12:02:54
Start date:	12/05/2024
Path:	C:\ProgramData\MPGPH131\MPGPH131.exe

Wow64 process (32bit):	true
Commandline:	C:\ProgramData\MPGPH131\MPGPH131.exe
Imagebase:	0xf00000
File size:	3'241'984 bytes
MD5 hash:	72007357BEB74FEA20E7DAA285212B16
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000003.00000002.2026410193.0000000000ABF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000003.00000002.2025872612.00000000009AD000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PrivateLoader, Description: Yara detected PrivateLoader, Source: 00000003.00000002.2026784616.0000000000F01000.00000040.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000003.00000003.1763214228.0000000000ABF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 47%, ReversingLabs • Detection: 59%, Virustotal, Browse
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\trixy1kjtHrReFnXF	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\span1kjtHrReFnXF	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\span1kjtHrReFnXF\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\span1kjtHrReFnXF\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\span1kjtHrReFnXF\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\span1kjtHrReFnXF\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\span1kjtHrReFnXF\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 Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\mHC5xGA2ZDf7Login 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\span1kjtHrReFnXF\hxHjRwjYwPT3Login 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\span1kjtHrReFnXF\B087runuAKfxWeb 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\span1kjtHrReFnXF\66rslgkYekRJHistory	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\span1kjtHrReFnXF\sYcixjslgY3sWeb 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\span1kjtHrReFnXF\mba9gPQiNkwLCookies	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\span1kjtHrReFnXF\PJJYS_IpzF0mCookies	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\span1kjtHrReFnXF\1_QlH4gDMSHgHistory	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\span1kjtHrReFnXF\19u7ECnptzzlWeb 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\span1kjtHrReFnXF\otYgbid_VcgTLogin 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\span1kjtHrReFnXF\8J4SxneIDllbLogin 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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\ByL8mAxGwSmaWeb 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\span1kjtHrReFnXF\rMqqLrP0489yHistory	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\span1kjtHrReFnXF\azTbUSfG7fMXWeb 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\span1kjtHrReFnXF\1WS737_IECbpCookies	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\span1kjtHrReFnXF\JhTxiIG1NfyxHistory	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\span1kjtHrReFnXF\ctu1BJdIHpHIWeb 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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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\8klzCUsmQMVYazLTWo6KoKU.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\span1kjtHrReFnXF\Ei8DrAmaYu9Ksignons.sqlite	success or wait	2	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\D87fZN3R3jFeplaces.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\02zdBXl47cvzcookies.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\mHC5xGA2ZDf7Login Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\hxHjRwjYwPT3Login Data For Account	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\B087runuAKfxWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\66rslgkYekRJHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\sYcixjslgY3sWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\mba9gPQiNkwLCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\PJJYS_lpzF0mCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\1_QlH4gDMSHgHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\19u7ECnptzzlWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\otYgbid_VcgTLogin Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\8J4SxneIDIlbLogin Data For Account	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\ByL8mAxGwSmaWeb Data	success or wait	1	F4B9DE	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\rMqqLrP0489yHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\azTbUSfG7fMXWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\1WS737_IECbpCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\JhTxiIG1NfyxHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\ctu1BJdIHpHIWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\8klzCUsmQMVYazLTWo6KoKU.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 35 31 34 39 37 31 32 30 36	1715514971206	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\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	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAsqpqp{ooh nnemn,m9lklPjjhhgdcc6bbaa>	success or wait	10	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\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	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\span1kjtHrReFnXF\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	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAsqpqp{ooh nnemn,m9lklPjjhhgdcc6bbaa>	success or wait	10	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\mHC5xGA2ZDf7Login 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 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\span1kjtHrReFnXF\hxHjRwjYwPT3Login 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 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	SQLite format 3@ .j	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\B087runuAKfxWeb 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 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	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\span1kjtHrReFnXF\66rslgkYekRJHistory	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 04 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 04 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	SQLite format 3@ ' .j	success or wait	2	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\sYcixjslgY3sWeb 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	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\span1kjtHrReFnXF\PJJYS_lpzF0mCookies	0	28672	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 0b 00 00 00 07 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 0b 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 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\span1kjtHrReFnXF\1_QlH4gDMSHgHistory	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 04 