ID: 1436950
Sample Name: file.exe
Cookbook: default.jbs
Time: 20:07:05
Date: 06/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

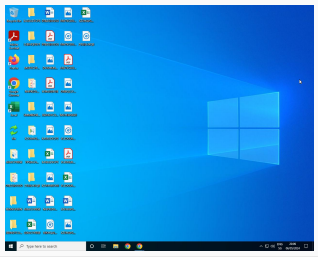
Windows Analysis Report

file.exe

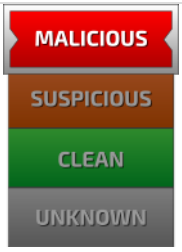
Overview

General Information

Sample name:	file.exe
Analysis ID:	1436950
MD5:	51014f1c86736..
SHA1:	6d0bab0a443ff...
SHA256:	1845d2a25b62...
Tags:	exe
Infos:	



Detection



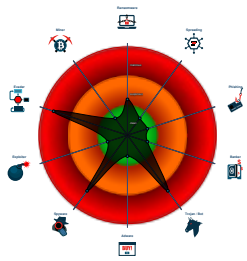
RisePro Stealer

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 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…
- Hides threads from debuggers

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 7428 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 51014F1C86736D8F91D432548062EBBF)
  - schtasks.exe (PID: 7488 cmdline: schtasks /create /f /RU "user" /tr "C:\ProgramData\MPGPH131\MPGPH131.exe" /tn "MPGPH131 HR" /sc HOURLY /rl HIGHEST MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 7496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - schtasks.exe (PID: 7536 cmdline: schtasks /create /f /RU "user" /tr "C:\ProgramData\MPGPH131\MPGPH131.exe" /tn "MPGPH131 LG" /sc ONLOGON /rl HIGHEST MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 7544 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - WerFault.exe (PID: 7324 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7428 -s 1980 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- MPGPH131.exe (PID: 7584 cmdline: C:\ProgramData\MPGPH131\MPGPH131.exe MD5: 51014F1C86736D8F91D432548062EBBF)
  - WerFault.exe (PID: 2816 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7584 -s 1960 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- MPGPH131.exe (PID: 7592 cmdline: C:\ProgramData\MPGPH131\MPGPH131.exe MD5: 51014F1C86736D8F91D432548062EBBF)
- RageMP131.exe (PID: 7672 cmdline: "C:\Users\user\AppData\Local\RageMP131\RageMP131.exe" MD5: 51014F1C86736D8F91D432548062EBBF)
  - WerFault.exe (PID: 8136 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7672 -s 1944 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- RageMP131.exe (PID: 7784 cmdline: "C:\Users\user\AppData\Local\RageMP131\RageMP131.exe" MD5: 51014F1C86736D8F91D432548062EBBF)
  - WerFault.exe (PID: 6536 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7784 -s 1908 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\wwigCWSFuz2MihL8u4G1uFC.zip	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\9wBRx7ST9VOnJqni_JpioUs.zip	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\tC131VXqxqwXyoqOe7muh9i.zip	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\PSdiYEtw_DOSPKoK_uBheap.zip	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2173403489.0000000001838000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000000.00000002.2023815185.0000000001CEC000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000008.00000002.2015798047.00000000019D2000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000003.1907164226.0000000001CE6000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
00000007.00000002.2022464307.000000000191E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RiseProStealer	Yara detected RisePro Stealer	Joe Security	
Click to see the 16 entries				

Sigma Signatures

System Summary

Sigma detected: CurrentVersion Autorun Keys Modification

Snort Signatures

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.4 - Destination IP: 147.45.47.93

Timestamp:	05/06/24-20:08:42.332746
SID:	2046269
Source Port:	49731
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (External IP) - Source IP: 147.45.47.93 - Destination IP: 192.168.2.4

Timestamp:	05/06/24-20:08:11.803337
SID:	2046267
Source Port:	58709
Destination Port:	49730
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.93 - Destination IP: 192.168.2.4

Timestamp:	05/06/24-20:07:53.913307
SID:	2046266
Source Port:	58709
Destination Port:	49730
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.4 - Destination IP: 147.45.47.93

Timestamp:	05/06/24-20:07:57.036164

SID:	2046269
Source Port:	49730
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN RisePro TCP Heartbeat Packet - Source IP: 192.168.2.4 - Destination IP: 147.45.47.93

Timestamp:	05/06/24-20:07:53.682907
SID:	2049060
Source Port:	49730
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.93 - Destination IP: 192.168.2.4

Timestamp:	05/06/24-20:08:04.120685
SID:	2046266
Source Port:	58709
Destination Port:	49733
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (External IP) - Source IP: 147.45.47.93 - Destination IP: 192.168.2.4

Timestamp:	05/06/24-20:08:05.646832
SID:	2046267
Source Port:	58709
Destination Port:	49733
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.93 - Destination IP: 192.168.2.4

Timestamp:	05/06/24-20:07:56.321028
SID:	2046266
Source Port:	58709
Destination Port:	49732
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.4 - Destination IP: 147.45.47.93

Timestamp:	05/06/24-20:08:18.051763
SID:	2046269
Source Port:	49738
Destination Port:	58709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 147.45.47.93 - Destination IP: 192.168.2.4

Timestamp:	05/06/24-20:07:56.309289
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: 147.45.47.93 - Destination IP: 192.168.2.4

Timestamp:	05/06/24-20:08:11.640975
SID:	2046266
Source Port:	58709
Destination Port:	49738
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (External IP) - Source IP: 147.45.47.93 - Destination IP: 192.168.2.4	
Timestamp:	05/06/24-20:08:15.381006
SID:	2046267
Source Port:	58709
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (External IP) - Source IP: 147.45.47.93 - Destination IP: 192.168.2.4	
Timestamp:	05/06/24-20:08:11.897367
SID:	2046267
Source Port:	58709
Destination Port:	49738
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.4 - Destination IP: 147.45.47.93	
Timestamp:	05/06/24-20:08:09.259896
SID:	2046269
Source Port:	49733
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: 147.45.47.93	
Timestamp:	05/06/24-20:08:30.364347
SID:	2046269
Source Port:	49732
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

Networking

- Snort IDS alert for network traffic
- 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 RisePro Stealer

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

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

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

Remote Access Functionality

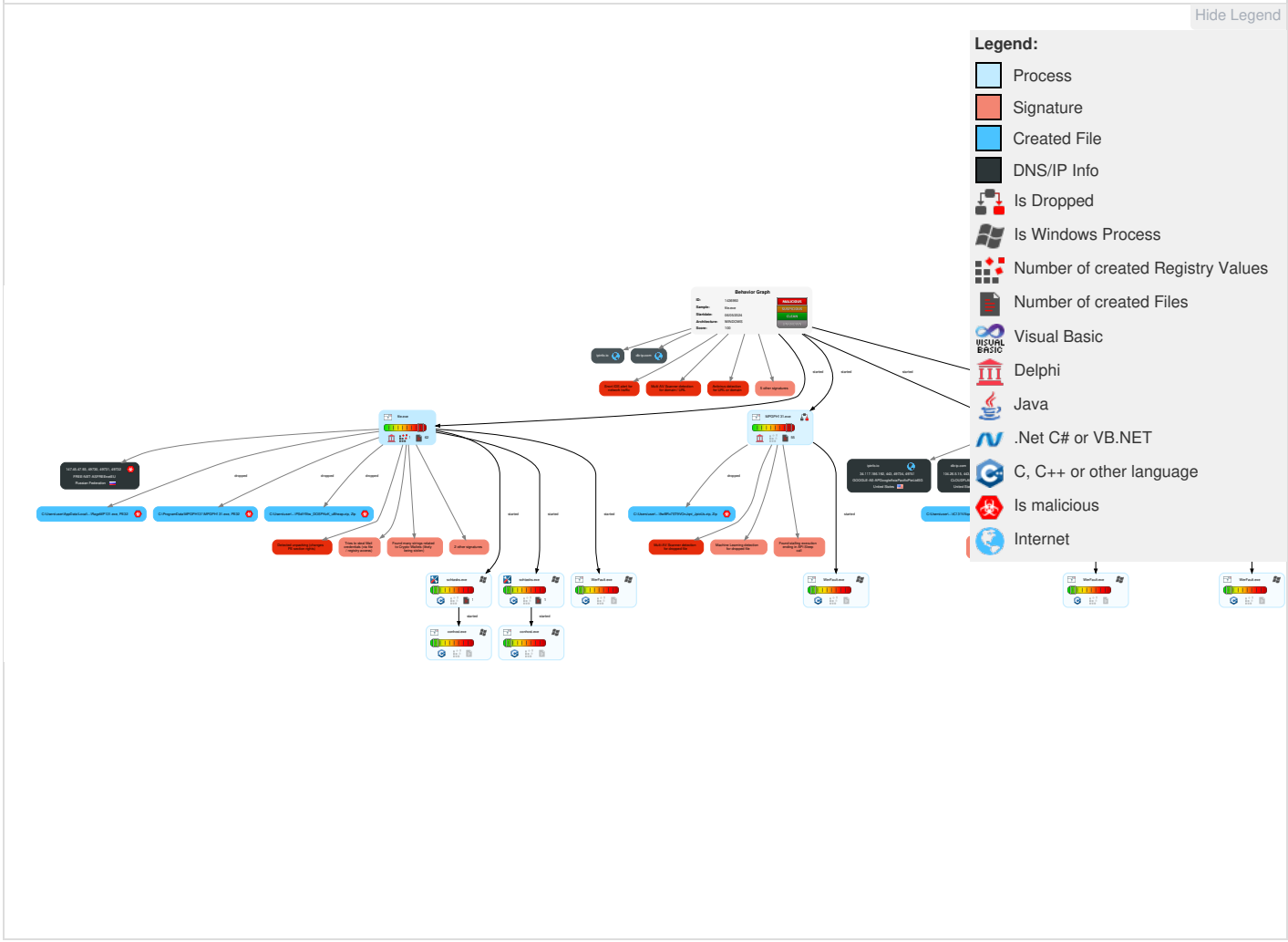
Yara detected RisePro Stealer

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	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 Email Collection	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	Input Capture	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	2 4 1 Security Software Discovery	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	1 2 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 1 Process Injection	DCSync	2 Process Discovery	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	1 Application Window 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 System Owner/User Discovery	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	Dynamic API Resolution	Network Sniffing	1 System Network Configuration Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement