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 04 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 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\span1kjtHrReFnXF\19u7ECnptzzlWeb 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	SQLite format 3@ 4!.j1	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\otYgbid_VcgTLogin Data	0	49152	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 18 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 01 00 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 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	SQLite format 3@ .O}	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\ByL8mAxGwSmaWeb Data	0	114688	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 38 00 00 00 00 00 00 00 00 00 00 00 24 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 4f 7d 05 00 00 00 05 07 fd 00 00 00 00 34 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	SQLite format 3@ 8$.O}4	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\rMqqLrP0489yHistory	0	126976	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 02 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 18 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 4f 7d 05 00 00 00 01 0f fd 00 00 00 00 1c 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 00 00	SQLite format 3@ .O}	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\azTbUSfG7fMXWeb Data	0	114688	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 38 00 00 00 00 00 00 00 00 00 00 00 24 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 4f 7d 05 00 00 00 05 07 fd 00 00 00 00 34 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	SQLite format 3@ 8$.O}4	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\JhTxiIG1NfyxHistory	0	126976	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 02 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 18 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 4f 7d 05 00 00 00 01 0f fd 00 00 00 00 1c 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@ .O}	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\ctu1BJdIHpHIWeb Data	0	114688	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 38 00 00 00 00 00 00 00 00 00 00 00 24 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 02 00 2e 4f 7d 05 00 00 00 05 07 fd 00 00 00 00 34 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	SQLite format 3@ 8$.O}4	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\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\trixy1kjtHrReFnXF\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 0d 0a 00 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\trixy1kjtHrReFnXF\Cookies\Chrome_Default.txt	0	4096	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 31 34 35 30 30 33 09 4e 49 44 09 45 4e 43 38 39 33 2a 5f 64 6a 45 77 33 2b 6b 2b 46 32 41 2f 72 4b 31 58 4f 58 32 42 58 55 71 36 70 59 32 4c 42 43 4f 7a 6f 58 4f 44 69 4a 6e 72 72 76 44 62 44 73 50 57 69 59 77 4b 5a 6f 77 67 39 50 78 48 71 6b 54 6d 33 37 48 70 77 43 35 32 72 58 70 6e 75 55 46 72 51 4d 70 56 33 69 4b 74 64 53 48 65 67 4f 6d 2b 58 67 75 5a 5a 36 74 47 61 43 59 32 68 47 56 79 52 38 4a 67 49 71 51 6d 61 31 57 4c 58 79 68 43 69 57 71 6a 6f 75 37 2f 63 33 71 53 65 61 4b 79 4e 6f 55 4b 48 61 34 54 55 4c 58 34 5a 6e 4e 4e 74 58 46 6f 43 75 5a 63 42 41 41 79 34 74 59 63 7a 2b 30 42 46 34 6a 2f 30 50 67 2b 4d 67 56 2b 73 37 33 36 37 6b 59 63 6a 4f 34 71 33 7a 77 63	.google.comTRUE/TRUE 1712145003 NIDENC893*_djEw3+k+F 2A/rK1XOX2 BXUq6pY2LBCOzoXODi JnrrvDbDsPWi YwKZowg9PxHqkTm37H pwC52rXpnuUF rQMpV3iKtdSHegOm+Xg uZZ6tGaCY2h GVyR8JgIqQma1WLXyh CiWqjou7/c3q SeaKyNoUKHa4TULX4Z nNNtXFoCuZcB AAy4tYcz+0BF4j/0Pg+M gV+s7367kYcjO4q3zwc	success or wait	1	F49914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\Cookies\Chrome_Default.txt	4096	1989	63 61 74 69 6f 6e 73 54 65 6c 65 6d 65 74 72 79 44 65 76 69 63 65 49 64 09 45 4e 43 38 39 33 2a 5f 64 6a 45 77 2f 45 50 6b 73 54 6e 42 6d 4d 42 45 51 71 53 30 72 6d 71 6c 78 36 5a 59 62 62 70 49 6d 4d 73 63 6d 66 75 6b 6c 38 56 32 66 79 68 47 66 36 43 73 52 79 4f 72 51 41 52 6e 6c 72 75 4e 75 63 57 4c 6e 38 62 58 62 75 37 2b 72 4d 77 72 78 45 6a 48 41 49 37 33 58 77 3d 3d 5f 62 33 69 30 75 36 4c 4c 63 4b 43 4d 55 61 46 2f 55 6c 51 67 45 50 53 4c 39 50 74 4c 5a 32 31 43 75 54 31 64 4a 6b 66 43 7a 4d 45 3d 2a 0d 0a 2e 63 2e 62 69 6e 67 2e 63 6f 6d 09 46 41 4c 53 45 09 2f 09 54 52 55 45 09 31 37 33 30 31 30 39 32 38 31 09 53 52 4d 5f 42 09 45 4e 43 38 39 33 2a 5f 64 6a 45 77 37 6d 56 46 74 59 35 63 5a 42 6d 63 53 49 64 39 6f 2b 4c 4f 36 70 59 78 5a 47 66 65	cationsTelemetryDeviceIdENC893*_djEw/EPksTnBmMBEQqS0rmqlx6ZYbbplmMscmfukl8V2fyhGf6CsRyOrQARnlruNucWLn8bXbu7+rMwrxEjHAI73Xw==_b3i0u6LLcKCMUaF/UlQgEPSL9PtLZ21CuT1dJkfCzME=*.c.bing.comFALSE/TRUE1730109281SRM_BENC893*_djEw7mVFtY5cZBmcSId9o+LO6pYxZGfe	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\information.txt	0	4096	42 75 69 6c 64 3a 20 74 61 6e 6f 73 0d 0a 56 65 72 73 69 6f 6e 3a 20 32 2e 30 0d 0a 0d 0a 44 61 74 65 3a 20 53 75 6e 20 4d 61 79 20 31 32 20 31 32 3a 30 33 3a 30 33 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 65 65 31 64 66 65 38 31 32 65 37 39 36 38 35 65 61 66 63 35 39 32 36 33 39 38 30 31 38 65 66 66 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: tanosVersion: 2.0Date: Sun May 12 12:03:03 2024MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}HWID: ee1dfe812e79685eafc5926398018effPath: 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\trixy1kjtHrReFnXF\information.txt	4096	2928	6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 31 30 31 36 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 38 30 38 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 31 35 36 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 31 32 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 34 33 34 38 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 34 34 31 32 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a	nDJLELYssjayClc.exe [1016]zDTa rlxjDyChCjnDJLELYssjay Clc.exe [3808]zDTarlxjDyChCjnD JLELYssjayClc.exe [3156]zDTarlxjDyChCj nDJLELYssjayClc.exe [3512]zDTa rlxjDyChCjnDJLELYssjay Clc.exe [4348]zDTarlxjDyChCjnD JLELYssjayClc.exe [4412]zDTarlxjDyChCj nDJ	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\information.txt	0	4096	42 75 69 6c 64 3a 20 74 61 6e 6f 73 0d 0a 56 65 72 73 69 6f 6e 3a 20 32 2e 30 0d 0a 0d 0a 44 61 74 65 3a 20 53 75 6e 20 4d 61 79 20 31 32 20 31 32 3a 30 33 3a 30 33 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 65 65 31 64 66 65 38 31 32 65 37 39 36 38 35 65 61 66 63 35 39 32 36 33 39 38 30 31 38 65 66 66 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: tanosVersion: 2.0Date: Sun May 12 12:03:03 2024Machin eID: 9e146be9-c76a-4720-bcdb-5 3011b87bd06GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}HWID: ee1dfe812e79685eafc592 6398018effPath: C:\ProgramData\MPGPH 1 31\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\trixy1kjtHrReFnXF\information.txt	4096	2928	6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 31 30 31 36 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 38 30 38 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 31 35 36 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 31 32 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 34 33 34 38 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 34 34 31 32 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a	nDJLELYssjayClc.exe [1016]zDTa rlxjDyChCjnDJLELYssjay Clc.exe [3808]zDTarlxjDyChCjnD JLELYssjayClc.exe [3156]zDTarlxjDyChCj nDJLELYssjayClc.exe [3512]zDTa rlxjDyChCjnDJLELYssjay Clc.exe [4348]zDTarlxjDyChCjnD JLELYssjayClc.exe [4412]zDTarlxjDyChCj nDJ	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\8klzCUsmQMVYazLTWo6KoKU.zip	0	40	50 4b 03 04 14 00 00 08 08 00 61 60 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	PKa`XCookies\	success or wait	4	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\8klzCUsmQMVYazLTWo6KoKU.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\8klzCUsmQMVYazLTWo6KoKU.zip	5248	314	50 4b 01 02 00 0b 14 00 00 08 08 00 61 60 fd 58 00 00 00 00 02 00 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 43 6f 6f 6b 69 65 73 5c 50 4b 01 02 00 0b 14 00 00 08 08 00 61 60 fd 58 51 6e fd 2b fd 0b 00 00 fd 17 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 61 60 fd 58 fd 28 fd fd fd 06 00 00 70 1b 00 00 0f 00 00 00 00 00 00 00 01 00 00 00 00 00 55 0c 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 61 60 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 54 13 00 00 70 61 73 73 77 6f 72 64 73 2e 74 78 74 50 4b 05 06 00 00 00 00 04	PKa`XCookies\PKa`XQn +(Cookies\ Chrome_Default.txtPKa` X(pUinfo rmation.txtPKa`XF!Tpass words.txtPK	success or wait	1	F49914	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\MPGPH131\MPGPH131.exe	0	64	success or wait	1	110E562	NtReadFile
C:\ProgramData\MPGPH131\MPGPH131.exe	0	20	success or wait	1	110E562	NtReadFile
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\span1kjtHrReFnXF\Ei8DrAmaYu9Ksignons.sqlite	0	100	end of file	1	1045968	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\8ghN89CsjOW1signons.sqlite	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\D87fZN3R3jFeplaces.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\D87fZN3R3jFeplaces.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\D87fZN3R3jFeplaces.sqlite	0	16	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\02zdBXl47cvzcookies.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\02zdBXl47cvzcookies.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\3b6N2Xdh3CYwplaces.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\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\Google\Chrome\User Data\Local State	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\mHC5xGA2ZDf7Login Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\mHC5xGA2ZDf7Login 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\span1kjtHrReFnXF\hxHjRwjYwPT3Login Data For Account	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\hxHjRwjYwPT3Login Data For Account	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\B087runuAKfxWebData	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\B087runuAKfxWebData	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\66rslgkYekRJHistory	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\66rslgkYekRJHistory	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\span1kjtHrReFnXF\sYcixjslgY3sWebData	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\sYcixjslgY3sWebData	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\span1kjtHrReFnXF\mba9gPQiNkwLCookies	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\span1kjtHrReFnXF\PJJYS_lpzF0mCookies	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\PJJYS_lpzF0mCookies	0	4096	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\PJJYS_lpzF0mCookies	0	4096	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\1_QlH4gDMSHgHistory	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\1_QlH4gDMSHgHistory	0	4096	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\1_QlH4gDMSHgHistory	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\span1kjtHrReFnXF\19u7ECnptzzlWebData	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\Default\Local Storage\leveldb\000003.log	0	4096	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\span1kjtHrReFnXF\otYgbid_VcgTLogin Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\otYgbid_VcgTLogin Data	0	2048	success or wait	1	1045968	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\8J4SxneIDIIbLogin Data For Account	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\ByL8mAxGwSmaWeb Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\rMqqLrP0489yHistory	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\rMqqLrP0489yHistory	0	4096	success or wait	1	1045968	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\span1kjtHrReFnXF\azTbUSfG7fMXWeb Data	0	100	success or wait	1	1045968	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	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\1WS737_IECbpCookies	0	100	end of file	1	1045968	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	4096	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\span1kjtHrReFnXF\JhTxiIG1NfyxHistory	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span1kjtHrReFnXF\JhTxiIG1NfyxHistory	0	4096	success or wait	1	1045968	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\span1kjtHrReFnXF\ctu1BJdIHpHIWeb Data	0	100	success or wait	1	1045968	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\trixy1kjtHrReFnXF\information.txt	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\Cookies\Chrome_Default.txt	0	4096	success or wait	2	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\Cookies\Chrome_Default.txt	0	4096	end of file	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\information.txt	0	4096	success or wait	2	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\information.txt	0	4096	end of file	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\passwords.txt	0	4096	success or wait	2	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy1kjtHrReFnXF\passwords.txt	0	4096	end of file	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\8klzCUsmQMVYazLTWo6KoKU.zip	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\8klzCUsmQMVYazLTWo6KoKU.zip	0	4096	success or wait	1	F48BE4	ReadFile