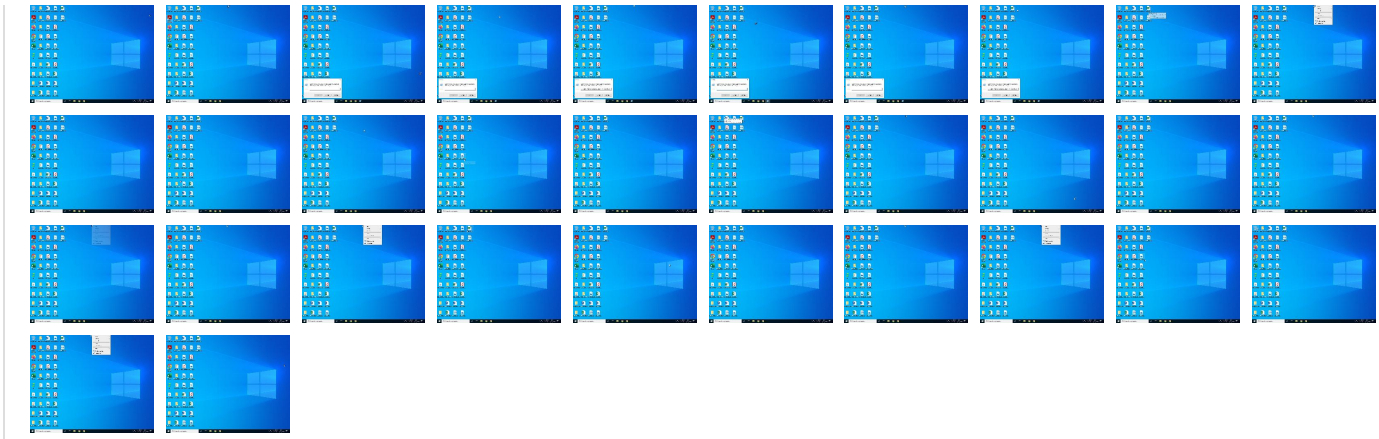
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	38%	Virustotal		Browse
file.exe	39%	ReversingLabs	Win32.Trojan.Generic	
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	39%	ReversingLabs	Win32.Trojan.Generic	
C:\ProgramData\MPGPH131\MPGPH131.exe	40%	Virustotal		Browse
C:\Users\user\AppData\Local\RageMP131\RageMP131.exe	39%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\RageMP131\RageMP131.exe	40%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pki-ocsp.symauth.com0	0%	URL Reputation	safe	
http://147.45.47.102:57893/hera/amadka.exeDatae	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exe	100%	Avira URL Cloud	malware	
http://147.45.47.102:57893/hera/amadka.exe68.0	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/lenin.exerbirdox/i	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exeD)a#	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/go.exe	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/lenin.exe)	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/lenin.exesepro	0%	Avira URL Cloud	safe	
http://https://t.4	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/lenin.exeUser	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exe	20%	Virustotal		Browse
http://193.233.132.56/cost/go.exe00.1	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exeData	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/lenin.exesepro	22%	Virustotal		Browse
http://193.233.132.56/cost/go.exe1	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exeletsM	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exe68.0	15%	Virustotal		Browse
http://147.45.47.102:57893/hera/amadka.exeN	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/go.exe00.1	18%	Virustotal		Browse
http://193.233.132.56/cost/lenin.exe	0%	Avira URL Cloud	safe	
http://193.233.132.56/cost/go.exe	25%	Virustotal		Browse
http://193.233.132.56/cost/go.execoin	0%	Avira URL Cloud	safe	
http://147.45.47.102:57893/hera/amadka.exeN	18%	Virustotal		Browse
http://193.233.132.56/cost/lenin.exe	26%	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://db-ip.com/demo/home.php?s=84.17.40.101	false		high
http://https://ipinfo.io/widget/demo/84.17.40.101	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://db-ip.com/demo/home.php?s=84.17.40.101c	RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	file.exe, 00000000.00000003.1865241711.000000001D6B000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00003.1864375367.0000000001D5A000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867863334.0000000001D78000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099008633.00000000018B3000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2102021978.00000000018D2000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2105243412.00000000018E7000.00000004.00020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820028873.0000000001A7A000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00003.1822926347.0000000001A9F000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820619276.0000000001A9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1867422417.0000000001AD2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1864465481.0000000001A98000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1865350119.0000000001ABC000.00000004.00000020.00020000.00000000.sdmp, DOGuPW8VgXDwWeb Data.5.dr, 1bA0iPxs1_tpWeb Data.8.dr, Z82s7O924lLeWeb Data.5.dr, Y7ezkCIN3tvGWeb Data.0.dr, QALFCGqIe0GzWeb Data.8.dr, V9veGYQ701aZWeb Data.7.dr, 4deeADJYPmpQWeb Data.0.dr, pTWMc6sLNinTWeb Data.7.dr, 42h4yDt09kAFWeb Data.7.dr	false		high
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.zvXrErQ5GYDF	3b6N2Xdh3CYwplaces.sqlite.8.dr	false		high
http://https://duckduckgo.com/ac/?q=	file.exe, 00000000.00000003.1865241711.000000001D6B000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00003.1864375367.0000000001D5A000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867863334.0000000001D78000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099008633.00000000018B3000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2102021978.00000000018D2000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2105243412.00000000018E7000.00000004.00020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820028873.0000000001A7A000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00003.1822926347.0000000001A9F000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820619276.0000000001A9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1867422417.0000000001AD2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1864465481.0000000001A98000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1865350119.0000000001ABC000.00000004.00000020.00020000.00000000.sdmp, DOGuPW8VgXDwWeb Data.5.dr, 1bA0iPxs1_tpWeb Data.8.dr, Z82s7O924lLeWeb Data.5.dr, Y7ezkCIN3tvGWeb Data.0.dr, QALFCGqIe0GzWeb Data.8.dr, V9veGYQ701aZWeb Data.7.dr, 4deeADJYPmpQWeb Data.0.dr, pTWMc6sLNinTWeb Data.7.dr, 42h4yDt09kAFWeb Data.7.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t.me/RiseProSUPPORTm	file.exe, 00000000.00000002.2023815185.0000000001CEC000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1907164226.0000000001CE6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://db-ip.com/demo/home.php?s=84.17.40.101g	file.exe, 00000000.00000002.2023815185.0000000001C7E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://147.45.47.102:57893/hera/amadka.exe	file.exe, 00000000.00000002.2023815185.0000000001C7E000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000002.2173403489.00000000017DE000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1874959213.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.00000000019D2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.0000000001A66000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1874632671.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1874348802.0000000001A65000.00000004.00000020.00020000.00000000.sdmp	false	• 20%, Virustotal, Browse • Avira URL Cloud: malware	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/	file.exe, 00000000.00000002.2023815185.0000000001C7E000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000002.2173403489.00000000017DE000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2056651399.00000000017DE000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2121250052.00000000016C8000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.00000000019D2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://db-ip.com/demo/home.php?s=84.17.40.101s	RageMP131.exe, 00000008.00000002.2015798047.00000000019D2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORTli	MPGPH131.exe, 00000005.00000002.2173403489.0000000001838000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2110910326.0000000001838000.00000004.00000020.00020000.00000000.sdmp	false		high
http://147.45.47.102:57893/hera/amadka.exe68.0	RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp	false	• 15%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://pki-crl.symauth.com/offlineca/TheInstituteofElectricalandElectronicsEngineersIncIEEERootCA.cr	file.exe, RageMP131.exe.0.dr, MPGPH131.exe.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	file.exe, 00000000.00000003.1865241711.000000001D6B000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1864375367.0000000001D5A000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867863334.0000000001D78000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099008633.00000000018B3000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2102021978.00000000018D2000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2105243412.00000000018E7000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820028873.0000000001A7A000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1822926347.0000000001A9F000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820619276.0000000001A9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1867422417.0000000001AD2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1864465481.0000000001A98000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1865350119.0000000001ABC000.00000004.00000020.00020000.00000000.sdmp, DOGuPW8VgXDwWeb Data.5.dr, 1bA0iPxs1_tpWeb Data.8.dr, Z82s7O924lLeWeb Data.5.dr, Y7ezkClN3tvGWeb Data.0.dr, QALFCGqIe0GzWeb Data.8.dr, V9veGYQ701aZWeb Data.7.dr, 4deeADJYPmpQWeb Data.0.dr, pTWMc6sLNinTWeb Data.7.dr, 42h4yDt09kAFWeb Data.7.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	file.exe, 00000000.00000003.1864720375.000000001D49000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867274750.0000000001D67000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099216190.0000000018B0000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2104564573.00000000018C5000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1822281358.0000000001A79000.00000004.00000020.00020000.00000000.sdmp, ELASOvMcSsNrHistory.7.dr, vd0z8wzGefD1History.8.dr, LhmhqtkXTkbYHistory.0.dr, iCl1DNg_vvFNHistory.5.dr, QZolPj_wU7yvHistory.8.dr, BhPLdlMH4HviHistory.5.dr, UqNl41FdpO7sHistory.0.dr, OAwfuvRJ7Zo3History.7.dr	false		high
http://147.45.47.102:57893/hera/amadka.exeDatae	MPGPH131.exe, 00000005.00000002.2173403489.00000000017DE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.233.132.56/cost/lenin.exerbirdox/i	file.exe, 00000000.00000002.2023815185.000000001C7E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://147.45.47.102:57893/hera/amadka.exeD)a#	RageMP131.exe, 00000008.00000003.1874959213.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.0000000001A66000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1874632671.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1874348802.0000000001A65000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t.me/risepro	MPGPH131.exe, 00000005.00000003.2056651399.00000000017DE000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2121250052.00000000016C800.00000004.00000020.00020000.00000000.sdmp	false		high
http://193.233.132.56/cost/lenin.exe)	file.exe, 00000000.00000002.2023815185.000000001C7E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://193.233.132.56/cost/go.exe	RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1874959213.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.00000000019D2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1874632671.0000000001A65000.00000004.00000020.00020000.00000000.sdmp	false	• 25%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://db-ip.com:443/demo/home.php?s=84.17.40.101e	RageMP131.exe, 00000008.00000002.2015798047.0000000001938000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_bot&	RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_bot#	MPGPH131.exe, 00000006.00000002.2121250052.00000000016C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	ELASOvMcSsNrHistory.7.dr, vd0z8wzGefD1History.8.dr, LhmhqtkXTkbYHistory.0.dr, iCl1DNg_vvFNHistory.5.dr, QZolPj_wU7yvHistory.8.dr, BhPLdlMH4HviHistory.5.dr, UqNl41FdpO7sHistory.0.dr, OAwfuvRJ7Zo3History.7.dr	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	file.exe, 00000000.00000003.1865241711.0000000001D6B000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1864375367.0000000001D5A000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867863334.0000000001D78000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099008633.00000000018B3000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2102021978.00000000018D2000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2105243412.00000000018E7000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820028873.0000000001A7A000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1822926347.0000000001A9F000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820619276.0000000001A9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1867422417.0000000001AD2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1864465481.0000000001A98000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1865350119.0000000001ABC000.00000004.00000020.00020000.00000000.sdmp, DOGuPW8VgXDwWeb Data.5.dr, 1bA0iPxs1_tpWeb Data.8.dr, Z82s7O924lLeWeb Data.5.dr, Y7ezkCIN3tvGWeb Data.0.dr, QALFCGqIe0GzWeb Data.8.dr, V9veGYQ701aZWeb Data.7.dr, 4deeADJYPmpQWeb Data.0.dr, pTWMc6sLNinTWeb Data.7.dr, 42h4yDt09kAFWeb Data.7.dr	false		high
http://https://t.me/risepro_botisepro_bot	file.exe, 00000000.00000002.2023815185.0000000001C7E000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.00000000019D2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://193.233.132.56/cost/lenin.exesepro	RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp	false	• 22%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ipinfo.io/widget/demo/84.17.40.101~W	RageMP131.exe, 00000008.00000002.2015798047.00000000019B7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://db-ip.com/ggg	MPGPH131.exe, 00000006.00000002.2121250052.00000000016C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORT7	RageMP131.exe, 00000008.00000002.2015798047.0000000001A18000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.4	MPGPH131.exe, 00000005.00000002.2173403489.00000000017DE000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2056651399.00000000017DE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.google.com/images/branding/product/ico/googleg_lodp.ico	file.exe, 00000000.00000003.1865241711.000000001D6B000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1864375367.0000000001D5A000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867863334.0000000001D78000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099008633.00000000018B3000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2102021978.00000000018D2000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2105243412.00000000018E7000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820028873.0000000001A7A000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1822926347.0000000001A9F000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820619276.0000000001A9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1867422417.0000000001AD2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1864465481.0000000001A98000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1865350119.0000000001ABC000.00000004.00000020.00020000.00000000.sdmp, DOGuPW8VgXDwWeb Data.5.dr, 1bA0iPxs1_tpWeb Data.8.dr, Z82s7O924lLeWeb Data.5.dr, Y7ezkClN3tvGWeb Data.0.dr, QALFCGqIe0GzWeb Data.8.dr, V9veGYQ701aZWeb Data.7.dr, 4deeADJYPmpQWeb Data.0.dr, pTWMc6sLNinTWeb Data.7.dr, 42h4yDt09kAFWeb Data.7.dr	false		high
http://https://db-ip.com/demo/home.php?s=84.17.40.101(	MPGPH131.exe, 00000006.00000002.2121250052.00000000016C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://ipinfo.io/https://www.maxmind.com/en/locate-my-ip-addressWs2_32.dll	file.exe, 00000000.00000002.2021619357.000000000F71000.00000040.00000001.01000000.00000003.sdmp, MPGPH131.exe, 00000005.00000002.2170553211.00000000002E1000.00000040.00000001.01000000.00000004.sdmp, MPGPH131.exe, 00000006.00000002.2119820314.00000000002E1000.00000040.00000001.01000000.00000004.sdmp, RageMP131.exe, 00000007.00000002.2020629490.0000000000611000.00000040.00000001.01000000.00000005.sdmp, RageMP131.exe, 00000008.00000002.2014597460.0000000000611000.00000040.00000001.01000000.00000005.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	file.exe, 00000000.00000003.1865241711.000000001D6B000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1864375367.0000000001D5A000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867863334.0000000001D78000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099008633.00000000018B3000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2102021978.00000000018D2000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2105243412.00000000018E7000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820028873.0000000001A7A000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1822926347.0000000001A9F000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820619276.0000000001A9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1867422417.0000000001AD2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1864465481.0000000001A98000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1865350119.0000000001ABC000.00000004.00000020.00020000.00000000.sdmp, DOGuPW8VgXDwWeb Data.5.dr, 1bA0iPxs1_tpWeb Data.8.dr, Z82s7O924ILeWeb Data.5.dr, Y7ezkClN3tvGWeb Data.0.dr, QALFCGqIe0GzWeb Data.8.dr, V9veGYQ701aZWeb Data.7.dr, 4deeADJYPmpQWeb Data.0.dr, pTWMc6sLNinTWeb Data.7.dr, 42h4yDt09kAFWeb Data.7.dr	false		high
http://193.233.132.56/cost/lenin.exeUser	RageMP131.exe, 00000008.00000003.1874959213.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.0000000001A66000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t.me/risepro_bot4.17.40.101	RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://upx.sf.net	Amcache.hve.18.dr	false		high
http://https://db-ip.com:443/demo/home.php?s=84.17.40.101o	MPGPH131.exe, 00000005.00000002.2173403489.000000000174D000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.2022464307.00000000019F4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/RiseProSUPPORT	RageMP131.exe, 00000007.00000002.2022464307.000000000191E000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.2022464307.00000000019F4000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.0000000001A18000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.0000000001938000.00000004.00000020.00020000.00000000.sdmp, 9wBRx7ST9VOnJqni_JpioUs.zip.5.dr, wwigCWSFuz2MihL8u4G1uFC.zip.8.dr, tC131VXqxqwXyoqOe7muh9i.zip.7.dr, PSdiYEtw_DOSPKoK_uBheap.zip.0.dr	false		high
http://193.233.132.56/cost/go.exe00.1	RageMP131.exe, 00000008.00000002.2015798047.00000000019D2000.00000004.00000020.00020000.00000000.sdmp	false	• 18%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	file.exe, 00000000.00000003.1864720375.000000001D49000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867274750.0000000001D67000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099216190.00000000018B0000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2104564573.00000000018C5000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1822281358.0000000001A79000.00000004.00000020.00020000.00000000.sdmp, ELASOvMcSsNrHistory.7.dr, vd0z8wzGefD1History.8.dr, LhmhqtkXTkbYHistory.0.dr, iCl1DNg_vvFNHistory.5.dr, QZolPj_wU7yvHistory.8.dr, BhPLdlMH4HviHistory.5.dr, UqNl41FdpO7sHistory.0.dr, OAwfuvRJ7Zo3History.7.dr	false		high