Analysis Process: schtasks.exe PID: **3852**, Parent PID: **744**

General

Target ID:	4
Start time:	12:02:54
Start date:	12/05/2024
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:	0x510000
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: **6880**, Parent PID: **3852**

General

Target ID:	5
Start time:	12:02:54
Start date:	12/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: MPGPH131.exe PID: **648**, Parent PID: **1044**

General

Target ID:	6
Start time:	12:02:56
Start date:	12/05/2024
Path:	C:\ProgramData\MPGPH131\MPGPH131.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\MPGPH131\MPGPH131.exe
Imagebase:	0xf00000
File size:	3'241'984 bytes
MD5 hash:	72007357BEB74FEA20E7DAA285212B16
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.2038444283.00000000008D7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PrivateLoader, Description: Yara detected PrivateLoader, Source: 00000006.00000002.2039072826.0000000000F01000.00000040.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000006.00000003.1786714219.0000000000999000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000006.00000002.2038444283.0000000000857000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
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\trixy7qiYjWFiJkre	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\span7qiYjWFiJkre	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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\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\span7qiYjWFiJkre\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\span7qiYjWFiJkre\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\span7qiYjWFiJkre\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\span7qiYjWFiJkre\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
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\TRbMB5IbyYCfLogin 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\span7qiYjWFiJkre_2Udgx0R4lC0Login 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\span7qiYjWFiJkre\SBUYXJCvH4fCWeb 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\span7qiYjWFiJkre\ITZ0bicyJ58aHistory	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\span7qiYjWFiJkre\v8KCsYORX8h7Web 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\span7qiYjWFiJkre\QxgKrYHoDHAeCookies	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\span7qiYjWFiJkre\zByDc7TM5G4BCookies	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\span7qiYjWFiJkre\m78YdG3PG6psHistory	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\span7qiYjWFiJkre\fp5Zfw4ryWNTWeb 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\span7qiYjWFiJkre\x6iuAgWaPHROLogin 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\span7qiYjWFiJkre\plJtyZ2j3iKJLogin 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\span7qiYjWFiJkre\J0EAMZmTySltWeb 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\span7qiYjWFiJkre\JsdnoRPI_10LHistory	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\span7qiYjWFiJkre\HK3i7VEtGMBbWeb 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\span7qiYjWFiJkre\pCsnq1VdvsvLCookies	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\span7qiYjWFiJkre\BdOSr6ULfsrrHistory	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\span7qiYjWFiJkre\rh5eReF6pk1JWeb 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\trixy7qiYjWFiJkre\passwords.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F429AF	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\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\trixy7qiYjWFiJkre\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\ZeTvTkc8PqqpWi0gm5JPfdt.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\span7qiYjWFiJkre\Ei8DrAmaYu9Ksignons.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\8ghN89CsjOW1signons.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\D87fZN3R3jFeplaces.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\02zdBXI47cvzcookies.sqlite	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\TRbMB5IbyYCfLogin Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre_2Udgx0R4lC0Login Data For Account	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\SBUYXJCvH4fCWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\ITZ0bicyJ58aHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\v8KCsYORX8h7Web Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\QxgKrYHoDHAeCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\zByDc7TM5G4BCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\m78YdG3PG6psHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\fp5Zfw4ryWNTWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\x6iuAgWaPHROLogin Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\plJtyZ2j3iKJLogin Data For Account	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\J0EAMZmTySltWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\JsdnoRPI_10LHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\HK3i7VEtGMBbWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\pCsnq1VdvsvLCookies	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\BdOSr6ULfsrrHistory	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\rh5eReF6pk1JWeb Data	success or wait	1	F4B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\ZeTvTkc8PqqpWi0gm5JPfdt.