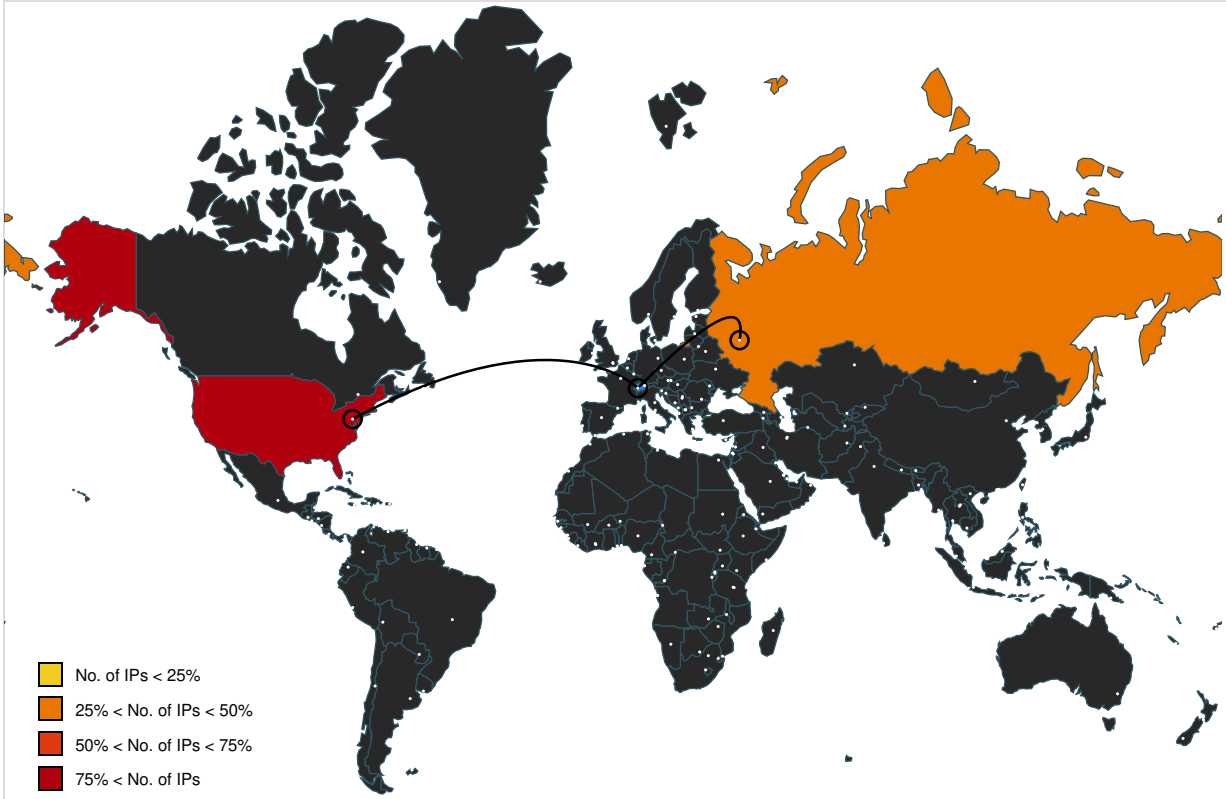
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.ecosia.org/newtab/	file.exe, 00000000.00000003.1865241711.000000001D6B000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1864375367.0000000001D5A000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867863334.0000000001D7800.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099008633.00000000018B3000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2102021978.00000000018D2000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2105243412.00000000018E7000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820028873.0000000001A7A000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1822926347.0000000001A9F000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820619276.0000000001A9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1867422417.0000000001AD2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1864465481.0000000001A98000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1865350119.0000000001ABC000.00000004.00000020.00020000.00000000.sdmp, DOGuPW8VgXDwWeb Data.5.dr, 1bA0iPxs1_tpWeb Data.8.dr, Z82s7O924lLeWeb Data.5.dr, Y7ezkClN3tvGWeb Data.0.dr, QALFCGqIe0GzWeb Data.8.dr, V9veGYQ701aZWeb Data.7.dr, 4deeADJYPmpQWeb Data.0.dr, pTWMc6sLNinTWeb Data.7.dr, 42h4yDt09kAFWeb Data.7.dr	false		high
http://https://ipinfo.io/Mozilla/5.0	file.exe, 00000000.00000002.2023815185.000000001C71000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2056651399.00000000017D7000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000002.2173403489.00000000017D1000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2121250052.00000000016C8000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.00000000019B7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	3b6N2Xdh3CYwplaces.sqlite.8.dr	false		high
http://147.45.47.102:57893/hera/amadka.exeData	RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	file.exe, 00000000.00000003.1865241711.0 000000001D6B000.00000004.00000020.000200 00.00000000.sdmp, file.exe, 00000000.000 00003.1864375367.0000000001D5A000.000000 04.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867863334.0000000001D7800 0.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099 008633.00000000018B3000.00000004.0000002 0.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2102021978.00000000018 D2000.00000004.00000020.00020000.0000000 0.sdmp, MPGPH131.exe, 00000005.00000003. 2105243412.00000000018E7000.00000004.000 00020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820028873.000000 0001A7A000.00000004.00000020.00020000.00 000000.sdmp, RageMP131.exe, 00000007.000 00003.1822926347.0000000001A9F000.000000 04.00000020.00020000.00000000.sdmp, Rage MP131.exe, 00000007.00000003.1820619276. 0000000001A9B000.00000004.00000020.00020 000.00000000.sdmp, RageMP131.exe, 000000 08.00000003.1867422417.0000000001AD2000. 00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.18644 65481.0000000001A98000.00000004.00000020 .00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1865350119.0000000001A BC000.00000004.00000020.00020000.0000000 0.sdmp, DOGuPW8VgXDwWeb Data.5.dr, 1bA0i Pxs1_tpWeb Data.8.dr, Z82s7O924ILeWeb Data.5.dr, Y7ezkCIN3tvGWeb Data.0.dr, QALFCGqIe0GzWeb Data.8.dr, V9veGYQ701aZWeb Data.7.dr, 4deeADJYPmpQWeb Data.0.dr, pTWMc6sLNinTWeb Data.7.dr, 42h4yDt09kAFWeb Data.7.dr	false		high
http://193.233.132.56/cost/go.exe1	RageMP131.exe, 00000007.00000002.2022464 307.00000000019A2000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://db-ip.com/demo/home.php?s=84.17.40.101D	MPGPH131.exe, 00000006.00000002.21212500 52.00000000016C8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://t.me/risepro_bot	RageMP131.exe, 00000008.00000002.2015798 047.00000000019D2000.00000004.00000020.0 0020000.00000000.sdmp, RageMP131.exe, 00 000008.00000003.1844046240.0000000001A1A 000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1873756554. 0000000001AF6000.00000004.00000020.00020 000.00000000.sdmp, RageMP131.exe, 000000 08.00000002.2015798047.0000000001A18000. 00000004.00000020.00020000.00000000.sdmp, passwords.txt.5.dr, passwords.txt.8.dr, password s.txt.7.dr, passwords.txt.0.dr	false		high
http://147.45.47.102:57893/hera/amadka.exeletsM	file.exe, 00000000.00000002.2023815185.0 000000001C7E000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t.me/risepro_botlater	MPGPH131.exe, 00000005.00000002.21734034 89.00000000017DE000.00000004.00000020.00 020000.00000000.sdmp, MPGPH131.exe, 0000 0005.00000003.2056651399.00000000017DE00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ipinfo.io/	RageMP131.exe, 00000008.00000002.2015798 047.000000000199B000.00000004.00000020.0 0020000.00000000.sdmp, RageMP131.exe, 00 000008.00000002.2015798047.0000000001963 000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047. 00000000019B7000.00000004.00000020.00020 000.00000000.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://www.maxmind.com/en/locate-my-ip-address	file.exe, MPGPH131.exe	false		high
http://147.45.47.102:57893/hera/amadka.exeN	MPGPH131.exe, 00000005.00000002.21734034 89.00000000017DE000.00000004.00000020.00 020000.00000000.sdmp	false	• 18%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://db-ip.com:443/demo/home.php?s=84.17.40.101	file.exe, 00000000.00000002.2023815185.0 000000001C7E000.00000004.00000020.000200 00.00000000.sdmp, MPGPH131.exe, 00000006 .00000002.2121250052.0000000001647000.00 000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://193.233.132.56/cost/lenin.exe	RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1874959213.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.00000000019D2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.0000000001A66000.00000004.00000020.00020000.00000000.sdmp	false	• 26%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.winimage.com/zLibDll	file.exe, 00000000.00000002.2021619357.000000000F71000.00000040.00000001.01000000.00000003.sdmp, MPGPH131.exe, 00000005.00000002.2170553211.00000000002E1000.00000040.00000001.01000000.00000004.sdmp, MPGPH131.exe, 00000006.00000002.2119820314.00000000002E1000.00000040.00000001.01000000.00000004.sdmp, RageMP131.exe, 00000007.00000002.2020629490.0000000000611000.00000040.00000001.01000000.00000005.sdmp, RageMP131.exe, 00000008.00000002.2014597460.0000000000611000.00000040.00000001.01000000.00000005.sdmp	false		high
http://https://support.mozilla.org	3b6N2Xdh3CYwplaces.sqlite.8.dr	false		high
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	ELASOvMcSsNrHistory.7.dr, vd0z8wzGefD1History.8.dr, LhmhqtkXTkbYHistory.0.dr, iCl1DNg_vvFNHistory.5.dr, QZolPj_wU7yvHistory.8.dr, BhPLdlMH4HviHistory.5.dr, UqNl41FdpO7sHistory.0.dr, OAwfuvRJ7Zo3History.7.dr	false		high
http://https://ipinfo.io:443/widget/demo/84.17.40.101	file.exe, 00000000.00000002.2023815185.000000001C71000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000002.2173403489.000000000174D000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000006.00000002.2121250052.0000000001647000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000002.2022464307.00000000019A2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000002.2015798047.0000000001938000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/risepro_bots	MPGPH131.exe, 00000005.00000002.2173403489.00000000017DE000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2056651399.00000000017DE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	file.exe, 00000000.00000003.1865241711.000000001D6B000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1864375367.0000000001D5A000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.1867863334.0000000001D78000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2099008633.00000000018B3000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2102021978.00000000018D2000.00000004.00000020.00020000.00000000.sdmp, MPGPH131.exe, 00000005.00000003.2105243412.00000000018E7000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820028873.0000000001A7A000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1822926347.0000000001A9F000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000007.00000003.1820619276.0000000001A9B000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1867422417.0000000001AD2000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1864465481.0000000001A98000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1865350119.0000000001ABC000.00000004.00000020.00020000.00000000.sdmp, DOGuPW8VgXDwWeb Data.5.dr, 1bA0iPxs1_tpWeb Data.8.dr, Z82s7O924lLeWeb Data.5.dr, Y7ezkClN3tvGWeb Data.0.dr, QALFCGqIe0GzWeb Data.8.dr, V9veGYQ701aZWeb Data.7.dr, 4deeADJYPmpQWeb Data.0.dr, pTWMc6sLNinTWeb Data.7.dr, 42h4yDt09kAFWeb Data.7.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://193.233.132.56/cost/go.execoin	RageMP131.exe, 00000008.00000003.1874959213.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, RageMP131.exe, 00000008.00000003.1874632671.0000000001A65000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	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
147.45.47.93	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:	1436950
Start date and time:	2024-05-06 20:07:05 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 9m 1s
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:	22
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@15/106@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
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.168.117.173, 52.182.143.212
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, ocsp.digicert.com, onedsblobprdcus15.centralus.cloudapp.azure.com, slscr.update.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, 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
19:07:52	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run RageMP131 C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
19:07:53	Task Scheduler	Run new task: MPGPH131 HR path: C:\ProgramData\MPGPH131\MPGPH131.exe
19:07:53	Task Scheduler	Run new task: MPGPH131 LG path: C:\ProgramData\MPGPH131\MPGPH131.exe
19:08:00	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run RageMP131 C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
20:08:28	API Interceptor	80x Sleep call for process: MPGPH131.exe modified
20:08:29	API Interceptor	4x 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):	3188736
Entropy (8bit):	7.981027272062894
Encrypted:	false
SSDEEP:	98304:DInXnNqIvqO74jZlyPeYy+sOnc6FqoMD:yglSO7sZae+FcSMD
MD5:	51014F1C86736D8F91D432548062EBBF
SHA1:	6D0BAB0A443FF43C293F57DFACE65DFEA47501A9
SHA-256:	1845D2A25B628C6FF5E489F83FF975A0C8140BBEEB8EA05F5404A45EE2F9C7EA
SHA-512:	E05A72A5DEDE84005AEDB80884CE191180BFD811A5AA197E18B5D467170B1E6B534B42EEF3F37782355193663F952599D7EB6D0121A6F1ADB2019CB3B547187
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39% • Antivirus: Virustotal, Detection: 40%, 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....96f.....'.....@.....@... .. ..P.....\..... .....0.....6.....@.....:.....@.....P...P.....<.....@.....D..... .....@.....p...b...D.....@....rsrc.....@..@.....x.....(...p.....@....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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_MPGPH131.exe_f22e2bf49a32bf74f5adbe8cba848017948e65f7_0010bad0 _640263cb-49b4-41b7-b487-4b818315d5ea\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):	1.0905694034302293
Encrypted:	false
SSDEEP:	192:+CRlrSzZ8DX0N/QB6E6jjYZrSruBl9zuiFGZ24lO826t:BKZekN/QEjC9zuiFGY4lO8p
MD5:	AA33BA4BF670C5953A2F6849F09214EE
SHA1:	9654FA3E4E28A7A5EC9712BD477049F87717B9BC
SHA-256:	60351DC8F18704950DA6429CDCB7657CF90F1FD55EBA315194453D155F1A7904