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 35 31 34 39 37 31 32 30 36	1715514971206	success or wait	1	F49914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\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 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\span7qiYjWFiJkre\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 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\span7qiYjWFiJkre\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	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\span7qiYjWFiJkre\TRbMB5IbyYCfLogin 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 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\span7qiYjWFiJkre_2Udgx0R4lC0Login 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	SQLite format 3@ .j	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\SBUYXJCvH4fCWeb 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	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\span7qiYjWFiJkre\ITZ0bicyJ58aHistory	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 04 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 04 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
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\v8KCsYORX8h7Web 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	2	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\zByDc7TM5G4BCookies	0	28672	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 0b 00 00 00 07 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 00 00 00 00 0b 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 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\span7qiYjWFiJkre\m78YdG3PG6psHistory	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 04 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 00 00 00 00 04 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	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\span7qiYjWFiJkre\fp5Zfw4ryWNTWeb 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\span7qiYjWFiJkre\x6iuAgWaPHROLogin Data	0	49152	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 18 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 01 00 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 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	SQLite format 3@ .O}	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\J0EAMZmTySltWeb Data	0	114688	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 38 00 00 00 00 00 00 00 00 00 00 00 24 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 4f 7d 05 00 00 00 05 07 fd 00 00 00 00 34 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	SQLite format 3@ 8$.O}4	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\JsdnoRPI_10LHistory	0	126976	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 02 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 18 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 4f 7d 05 00 00 00 01 0f fd 00 00 00 00 1c 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	SQLite format 3@ .O}	success or wait	1	FD69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\BdOSr6ULfsrrHistory	0	126976	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 02 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 18 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 4f 7d 05 00 00 00 01 0f fd 00 00 00 00 1c 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	SQLite format 3@ .O}	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\rh5eReF6pk1JWeb Data	0	114688	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 38 00 00 00 00 00 00 00 00 00 00 00 24 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 4f 7d 05 00 00 00 05 07 fd 00 00 00 00 34 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 00 00 00 00	SQLite format 3@ 8$.O}4	success or wait	1	FD69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\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		success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\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 0d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd		success or wait	1	F49914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\Cookies\Chrome_Default.txt	0	4096	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 31 34 35 30 30 33 09 4e 49 44 09 45 4e 43 38 39 33 2a 5f 64 6a 45 77 33 2b 6b 2b 46 32 41 2f 72 4b 31 58 4f 58 32 42 58 55 71 36 70 59 32 4c 42 43 4f 7a 6f 58 4f 44 69 4a 6e 72 72 76 44 62 44 73 50 57 69 59 77 4b 5a 6f 77 67 39 50 78 48 71 6b 54 6d 33 37 48 70 77 43 35 32 72 58 70 6e 75 55 46 72 51 4d 70 56 33 69 4b 74 64 53 48 65 67 4f 6d 2b 58 67 75 5a 5a 36 74 47 61 43 59 32 68 47 56 79 52 38 4a 67 49 71 51 6d 61 31 57 4c 58 79 68 43 69 57 71 6a 6f 75 37 2f 63 33 71 53 65 61 4b 79 4e 6f 55 4b 48 61 34 54 55 4c 58 34 5a 6e 4e 4e 74 58 46 6f 43 75 5a 63 42 41 41 79 34 74 59 63 7a 2b 30 42 46 34 6a 2f 30 50 67 2b 4d 67 56 2b 73 37 33 36 37 6b 59 63 6a 4f 34 71 33 7a 77 63	.google.comTRUE/TRUE 1712145003 NIDENC893*_djEw3+k+F2A/rK1XOX2 BXUq6pY2LBCOzoXODi JnrrvDbDsPWi YwKZowg9PxHqkTm37H pwC52rXpnuUF rQMpV3iKtdSHegOm+Xg uZZ6tGaCY2h GVyR8JgIqQma1WLXyh CiWqjou7/c3q SeaKyNoUKHa4TULX4Z nNNtXFoCuZcB AAy4tYcz+0BF4j/0Pg+M gV+s7367kYcjO4q3zwc	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\Cookies\Chrome_Default.txt	4096	1989	63 61 74 69 6f 6e 73 54 65 6c 65 6d 65 74 72 79 44 65 76 69 63 65 49 64 09 45 4e 43 38 39 33 2a 5f 64 6a 45 77 2f 45 50 6b 73 54 6e 42 6d 4d 42 45 51 71 53 30 72 6d 71 6c 78 36 5a 59 62 62 70 49 6d 4d 73 63 6d 66 75 6b 6c 38 56 32 66 79 68 47 66 36 43 73 52 79 4f 72 51 41 52 6e 6c 72 75 4e 75 63 57 4c 6e 38 62 58 62 75 37 2b 72 4d 77 72 78 45 6a 48 41 49 37 33 58 77 3d 3d 5f 62 33 69 30 75 36 4c 4c 63 4b 43 4d 55 61 46 2f 55 6c 51 67 45 50 53 4c 39 50 74 4c 5a 32 31 43 75 54 31 64 4a 6b 66 43 7a 4d 45 3d 2a 0d 0a 2e 63 2e 62 69 6e 67 2e 63 6f 6d 09 46 41 4c 53 45 09 2f 09 54 52 55 45 09 31 37 33 30 31 30 39 32 38 31 09 53 52 4d 5f 42 09 45 4e 43 38 39 33 2a 5f 64 6a 45 77 37 6d 56 46 74 59 35 63 5a 42 6d 63 53 49 64 39 6f 2b 4c 4f 36 70 59 78 5a 47 66 65	cationsTelemetryDeviceIdENC893 *_djEw/EPksTnBmMBEQqS0rmqlx6ZY bbpImMscmfukl8V2fyhGf6CsRyOrQA RnlruNucWLn8bXbu7+rMwrxEjHAI73 Xw==_b3i0u6LLcKCMUaF/UlQgEPSL9 PtLZ21CuT1dJkfCzME=*.c.bing.com FALSE/TRUE 1730109281 SRM_BENC893*_djEw7mVFtY5cZBmcSId9o+LO6pYxZGfe	success or wait	1	F49914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\information.txt	0	4096	42 75 69 6c 64 3a 20 74 61 6e 6f 73 0d 0a 56 65 72 73 69 6f 6e 3a 20 32 2e 30 0d 0a 0d 0a 44 61 74 65 3a 20 53 75 6e 20 4d 61 79 20 31 32 20 31 32 3a 30 33 3a 30 35 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 65 65 31 64 66 65 38 31 32 65 37 39 36 38 35 65 61 66 63 35 39 32 36 33 39 38 30 31 38 65 66 66 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: tanosVersion: 2.0Date: Sun May 12 12:03:05 2024MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}HWID: ee1dfe812e79685eafc5926398018effPath: C:\ProgramData\MPGPH131\MPGPH131.exeWork Dir: C:\	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\information.txt	4096	2928	6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 31 30 31 36 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 38 30 38 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 31 35 36 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 35 31 32 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 34 33 34 38 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 34 34 31 32 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a	nDJLELYssjayClc.exe [1016]zDTarlxjDyChCjnDJLELYssjayClc.exe [3808]zDTarlxjDyChCjnDJLELYssjayClc.exe [3156]zDTarlxjDyChCjnDJLELYssjayClc.exe [3512]zDTarlxjDyChCjnDJLELYssjayClc.exe [4348]zDTarlxjDyChCjnDJLELYssjayClc.exe [4412]zDTarlxjDyChCjnDJ	success or wait	1	F49914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\information.txt	0	4096	42 75 69 6c 64 3a 20 74 61 6e 6f 73 0d 0a 56 65 72 73 69 6f 6e 3a 20 32 2e 30 0d 0a 0d 0a 44 61 74 65 3a 20 53 75 6e 20 4d 61 79 20 31 32 20 31 32 3a 30 33 3a 30 35 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 65 65 31 64 66 65 38 31 32 65 37 39 36 38 35 65 61 66 63 35 39 32 36 33 39 38 30 31 38 65 66 66 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: tanosVersion: 2.0Date: Sun May 12 12:03:05 2024MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}HWID: ee1dfe812e79685eafc5926398018effPath: C:\ProgramData\MPGPH131\MPGPH131.exeWork Dir: C:\	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\information.txt	4096	2928	6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 31 30 31 36 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 38 30 38 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 31 35 36 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 33 35 31 32 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 34 33 34 38 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a 4c 45 4c 59 73 73 6a 61 79 43 6c 63 2e 65 78 65 20 5b 34 34 31 32 5d 0d 0a 7a 44 54 61 72 6c 78 6a 44 79 43 68 43 6a 6e 44 4a	nDJLELYssjayClc.exe [1016]zDTarlxjDyChCjnDJLELYssjayClc.exe [3808]zDTarlxjDyChCjnDJLELYssjayClc.exe [3156]zDTarlxjDyChCjnDJLELYssjayClc.exe [3512]zDTarlxjDyChCjnDJLELYssjayClc.exe [4348]zDTarlxjDyChCjnDJLELYssjayClc.exe [4412]zDTarlxjDyChCjnDJ	success or wait	1	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\ZeTvTkc8PqqpWi0gm5JPfdt.zip	0	40	50 4b 03 04 14 00 00 08 08 00 62 60 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	PKb`XCookies\	success or wait	4	F49914	WriteFile