SHA-512:	667BC52BE4258C36A5ACD14726F8841A8C276546B9E269DDEF15F85AEDBF8019134420E3C82870C1B7F1C613AD4DF17C7126C6C1C9329D47CFE56BA909DD883
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.=.1.3.3.5.9.4.9.2.5.2.3.6.1.6.6.8.2.3.....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.=.1.3.3.5.9.4.9.2.5.2.4.1.9.4.8.0.3.0.....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.=.6.4.0.2.6.3.c.b.-.4.9.b.4.-.4.1.b.7.-.b.4.8.7.-.4.b.8.1.8.3.1.5.d.5.e.a.....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.=.c.c.6.d.0.b.0.6.-.3.3.0.5.-.4.8.8.2.-.9.8.3.4.-.f.8.8.3.7.c.5.e.f.e.e.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.M.P.G.P.H.1.3.1...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.r.o.s.s.D.e.v.i.c.e.S.e.t.t.i.n.g.s.H.o.s.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.d.a.0.-.0.0.0.1.-.0.0.1.4.-.8.8.1.5.-.6.f.5.0.e.0.9.f.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.!.0.0.0.0.6.d.0.b.a.b.0.a.4.4.3.f.f.4.3.c.2.9.3.f.5.7.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RageMP131.exe_d8cfe4b0b9575b2ab71f14e55e4d6484872cb94_df5fde7b_aa9d6a92-8d2d-4559-99fe-1b134b7dfc56\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):	1.0964596449196107
Encrypted:	false
SSDEEP:	192:q4Es50W0MpLFgjYZrSruBF9zuiFGZ24IO8ilp:2s509MpLFgjC9zuiFGY4IO8ij
MD5:	C31F66AAD3C803A9195EE514D87571F5
SHA1:	3CD88A966E201D2B26E21456B1A9D2A4E4C1B92B
SHA-256:	91757B335D88B354A602F9841711687C8233E333C2211AE0B6D2E070D8990066
SHA-512:	0A1DF693A8AA45C2EF00B40EB6CBF35887AB0B119E85C15ED8927376B6EAE23BB2FF7557557C17BBD55222C0AB307685B34F0DDBB790B5D9F3B242043AB389B5
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.=.1.3.3.5.9.4.9.2.4.9.6.6.4.2.4.1.7.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.5.9.4.9.2.4.9.7.5.9.5.5.3.7.0.....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.=.a.a.9.d.6.a.9.2.-.8.d.2.d.-.4.5.5.9.-.9.9.f.e.-.1.b.1.3.4.b.7.d.f.c.5.6.....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.=.a.1.0.f.e.e.f.d.-.f.f.d.5.-.4.2.c.8.-.a.e.b.e.-.b.d.8.c.a.f.a.9.6.b.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.=.R.a.g.e.M.P.1.3.1...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.r.o.s.s.D.e.v.i.c.e.S.e.t.t.i.n.g.s.H.o.s.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.d.f.8.-.0.0.0.1.-.0.0.1.4.-.5.e.3.e.-.d.c.5.4.e.0.9.f.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.!.0.0.0.0.6.d.0.b.a.b.0.a.4.4.3.f.f.4.3.c.2.9.3.f.5.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RageMP131.exe_d8cfe4b0b9575b2ab71f14e55e4d6484872cb94_df5fde7b_f3afe759-c551-431a-a54b-014b05a40ae0\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):	1.0899393167777214
Encrypted:	false
SSDEEP:	192:vBUnW0W0MpLFgjTZrlyLB+EzuiFGZ24IO8il:5UnW09MpLFgjNEzuiFGY4IO8i
MD5:	2CA776CB2C6318C667E984C174AFB133
SHA1:	4BC3A2B560AAB09D12431FFA495939F944C53DA6
SHA-256:	6C7F40749FECF3111C83ECF8FF43F1585FACB4C409D8F831B06498E4456DC3EC
SHA-512:	BA0D5D032969503344857F6745266A106D48F2BDF87415E3DBBC24CB710DA3F14C3618D24EC89DE4ACD00512A45DDD4639E7272BF38A230706F42F0E03A291F7
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.=.1.3.3.5.9.4.9.2.5.0.0.1.5.8.8.7.2.5.....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.=.1.3.3.5.9.4.9.2.5.0.0.8.4.6.3.9.3.6.....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.=.f.3.a.f.e.7.5.9.-.c.5.5.1.-.4.3.1.a.-.a.5.4.b.-.0.1.4.b.0.5.a.4.0.a.e.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.=.c.3.3.0.3.1.5.d.-.7.f.3.c.-.4.1.f.8.-.8.9.9.0.-.7.7.d.9.6.2.3.4.b.1.5.3.....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.=.R.a.g.e.M.P.1.3.1...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.r.o.s.s.D.e.v.i.c.e.S.e.t.t.i.n.g.s.H.o.s.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.e.6.8.-.0.0.0.1.-.0.0.1.4.-.4.9.3.4.-.a.e.5.9.e.0.9.f.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.!.0.0.0.0.6.d.0.b.a.b.0.a.4.4.3.f.f.4.3.c.2.9.3.f.5.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_751fa919568148cae58711204775ef674bafd71f_50e30abd_2c1d9ae0-1b69-4126-ae64-d738448a55b5\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):	1.0843647047578129
Encrypted:	false
SSDEEP:	192:rPBlVv2PXh07VKrl3jxZrBruVzfzuiFGZ24IO8iB:Vf2vi7VKsjwfzuiFGY4IO8S