C:\Users\user\AppData\Local\Temp\ZeTvTkc8PqqpWi0gm5JPfdt.zip	14	12	00 00 00 00 02 00 00 00 00 00 00 00		success or wait	4	F49914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ZeTvTkc8PqqpWi0gm5JPfdt.zip	5250	314	50 4b 01 02 00 0b 14 00 00 08 08 00 62 60 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 43 6f 6f 6b 69 65 73 5c 50 4b 01 02 00 0b 14 00 00 08 08 00 62 60 fd 58 51 6e fd 2b fd 0b 00 00 fd 17 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 62 60 fd 58 fd fd 7a fd fd 06 00 00 70 1b 00 00 0f 00 00 00 00 00 00 00 01 00 00 00 00 00 55 0c 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 62 60 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 56 13 00 00 70 61 73 73 77 6f 72 64 73 2e 74 78 74 50 4b 05 06 00 00 00 00 04	PKb`XCookies\PKb`XQn+(Cookies\Chrome_Default.txtPKb`XzpUinformation.txtPKb`XF!Vpasswords.txtPK	success or wait	1	F49914	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\MPGPH131\MPGPH131.exe	0	64	success or wait	1	110E562	NtReadFile
C:\ProgramData\MPGPH131\MPGPH131.exe	0	20	success or wait	1	110E562	NtReadFile
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\span7qiYjWFiJkre\Ei8DrAmaYu9Ksignons.sqlite	0	100	end of file	2	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\D87fZN3R3jFeplaces.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\D87fZN3R3jFeplaces.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\02zdBXl47cvzcookies.sqlite	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\02zdBXl47cvzcookies.sqlite	0	32768	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\3b6N2Xdh3CYwplaces.sqlite	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\Temp\span7qiYjWFiJkre\TRbMB5IbyYCfLogin 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\Temp\span7qiYjWFiJkre_2Udgx0R4lC0Login Data For Account	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre_2Udgx0R4lC0Login Data For Account	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\SBUYXJCvH4fCWeb Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\SBUYXJCvH4fCWeb Data	0	2048	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\ITZ0bicyJ58aHistory	0	100	success or wait	2	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\ITZ0bicyJ58aHistory	0	4096	success or wait	2	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\span7qiYjWFiJkre\v8KCsYORX8h7Web Data	0	100	success or wait	2	1045968	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\v8KCsYORX8h7Web Data	0	2048	success or wait	2	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\span7qiYjWFiJkre\QxgKrYHoDHAeCookies	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\span7qiYjWFiJkre\zByDc7TM5G4BCookies	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\zByDc7TM5G4BCookies	0	4096	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\zByDc7TM5G4BCookies	0	4096	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\m78YdG3PG6psHistory	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\Temp\span7qiYjWFiJkre\fp5Zfw4ryWNTWebData	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\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	0	4096	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	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\x6iuAgWaPHROLogin Data	0	100	success or wait	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\x6iuAgWaPHROLogin Data	0	2048	success or wait	1	1045968	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	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\plJtyZ2j3iKJLogin Data For Account	0	100	end of file	1	1045968	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\J0EAMZmTyStWeb Data	0	100	success or wait	1	1045968	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	4096	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	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\pCsnq1VdvsvLCookies	0	100	end of file	1	1045968	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	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\span7qiYjWFiJkre\BdOSr6ULfsrrHistory	0	100	success or wait	1	1045968	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\span7qiYjWFiJkre\rh5eReF6pk1JWebData	0	100	success or wait	1	1045968	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	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\information.txt	0	4096	success or wait	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\Cookies\Chrome_Default.txt	0	4096	success or wait	2	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\Cookies\Chrome_Default.txt	0	4096	end of file	1	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\information.txt	0	4096	success or wait	4	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixy7qiYjWFiJkre\information.txt	0	4096	end of file	2	F48BE4	ReadFile
C:\Users\user\AppData\Local\Temp\ZeTvTkc8PqqpWi0gm5JPfdt.zip	0	4096	success or wait	1	F48BE4	ReadFile

Analysis Process: RageMP131.exe PID: **7236**, Parent PID: **2580**

General

Target ID:	7
Start time:	12:03:02
Start date:	12/05/2024

Path:	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\RageMP131\RageMP131.exe"
Imagebase:	0xb80000
File size:	3'241'984 bytes
MD5 hash:	72007357BEB74FEA20E7DAA285212B16
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_PrivateLoader, Description: Yara detected PrivateLoader, Source: 00000007.00000002.1858273700.0000000000B81000.00000040.00000001.01000000.00000006.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 47%, ReversingLabs • Detection: 59%, Virustotal, Browse
Reputation:	low
Has exited:	true

Analysis Process: WerFault.exe PID: 7448, Parent PID: 744

General

Target ID:	10
Start time:	12:03:06
Start date:	12/05/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 744 -s 2028
Imagebase:	0xfd0000
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: WerFault.exe PID: 7564, Parent PID: 1436

General

Target ID:	13
Start time:	12:03:10
Start date:	12/05/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1436 -s 1956
Imagebase:	0xfd0000
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: WerFault.exe PID: 7584, Parent PID: 648

General

Target ID:	15

Start time:	12:03:10
Start date:	12/05/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 648 -s 1908
Imagebase:	0xfd0000
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: **7768**, Parent PID: **2580**

General

Target ID:	16
Start time:	12:03:13
Start date:	12/05/2024
Path:	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\RageMP131\RageMP131.exe"
Imagebase:	0xb80000
File size:	3'241'984 bytes
MD5 hash:	72007357BEB74FEA20E7DAA285212B16
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_PrivateLoader, Description: Yara detected PrivateLoader, Source: 00000010.00000002.1922715500.0000000000B81000.00000040.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

Disassembly

No disassembly