MD5:	9CD05F7201C84C3EAE853B7F6D11EB79
SHA1:	C69913D9107A9550DCD24C8FBAAC87EA493CD6EE
SHA-256:	7E562B75DF4D1B182C40666680F5773D52382E02AF2EE8C97C5C22A18B7DE357
SHA-512:	AF13F61976C03AE2758B6801CDC93FF1C6489C273804DCA22BBF2825FC69E0014CA86608568E697D4B11FDA4B27D7066FA22464DD7B8C86515CB51B7D51B229
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.=.1.3.3.5.9.4.9.2.5.0.0.4.8.2.9.0.2.4.....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.=.1.3.3.5.9.4.9.2.5.0.1.0.2.9.7.8.3.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.c.1.d.9.a.e.0.-.1.b.6.9.-.4.1.2.6.-.a.e.6.4.-.d.7.3.8.4.4.8.a.5.5.b.5.....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.=.9.3.d.f.3.2.1.a.-.d.3.8.9.-.4.b.1.a.-.b.c.e.2.-.7.7.6.6.a.6.c.d.e.e.4.f.....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.=.0.0.0.0.1.d.0.4.-.0.0.0.1.-.0.0.1.4.-.7.9.c.a.-.d.0.4.e.e.0.9.f.d.a.0.1.....T.a.r.g.e.t.A.p.p.l.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.!.0.0.0.0.6.d.0.b.a.b.0.a.4.4.3.f.f.4.3.c.2.9.3.f.5.7.d.f.a.c.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER144F.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 6 18:08:17 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	129244
Entropy (8bit):	1.8664892656470333
Encrypted:	false
SSDEEP:	384:R4IKedBfue6DB09Rj/MAaC/ak3eC36irjRv4AtqoT6PdbeJ5A3XziCG46Mh:KeHfue6DBUjDjswRv4xoqdKn+XMg
MD5:	F9F6B87B2052478E4B155A5705524DB8
SHA1:	B75BBB89FD21007880E55E5856E8B2FCC1811953
SHA-256:	418E0D7556EC9DC5E72AA0825EE4B9828DB616C32510FC77B91B512FCAD2491E
SHA-512:	541714E05BDB62BAFE8FADE90FDFA08EC6C3737E083E2A6DF989BE7B27C205D5FA3F131C1AA6E63D6FF24449FD3E43953E393BDD51C24285884F5343656C06F
Malicious:	false
Preview:	MDMP..a..... .....9f.....D.....H...X.....I....%.....$....U.....`.....8.....T.....M..L.....&.....'.....eJ.....(.. ....GenuineIntel.....T.....9f..... ..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\WER16F0.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8396
Entropy (8bit):	3.7025230006291654
Encrypted:	false
SSDEEP:	192:R6l7wVeJ6t606Y9VSUj3gmflJJRoprZ89biXsf0eGWm:R6lXJo606YvSUj3gmflJJRbicfS
MD5:	E6961886BC4A7B550AAF54ABD3849F11
SHA1:	F2C3E87EC9F01A616259B4F9C66866740B82CAEA
SHA-256:	1200C767DED18A9A0C8B1D9090F1D70141D3310BDA28D86C9ABF9C5FB42AB6CD
SHA-512:	8D6B440DAB44E3295104A062DD72ADF3809B3B89B357C9DB838FC47368EABE650333FFB19C5AEE2D39EC8E35FF91585963BACBBBBD5F8FAAFDF14E4B549DE241
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.>.7.6.7.2.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER172F.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4718
Entropy (8bit):	4.510283429940356
Encrypted:	false
SSDEEP:	48:cvIwWl8zsNJg77al9joWpW8VYmYm8M4JSfFqdQu+q81e0Tvz9effd:uIjfnI71B7VuJ0uKlend
MD5:	9A41A724EBF1E9CC1E1D6FC1FDB3DBBF
SHA1:	6BD16B91535283A61E6EE7FD473D288ED132F94B
SHA-256:	D5B8DDF8CB785699A78F105CFEA83D7E32CEE824ABC7C15318CEA00FB2189DD1

SHA-512:	36E323F23DABC97E2E6AE0422BE518EB4F15A8565F43FA1FE89184A0EC99F52A7C23BD6FAC57E5938C69D9216F60E8402028E1CCE3E3121601CA3855B1B2234 3
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="311590" />.. <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\WER220B.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 6 18:08:20 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	127924
Entropy (8bit):	1.8698917211657768
Encrypted:	false
SSDEEP:	384:51jiWdU0lISe6UuyEafkiToPX/XMmENHNiHLD5rwWKN/3oPH:GW+jSe6UuKfkaVKX5kWk3o/
MD5:	C8550F84FCB3CC9A144BC3D89C405C3C
SHA1:	F51039719BC58DB77F103C6775CE38CCEED458E1
SHA-256:	CAEBC1E69932E0B4BBCDD9ADAD22830F460A0CF7369BA720E24A924E935A9A69
SHA-512:	8C2F1C562E6DA9AD03ACFDC444F2ACE0FF05B5DF35330F3C5571D755DAE0341DF640E0FD96E715D9D078A2A14FE6CCFABC41822B76BCF5FABA76EC9735FB 3E4
Malicious:	false
Preview:	MDMP..a..... .....9f.....D.....X.....l...4%.....T.....`.....8.....T.....K.....%.....'.....eJ.....$(... ...GenuineIntel.....T.....h.....9f..... ..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\WER2333.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 6 18:08:20 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	128722
Entropy (8bit):	1.8718952625692038
Encrypted:	false
SSDEEP:	384:KOhkAVdUFE4suu69LBqtL0GPrh1LG77G8r+kp6N4WoErtFFHjy2lx03a:XV2FEfuu69ItbjhVG7lZw/Jlwa
MD5:	3FDD9DDD24F867247F550D79576492B5
SHA1:	CBB6B106E4E9A38AC7F27442A390EB76394D4516
SHA-256:	4BD6E64F1B061E12233D81586387E019CDCA3983F4EE4D40D9D0C30AEB570672
SHA-512:	CC514C666E3BF56F59EAC186B0298C1AFAA4814826382F1C9D5A9588DAA4C77D40006954C777DD6E5CF27EC722051B5A1323DCEDC7D6153544E7EFF536E3FE 0
Malicious:	false
Preview:	MDMP..a..... .....9f.....D.....H...X.....l....%.....U.....`.....8.....T.....N.....&.....'.....eJ.....(... ...GenuineIntel.....T.....v.9f.....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\WER2334.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8396
Entropy (8bit):	3.7010156450821152
Encrypted:	false
SSDEEP:	192:R6l7wVeJKN6r6Y9YSUb4gmflJJRopra89bOOsfTam:R6lXJY6r6YSSUb4gmflJJRuONff
MD5:	35D2004C8B1C4F58AF70EDAC2D347B77
SHA1:	C6DE8C24B7B7A32F81759DF12B072406EF95A652
SHA-256:	04CE5EB49FBA8D9C7F4A6F34D0CAF04B0697697D6D0B3BCAA073528AAC159919
SHA-512:	DFFC4F48A1E8A69D024D02368D207E6FF5EE6CB1E4116B28128DA5AC1EB831CDF571ADE17C532C3353BE1E65D1D9A11A114777DC9C32E6DAF1C5FC8FF94C6 9FC
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.>.7.7.8.4.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2364.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4718
Entropy (8bit):	4.5132178215338925
Encrypted:	false
SSDEEP:	48:cvIwWl8zsWJg77al9joWpW8VYSYm8M4JSfFo+q81WTvz9eQfd:uIjfsl71B7VyJpfleed
MD5:	224398A0D108958FB7ED8230FFE3B5EC
SHA1:	BF6C7E2EFDE59198909C1502CB36C819704688A0
SHA-256:	472A7539216723B5D1F7C8AFA77AF595C3104DCDA0CDEF7103A208A79A51AC76
SHA-512:	5C2B34CBD28B99FFCE63BCD5B168F3E9C8B719A9499E91AD66C433128C9F6E838A8CE84EB6B1E5675775F8176B54A83A3E92DE454813F0E2AAA6735E1581E8A8
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="311591" />.. <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\WER242E.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):	8376
Entropy (8bit):	3.6983318919204144
Encrypted:	false
SSDEEP:	192:R6l7wVeJrCG6rE6Y9dSUcZmgmfBtJJKprZ89bOOe0sf3am:R6lXJv6w6YnSUc4gmfrJJpOnf7
MD5:	C9E49EE149F5CE16D9DC0F377D895655
SHA1:	4FE1A3DBA67C58A31C6330AA8B3951A6CC37F3DD
SHA-256:	37CE4B8B644B3DFB082DC6BF495E23BBBB1C3632642EB5F2673DFE90F9DDC858
SHA-512:	72EA2E1253A4760A758DDB1C72014EE2E335C35862C0B5379981D75A330027227243F1E6CAC04C61CE7D956E82CFB1DAB8B58712011F4404B358969EA1224CCA
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.>.7.4.2.8.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER245E.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):	4.492181588108718
Encrypted:	false
SSDEEP:	48:cvIwWl8zsWJg77al9joWpW8VYlYm8M4JwwhfFA+q8qhskTvzCn/fd:uIjfsl71B7VRJyfKnHd
MD5:	D458114B6F7E01BD639DF7FEBB4916CB
SHA1:	51C5D93ED0FB43D2D48ABF19675D4ADAF9B822D1
SHA-256:	866CDE98BFD62F6BF7A6C22D5E1F0DE64847B93C3AC6F985D236B3DC5265A37F
SHA-512:	06AA5AADDD6B7FA5803B832D1676B3DE09BDA661F99434198CA3CE34F9DC5A49436A1DA86CDD07372B1E278B93D8247286596B10C78C1AE97C0BEB1644540FFC
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="311591" />.. <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\WER7D98.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 6 18:08:43 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	124194
Entropy (8bit):	1.8790490714345165
Encrypted:	false
SSDEEP:	384:+04+dlGue661ofmc58qELqtdiNcpBefBrt6RJ8TG0ROuf:8+LGue661ofzWqnycpOr+b0RXf
MD5:	666AD78D41360D232AFBD74E5088E4AF
SHA1:	8D3C807B86443A474F50855BB2293B8043912961
SHA-256:	784D43CA6CFD82D5923C30E95CE46BD122B0E6CA8533A0A6B4EF2804D8A3918A
SHA-512:	0494860663F59C75D99EE3F5D1D9DBB27B3A58D1B6013A5390165623EEDBAF94CE2BA7AACDEDDEE22828DB1F022DDE5EC22030F9E35B255CA61205726862CF0E
Malicious:	false
Preview:	MDMP..a..... .....9f.....H...(.....l...p%.....4....R.....`.....8.....T.....xL.....%.....'.....eJ.....`(.....GenuineIntel.....T.....y.9f.....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\WER7E83.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):	6384
Entropy (8bit):	3.7273716578467684
Encrypted:	false
SSDEEP:	192:R6l7wVeJfuJ6ntYiPJJcprB89bjnsfrqBm:R6lXJw6tYgJJPjsfh
MD5:	3919D0B5A08663536B506AE5758B9FFE
SHA1:	1BDA3AF002C47E682A7F1A718A7FFA4C21B42ED1
SHA-256:	C8533F1FAAD22712B4F70CD978122BF7705BDB47F0234AD1FC7A5FED095C55C6
SHA-512:	A6E05F0DFE3D61F17C4F285400BEC7C6710458A282D29480CF4D2BF1384F9F160DC8FD7FA456F25E379012E5150C36F21CBA27804AD30FC11620E78C7B9F3A5
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.>.7.5.8.4.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7EB3.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):	4.521361199821821
Encrypted:	false
SSDEEP:	48:cvIwWl8zsWJg77aI9joWpW8VY6Ym8M4Jk8zFP+q8xY1/TvzxkNfd:uIjfsI71B7VWJHNaU/5kRd
MD5:	F3BACA1D7789E4C51527FE225FB036A0
SHA1:	F7073469427 47E8E7C267084DC68792C5DCA7DAB
SHA-256:	740CA628ACD3BE0AB96F77E0A287931992B7D6364322F4DB5B711385BFB8348C
SHA-512:	3601C028B3B832EA997FBA6ADC10520F971BDE1CEEFB51FB5CD77B3BD421B8DABF2030671E336E8440CDF5B3609F1026E725B0160B4BDD20BD1F358A5E3ED54A
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="311591" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\Users\user\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):	3188736
Entropy (8bit):	7.981027272062894
Encrypted:	false
SSDEEP:	98304:DInXnNqIvqO74jZlyPeYy+sOnc6FqoMD:ygISO7sZae+FcSMD
MD5:	51014F1C86736D8F91D432548062EBBF
SHA1:	6D0BAB0A443FF43C293F57DFACE65DFEA47501A9
SHA-256:	1845D2A25B628C6FF5E489F83FF975A0C8140BBEEB8EA05F5404A45EE2F9C7EA
SHA-512:	E05A72A5DEDE84005AEDB80884CE191180BFD811A5AA197E18B5D467170B1E6B534B42EEF3F37782355193663F952599D7EB6D0121A6F1ADB2019CB3B547187
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39% • Antivirus: Virustotal, Detection: 40%, 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....96f.....'.....@.....@... .. ..P.....\.....0.....6.....@.....:.....@.....P...P.....<.....@.....D.....@.....p...b...D.....@....rsrc.....@..@.....x.....(...p.....@....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\9wBRx7ST9VOnJqni_JpioUs.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):	5526
Entropy (8bit):	7.899067442079574
Encrypted:	false
SSDEEP:	96:VTbWGzqeAoMq+YK0KF8cAJiI2i+uvUmGsFQT0ozoPCMHz3KJY9LpO:NqASpF8wF+hFQ0koPl6Jb
MD5:	5FC9973F4733EB3DA520CD2B5F842AC6
SHA1:	56834308A0D9A532070C01D8D6AB59539A6DE240
SHA-256:	CFCF7416481CB10ED8D5A2B87DE7AC638BEA81AD3DD5B498BD26B9185C0FD28D
SHA-512:	97D52200FB94EDC3A06112AEF3F7B917053A42E02E4D2139CB804B65B365F90593E437BE6155139411B7D9BF29B788F0F35F1EFE2EA6BB8F56412074363217C7
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: C:\Users\user\AppData\Local\Temp\9wBRx7ST9VOnJqni_JpioUs.zip, Author: Joe Security

Preview:	PK.....X.....Cookies\..PK.....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.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\PSdiYEtw_DOSPKoK_uBheap.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):	5593
Entropy (8bit):	7.897308670656991
Encrypted:	false
SSDEEP:	96:WYWGzqeAoMq+YK0KF8cAJiI2i+uVrV0C/SAcrQb1o8ygX3KJvx:RqASpF8wFqa8SP8v6JZ
MD5:	EAC7219D7514E3DB624FD2DFA63C5985
SHA1:	AC7D38B5171840603101CF3BD8ABC604FFAEEF63
SHA-256:	D86D27A46CBC1DD538D02498EC5E03BFDB71DFE5F294EDDA9DA33D354EC94895
SHA-512:	063768A2A0CE9ED77CAD8AF74D4C89FE37CD2AB11AB7557C21AE90FE189F3C7F92802395799FD67A92C136C1F45A5BD5BA7BD9E5B62E7187B6579F1B710920D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: C:\Users\user\AppData\Local\Temp\PSdiYEtw_DOSPKoK_uBheap.zip, Author: Joe Security
Preview:	PK.....X.....Cookies\..PK.....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.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\rage131MP.tmp

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.71929452566698
Encrypted:	false
SSDEEP:	3:LXRJQn:bRen
MD5:	1FCDAF381F15F605ABAAFF8DE3887A8B
SHA1:	6940164F10801D9DA5792A4DDF59C4FAF2063B64
SHA-256:	46EC0FC8056E99872F7040240226EED9F44C4BEF644630C1F7B06C8F88DC4514
SHA-512:	4CFBA1A1A825C6EFAA0FE90C27CE924381F975E6A17C80A6495BBCC3A39AD6A9059071898632C61FCF8055082391C8A473ADDC62D1C501F8FA572A448898207
Malicious:	false
Preview:	1715022640625

C:\Users\user\AppData\Local\Temp\spanHju_g2DxItFq\02zdBXl47cvzcookies.sqlite

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\1bA0iPxs1_tpWeb Data	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\3b6N2Xdh3CYwplaces.sqlite	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\7Ndzc20NqBT6Login Data	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\D87fZN3R3jFeplaces.sqlite	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\LjKc4cZCdkn6Login Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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+lIF7CVEq8Ma0D0HOlf/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\spanHju_g2DxItFq\N00nD6NyQ3cLCookies

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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:/xealJiyIsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOI:/xGZR8wbtxq5uWRHKloIN7Yltnb6Ggz
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\spanHju_g2DxItFq\NxTOOE3P877HHistory

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\QALFCGqIe0GzWeb Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\QZolPj_wU7yvHistory

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\spanHju_g2DxItFq\S9TwIATY7544Web Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1 8
Malicious:	false

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

C:\Users\user\AppData\Local\Temp\spanHju_g2DxItFq\Y4Fgx64HQvbuWeb Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\a7mDNvwnbxnHLogin Data For Account

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\erLXBsfZOb13History

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\m736MhFnnhWLWeb Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\ru4TymmQRM2zWeb Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanHju_g2DxItFq\vd0z8wzGefD1History

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spanMW7ZIM5Bq6VF\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, cook ie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08235737944063153

Encrypted:	false
SSDEEP:	12:DQAsfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQAsff32mNVpP965Ra8KN0MG/lO
MD5:	369B6DD66F1CAD49D0952C40FEB9AD41
SHA1:	D05B2DE29433FB113EC4C558FF33087ED7481DD4
SHA-256:	14150D582B5321D91BDE0841066312AB3E6673CA51C982922BC293B82527220D
SHA-512:	771054845B27274054B6C73776204C235C46E0C742ECF3E2D9B650772BA5D259C8867B2FA92C3A9413D3E1AD35589D8431AC683DF84A53E13CDE361789045928
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....}..}..... ....

C:\Users\user\AppData\Local\Temp\spanMW7ZIM5Bq6VF\1TlhGNMGRIBAHistory

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\spanMW7ZIM5Bq6VF\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, 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\spanMW7ZIM5Bq6VF\4deeADJYPmpQWeb 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:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....l.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\spanMW7ZIM5Bq6VF\8ZyHikzPP6RfHistory

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:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F79838
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Temp\spanMW7ZIM5Bq6VF\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, 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\spanMW7ZIM5Bq6VF\lp1jlTBVvpfpWeb 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:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D8
Malicious:	false

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

C:\Users\user\AppData\Local\Temp\spanMW7ZIM5Bq6VF\KD92s1mFJPJgLogin 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:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\spanMW7ZIM5Bq6VF\K_LAuSWvaNiyWeb 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:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\spanMW7ZIM5Bq6VF\LhmhqtkXTkbYHistory

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+UlYysX0lxQzh/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\spanMW7ZIM5Bq6VF\N6snpryO8uf5Login 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\spanMW7ZIM5Bq6VF\OXHUVahmxrt1Cookies

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:/xealJiylsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOl:/xGZR8wbtxq5uWRHKloIN7Yltnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C27819621(3
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\Users\user\AppData\Local\Temp\spanMW7ZIM5Bq6VF\TLE_gXdWplrQLogin 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:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88 F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\spanMW7ZIM5Bq6VF\UqNl41FdpO7sHistory

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+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\spanMW7ZIM5Bq6VF\Y7ezkClN3tvGWeb 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\spanMW7ZIM5Bq6VF\c_G5qyHoUqdbWeb 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\spanMW7ZIM5Bq6VF\sQSDtQYbXNYdWeb 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:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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\spanVDXBLDHnzSSM\0bTBLNjSXQ3WWeb 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\spanVDXBLDHnzSSM\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\spanVDXBLDHnzSSM\BhPLdlMH4HviHistory

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+UlYysX0lxQzh/tsVL:8Ys3QMmRtH+bF+Ul3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0
SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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, 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\spanVDXBLDHnzSSM\DOGuPW8VgXDwWeb 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\spanVDXBLDHnzSSM\Hveaex_QIWEUWeb 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\spanVDXBLDHnzSSM\S1kWLfoUHhbSLogin 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\spanVDXBLDHnzSSM\Ss_aLcG4kfDuHistory	
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\spanVDXBLDHnzSSM\Z82s7O924lLeWeb 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\spanVDXBLDHnzSSM\ZhaKbTXVRlMcLogin 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\spanVDXBLDHnzSSM\iCl1DNg_vvFNHistory

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+UlYysX0lxQzh/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\spanVDXBLDHnzSSM\ruxveYYrnNxbWeb 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\spanVDXBLDHnzSSM\suF4nwudmtWhCookies

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:/xGZR8wbtxq5uWRHKloIN7Yltnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C27819621C3
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$.....

C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\uxiBTU0fcTIoHistory

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\spanVDXBLDHnzSSM\yabQsRD6rxEWLogin 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\spanVDXBLDHnzSSM\ycP9pvgLeKxDWeb 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\spansEwF_O0f6T2F\02zdBXl47cvzcookies.sqlite	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cook ie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08235737944063153
Encrypted:	false
SSDEEP:	12:DQAsfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQAsff32mNVpP965Ra8KN0MG/lO
MD5:	369B6DD66F1CAD49D0952C40FEB9AD41
SHA1:	D05B2DE29433FB113EC4C558FF33087ED7481DD4
SHA-256:	14150D582B5321D91BDE0841066312AB3E6673CA51C982922BC293B82527220D
SHA-512:	771054845B27274054B6C73776204C235C46E0C742ECF3E2D9B650772BA5D259C8867B2FA92C3A9413D3E1AD35589D8431AC683DF84A53E13CDE361789045928
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....}..}..... ....

C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\3b6N2Xdh3CYwplaces.sqlite	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\42h4yDt09kAFWeb Data	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\D87fZN3R3jFeplaces.sqlite	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\ELASOvMcSsNrHistory	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\HQFayTHWA4CIWeb Data	
Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\OAwfuvRJ7Zo3History

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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+UlYysX0lxQzh/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\spansEwF_O0f6T2F\OrF8rFJrkbX9Web Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\UaBkH_1UtTljHistory

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\V9veGYQ701aZWeb Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\cCZagzzOxnzSLogin Data For Account

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\h7vTUP6iIQXbLogin Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\kGWzVJBhnyHSCookies

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\l9WMfadWVY3RHistory

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\ne2K7r4K6MmbWeb Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\pSuV50rXNRR3Login Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\spansEwF_O0f6T2F\pTWMc6sLNinTWeb Data

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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\tC131VXqxqwXyoqOe7muh9i.zip

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	5574
Entropy (8bit):	7.898028478345893
Encrypted:	false
SSDEEP:	96:RWGzqeAoMq+YK0KF8cAJiI2i+uZ7czpYizCaGnwdUUt0S3KJ2G:VqASpF8wFOIzTfZdUUOS6J2G
MD5:	181A27FA5AF5932F05CBA9FE173536AE
SHA1:	E2FA21601E1FFC2FEE7270F173EC6E3D6F835E12
SHA-256:	1FB0A2B4677EC01D15EEE4828D78D6DFEA081F662AF47AB74F7A628DF82BDC5B
SHA-512:	4BC872A05C20C7BF8D5F8DF2300799CAD9FB30363C91A95B6636E999DE0D4236DDAF8CE73007C34F5FB0770CB8F5D8EF878EF19419F6823522651C11F6F15A3
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: C:\Users\user\AppData\Local\Temp\tC131VXqxqwXyoqOe7muh9i.zip, Author: Joe Security
Preview:	PK.....X.....Cookies\..PK.....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.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\trixyHju_g2DxItFq\Cookies\Chrome_Default.txt

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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+H13M00HIdLm+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 _OVCqFkLEwhvzeADNQOF5RSmkDfh5RqfqlOkx5QWo4Lltvwb0CvwBFD8ujlm3BAgIOeGca3ZatkLMUkH

C:\Users\user\AppData\Local\Temp\trixyHju_g2DxItFq\information.txt

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	6597
Entropy (8bit):	5.381904966077102
Encrypted:	false
SSDEEP:	96:xdQ4zn5RoEcT4Aisph+9hcmpN8Xa77Y6lANUbg3x:xqECEvAtphWhcmpN8Xa7sB
MD5:	0E695507ED2A8C5FF8124A8AF693AE01
SHA1:	01CED25903043763C9CE64EEA02556A7B3D43ED7
SHA-256:	3E790E17AE8188098232BE6EF2FD222C7DADA28AFA96EA285624BE80047BDF63
SHA-512:	C860C7D495E6A21BCCCCCFB158F416CE8B520806C39C114A6242D3B1B74D000C2540F92822FCC198A614D857E1B73AB4F8439E8168C8BE5C3089F7BFE6B1FF 2
Malicious:	false
Preview:	Build: domen..Version: 2.0....Date: Mon May 6 20:08:16 2024.MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06..GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6 963}..HWID: 7e55834bc82db041109988ce9c6b5293....Path: C:\Users\user\AppData\Local\RageMP131\RageMP131.exe..Work Dir: C:\Users\user\AppData\Local\Temp\ trixyHju_g2DxItFq....IP: 84.17.40.101..Location: US, Miami..ZIP (Autofills): -..Windows: Windows 10 Pro [x64]..Computer Name: 936905 [WORKGROUP]..User Name: use r..Display Resolution: 1280x1024..Display Language: en-CH..Keyboard Languages: English (United Kingdom) / English (United Kingdom)..Local Time: 6/5/2024 20:8:16 ..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]..svch ost.exe [752]..fontdrvhost.exe [776]..fontdrvho

C:\Users\user\AppData\Local\Temp\trixyHju_g2DxItFq\passwords.txt

Process:	C:\Users\user\AppData\Local\RageMP131\RageMP131.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:	B17ADF4AA80CADC581A09C72800DA22F62E5FB32953123F2C513D2E88753C430CC996E82AAE7190C8CB3340FCF2D9E0D759D99D909D2461369275FBE5C68C2 A
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\trixyMW7ZIM5Bq6VF\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:	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+H13M00HIdLm+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 _OVCqFkLEwhvzeADNQOF5RSmkDfh5RqfqlOkx5QWo4LItvwb0CvwBFD8ujlm3BAgIOeGca3ZatkLMUkH

C:\Users\user\AppData\Local\Temp\trixyMW7ZIM5Bq6VF\information.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	6576
Entropy (8bit):	5.373448179428926
Encrypted:	false
SSDEEP:	96:xdQ4zZ5RoEcT4Aisph+9hcmpN8Xa77Y6lANUbg3x:xq4CEvAtphWhcmpN8Xa7sB
MD5:	930E032F5DEA77A44698333A52DEFB69
SHA1:	A74D3CD49EC58C26376E4BC88414306DD76B822D
SHA-256:	3B9826CE5FA664406D0C5F2910C50361C4533B3696B41F74FA8EC0D4A7450DCF
SHA-512:	BC62D5CA2610E9E8112676798CF8C7D7010AC32E77FE2B79C4CC1DAD1CFE7E7FC0343914D2EE4603E5AC5A4CC3B5DEE89033D9D7A67E0A078AAFEB8D5B6C FC50
Malicious:	false
Preview:	Build: domen..Version: 2.0....Date: Mon May 6 20:08:16 2024.MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06..GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6 963}..HWID: 7e55834bc82db041109988ce9c6b5293....Path: C:\Users\user\Desktop\file.exe..Work Dir: C:\Users\user\AppData\Local\Temp\trixyMW7ZIM5Bq6VF....IP: 84.17.40.101..Location: US, Miami..ZIP (Autofills): -..Windows: Windows 10 Pro [x64]..Computer Name: 936905 [WORKGROUP]..User Name: user..Display Resolution: 1280x1024..Display Language: en-CH..Keyboard Languages: English (United Kingdom) / English (United Kingdom)..Local Time: 6/5/2024 20:8:16..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]..fontdr vhost.exe [776]..fontdrvhost.exe [784]..svchost

C:\Users\user\AppData\Local\Temp\trixyMW7ZIM5Bq6VF\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:	48:4MMMMMMMMMdMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMMMdMMMMMMMM3:q
MD5:	B3E9D0E1B8207AA74CB8812BAAF52EAE
SHA1:	A2DCE0FB6B0BBC955A1E72EF3D87CADCC6E3CC6B
SHA-256:	4993311FC913771ACB526BB5EF73682EDA69CD31AC14D25502E7BDA578FFA37C
SHA-512:	B17ADF4AA80CADC581A09C72800DA22F62E5FB32953123F2C513D2E88753C430CC996E82AAE7190C8CB3340FCF2D9E0D759D99D909D2461369275FBE5C68C2 A
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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+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\trixyVDXBLDHnzSSM\information.txt

Process:	C:\ProgramData\MPGPH131\MPGPH131.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	6392
Entropy (8bit):	5.373770793597438
Encrypted:	false
SSDEEP:	96:xd+4zq5RoKLcT4Aisph+9hcBp18B77Y6YANUbg3x:xI3CKLvAtphWhcBp18B7nB
MD5:	A70CF1A3EB112594FC8FE6A68FF29338
SHA1:	7A9F13419E522DCE27508415D8A68F6A9F303B96
SHA-256:	F3EF57433D1876FDC9F35E989E076F3D2DCD1952FC512BADF4B604D69B03988D
SHA-512:	D44A121050C62FC25654BDE6CBDD803DA4F99203798DB319E0BC6D2AB279B7C2C2EC38BA52CB06B9F554D03BB8A0F4D4CEB0911D5A37F0BD921D38CADFC7130
Malicious:	false
Preview:	Build: domen..Version: 2.0....Date: Mon May 6 20:08:47 2024.MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06..GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}..HWID: 7e55834bc82db041109988ce9c6b5293....Path: C:\ProgramData\MPGPH131\MPGPH131.exe..Work Dir: C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM....IP: 84.17.40.101..Location: US, Miami..ZIP (Autofills): -..Windows: Windows 10 Pro [x64]..Computer Name: 936905 [WORKGROUP]..User Name: user..Display Resolution: 1280x1024..Display Language: en-CH..Keyboard Languages: English (United Kingdom) / English (United Kingdom)..Local Time: 6/5/2024 20:8:47..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]..sv

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.981027272062894
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:	3'188'736 bytes
MD5:	51014f1c86736d8f91d432548062ebbf
SHA1:	6d0bab0a443ff43c293f57dface65dfea47501a9
SHA256:	1845d2a25b628c6ff5e489f83ff975a0c8140bbeeb8ea05f5404a45ee2f9c7ea
SHA512:	e05a72a5dede84005aedb80884ce191180bfd811a5aa197e18b5d467170b1e6b534b42eef3f37782355193663f952599d7eb6d0121a6f1adb2019cb3b547187d
SSDEEP:	98304:DlnXnNqIvqO74jZlyPeYy+sOnc6FqoMD:yglSO7sZae+FcSMD
TLSH:	80E5331035537 54DF91C23BB0B7E4BB213606CB76A520BE7926D391FAAEB5C876084E2
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:	0xf5ca8c
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:	0x663639CA [Sat May 4 13:36:10 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	272279f18f704f637aa129691266b291

Entrypoint Preview
Instruction
jmp 00007F8A1D4E259Ah
add byte ptr [eax+0000000Eh], bl
add byte ptr [eax], al
pushad
call 00007F8A1D4E2595h
pop ebp
sub ebp, 00000010h
sub ebp, 00B5CA8Ch
jmp 00007F8A1D4E2599h
and dword ptr [esi+edx-357347C5h], 000300B5h
add eax, 0000004Ch
mov ecx, 000005B0h
mov edx, E63CE4B7h
xor byte ptr [eax], dl
inc eax
dec ecx
jne 00007F8A1D4E258Ch
jmp 00007F8A1D4E2599h
cmp eax, 3CBFE389h
jp 00007F8A1D4E25CEh
mov esi, dword ptr [edi+7636B7B7h]
dec edi
mov bh, B7h
mov bh, B4h
jp 00007F8A1D4E25A1h
mov cl, B7h
mov bh, B7h
or eax, B7B7B79Fh
inc eax
push ebp
mov ah, 7Fh
cmp al, 36h
mov ebx, B4B7B7B7h
jc 00007F8A1D4E25CCh
rcl dword ptr [ebx-6C4CC1B5h], cl
cmp dl, bl
xchg eax, ebx
dec ebx

Instruction
mov bl, 93h
fbld [edi-20486910h]
retf
xor al, 23h
mov bh, B6h
wait
xchg eax, ebx
fistp qword ptr [edi]
leave
sub bl, 0000005Fh
mov dl, B7h
mov bh, B7h
pop esi
xchg dword ptr [edi-2CC54849h], esi
xchg eax, ebx
dec ebx
wait
xchg eax, ebx
cmp bl, bl
xchg eax, ebx
mov bh, 3Ch
xor bh, byte ptr [edi+3CB7B7B7h]
and bh, byte ptr [ebx+3CB7B7B7h]
cmp ah, byte ptr [edi+76B7B7B7h]
pop esi
mov ch, 86h
mov ch, 34h
jne 00007F8A1D4E2545h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x940050	0xd0b	.data
IMAGE_DIRECTORY_ENTRY_IMPORT	0x940d5c	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	0x940030	0x10	.data
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x940000	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	
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	0x93600	1c30c55f327dff326a32a79b19e348d6	False	0.9999685247031382	data	7.999675017725288	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x15d000	0x28000	0x10200	74548ae799e79fc20306cc602d37a794	False	0.9983648255813954	data	7.99639087266641	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
	0x185000	0x5000	0x800	3818ed903188218960f33e014f774303	False	0.9970703125	data	7.83802229172669	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	190e1a61abc7d6a0a7c981417fcc65a3	False	0.9881616709183674	data	7.972593331740996	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	0x78f000	0x32800	06bf0b39137a35cdc92c7a5f4bd29b27	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.data	0x93d000	0x221000	0x221000	09fd6339de78073bdda8de6df01391d2	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
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

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
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	

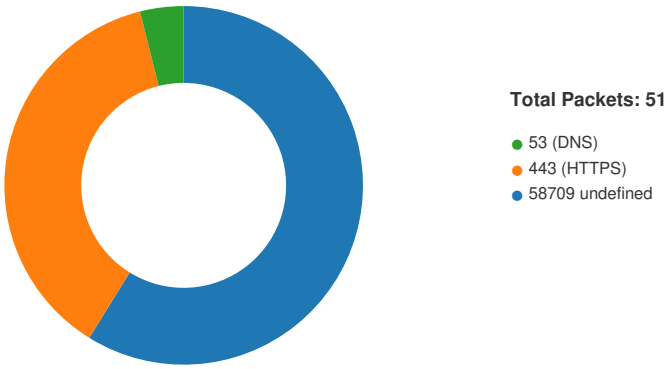
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/06/24-20:08:42.332746	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49731	58709	192.168.2.4	147.45.47.93
05/06/24-20:08:11.803337	TCP	2046267	ET TROJAN [ANY.RUN] RisePro TCP (External IP)	58709	49730	147.45.47.93	192.168.2.4
05/06/24-20:07:53.913307	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49730	147.45.47.93	192.168.2.4
05/06/24-20:07:57.036164	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49730	58709	192.168.2.4	147.45.47.93
05/06/24-20:07:53.682907	TCP	2049060	ET TROJAN RisePro TCP Heartbeat Packet	49730	58709	192.168.2.4	147.45.47.93
05/06/24-20:08:04.120685	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49733	147.45.47.93	192.168.2.4
05/06/24-20:08:05.646832	TCP	2046267	ET TROJAN [ANY.RUN] RisePro TCP (External IP)	58709	49733	147.45.47.93	192.168.2.4
05/06/24-20:07:56.321028	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49732	147.45.47.93	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/06/24-20:08:18.051763	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49738	58709	192.168.2.4	147.45.47.93
05/06/24-20:07:56.309289	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49731	147.45.47.93	192.168.2.4
05/06/24-20:08:11.640975	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	58709	49738	147.45.47.93	192.168.2.4
05/06/24-20:08:15.381006	TCP	2046267	ET TROJAN [ANY.RUN] RisePro TCP (External IP)	58709	49731	147.45.47.93	192.168.2.4
05/06/24-20:08:11.897367	TCP	2046267	ET TROJAN [ANY.RUN] RisePro TCP (External IP)	58709	49738	147.45.47.93	192.168.2.4
05/06/24-20:08:09.259896	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49733	58709	192.168.2.4	147.45.47.93
05/06/24-20:08:30.364347	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49732	58709	192.168.2.4	147.45.47.93

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 20:07:53.429881096 CEST	49730	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:53.671523094 CEST	58709	49730	147.45.47.93	192.168.2.4
May 6, 2024 20:07:53.671605110 CEST	49730	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:53.682907104 CEST	49730	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:53.913306952 CEST	58709	49730	147.45.47.93	192.168.2.4
May 6, 2024 20:07:53.957776070 CEST	49730	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:53.976671934 CEST	58709	49730	147.45.47.93	192.168.2.4
May 6, 2024 20:07:55.824038982 CEST	49731	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:55.824769974 CEST	49732	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:56.065807104 CEST	58709	49731	147.45.47.93	192.168.2.4
May 6, 2024 20:07:56.065886021 CEST	49731	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:56.066797018 CEST	58709	49732	147.45.47.93	192.168.2.4
May 6, 2024 20:07:56.066957951 CEST	49732	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:56.071782112 CEST	49732	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:56.072952032 CEST	49731	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:56.309288979 CEST	58709	49731	147.45.47.93	192.168.2.4
May 6, 2024 20:07:56.321027994 CEST	58709	49732	147.45.47.93	192.168.2.4
May 6, 2024 20:07:56.364065886 CEST	49731	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:56.364069939 CEST	49732	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:56.367609978 CEST	58709	49731	147.45.47.93	192.168.2.4
May 6, 2024 20:07:57.036164045 CEST	49730	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:57.320930958 CEST	58709	49730	147.45.47.93	192.168.2.4
May 6, 2024 20:07:59.426615953 CEST	49731	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:59.457962036 CEST	49732	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:07:59.711488008 CEST	58709	49731	147.45.47.93	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 20:07:59.742330074 CEST	58709	49732	147.45.47.93	192.168.2.4
May 6, 2024 20:08:03.631109953 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:03.875864983 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:03.875960112 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:03.885246992 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:04.120685101 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:04.176578999 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:04.182113886 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:05.646831989 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:05.692157030 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:05.936779976 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:05.989051104 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:06.098227024 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:06.103302002 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:06.103332996 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:06.103409052 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:06.106945992 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:06.106961966 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:06.339298964 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:06.339395046 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:06.341357946 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:06.341366053 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:06.341618061 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:06.384519100 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:06.395313978 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:06.418107986 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:06.464109898 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:06.599848032 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:06.599961042 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:06.603946924 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:08.198303938 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:08.198335886 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:08.198354006 CEST	49734	443	192.168.2.4	34.117.186.192
May 6, 2024 20:08:08.198359966 CEST	443	49734	34.117.186.192	192.168.2.4
May 6, 2024 20:08:08.373500109 CEST	49735	443	192.168.2.4	104.26.5.15
May 6, 2024 20:08:08.373542070 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.373617887 CEST	49735	443	192.168.2.4	104.26.5.15
May 6, 2024 20:08:08.373917103 CEST	49735	443	192.168.2.4	104.26.5.15
May 6, 2024 20:08:08.373934031 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.604105949 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.604253054 CEST	49735	443	192.168.2.4	104.26.5.15
May 6, 2024 20:08:08.606523991 CEST	49735	443	192.168.2.4	104.26.5.15
May 6, 2024 20:08:08.606535912 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.606745005 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.607738972 CEST	49735	443	192.168.2.4	104.26.5.15
May 6, 2024 20:08:08.652112007 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.964488983 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.964575052 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.964665890 CEST	49735	443	192.168.2.4	104.26.5.15
May 6, 2024 20:08:08.964890957 CEST	49735	443	192.168.2.4	104.26.5.15
May 6, 2024 20:08:08.964917898 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.964930058 CEST	49735	443	192.168.2.4	104.26.5.15
May 6, 2024 20:08:08.964935064 CEST	443	49735	104.26.5.15	192.168.2.4
May 6, 2024 20:08:08.965241909 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:09.259840012 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:09.259896040 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:09.266164064 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:09.317173004 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:09.556468010 CEST	58709	49733	147.45.47.93	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 20:08:09.556528091 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:09.561661959 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:09.614058971 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:09.853571892 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:09.858696938 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:09.910964012 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:09.942348957 CEST	49733	58709	192.168.2.4	147.45.47.93
May 6, 2024 20:08:10.222027063 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:10.222080946 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:10.222093105 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:10.222107887 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:10.222120047 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:10.222131968 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:10.222142935 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:10.222156048 CEST	58709	49733	147.45.47.93	192.168.2.4
May 6, 2024 20:08:10.222155094 CEST	49733	58709	192.168.2.4	147.45.47.93

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 20:08:05.762731075 CEST	63557	53	192.168.2.4	1.1.1.1
May 6, 2024 20:08:05.874954939 CEST	53	63557	1.1.1.1	192.168.2.4
May 6, 2024 20:08:08.260582924 CEST	58175	53	192.168.2.4	1.1.1.1
May 6, 2024 20:08:08.372803926 CEST	53	58175	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 6, 2024 20:08:05.762731075 CEST	192.168.2.4	1.1.1.1	0x6e54	Standard query (0)	ipinfo.io	A (IP address)	IN (0x0001)	false
May 6, 2024 20:08:08.260582924 CEST	192.168.2.4	1.1.1.1	0xc7ac	Standard query (0)	db-ip.com	A (IP address)	IN (0x0001)	false

DNS Answers

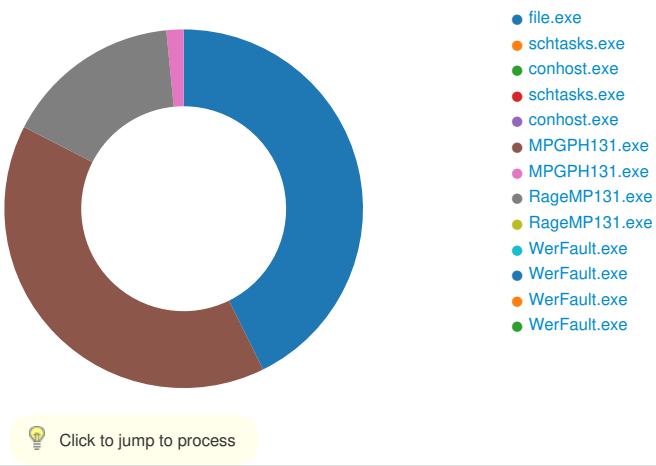
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 6, 2024 20:08:05.874954939 CEST	1.1.1.1	192.168.2.4	0x6e54	No error (0)	ipinfo.io		34.117.186.192	A (IP address)	IN (0x0001)	false
May 6, 2024 20:08:08.372803926 CEST	1.1.1.1	192.168.2.4	0xc7ac	No error (0)	db-ip.com		104.26.5.15	A (IP address)	IN (0x0001)	false
May 6, 2024 20:08:08.372803926 CEST	1.1.1.1	192.168.2.4	0xc7ac	No error (0)	db-ip.com		172.67.75.166	A (IP address)	IN (0x0001)	false
May 6, 2024 20:08:08.372803926 CEST	1.1.1.1	192.168.2.4	0xc7ac	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: 7428, Parent PID: 2580

General

Target ID:	0
Start time:	20:07:50
Start date:	06/05/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0xf70000
File size:	3'188'736 bytes
MD5 hash:	51014F1C86736D8F91D432548062EBBF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000002.2023815185.0000000001CEC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000003.1907164226.0000000001CE6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.2023815185.0000000001C7E000.00000004.00000020.00020000.00000000.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	103FEDF	RegSetValueExA

Analysis Process: schtasks.exe PID: 7488, Parent PID: 7428

General

Target ID:	1
Start time:	20:07:52

Start date:	06/05/2024
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:	0xeb0000
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: 7496, Parent PID: 7488

General

Target ID:	2
Start time:	20:07:52
Start date:	06/05/2024
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: schtasks.exe PID: 7536, Parent PID: 7428

General

Target ID:	3
Start time:	20:07:52
Start date:	06/05/2024
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:	0xeb0000
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: 7544, Parent PID: 7536

General

Target ID:	4
Start time:	20:07:52
Start date:	06/05/2024
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: 7584, Parent PID: 1044

General

Target ID:	5
Start time:	20:07:53
Start date:	06/05/2024
Path:	C:\ProgramData\MPGPH131\MPGPH131.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\MPGPH131\MPGPH131.exe
Imagebase:	0x2e0000
File size:	3'188'736 bytes
MD5 hash:	51014F1C86736D8F91D432548062EBBF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000005.00000002.2173403489.0000000001838000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000005.00000003.2110910326.0000000001838000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2173403489.00000000017DE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000005.00000002.2173403489.000000000174D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs • Detection: 40%, 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\trixyVDXBLDHnzSSM	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	33A4D7	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	33A4FD	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\S1kWLfoUHhbSLogin 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ZhaKbTXVRlMcLogin 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\DOGuPW8VgXDwWeb 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\iCl1DNg_vvFNHistory	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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Z82s7O924lLeWeb 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\POQox6AEGKfdCookies	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	3B69A6	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\suF4nwudmtWhCookies	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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\BhPLdlMH4HviHistory	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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ycP9pvgLeKxDWeb 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\yabQsRD6rxEWLogin 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\1gXU59PpK6kvLogin 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\0bTBLNjSXQ3WWeb 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\uxiBTU0fcTIoHistory	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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ruxveYYrnNxbWeb 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\YkLhqolvvz3HCookies	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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Ss_aLcG4kfDuHistory	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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Hveaex_QIWEUWeb 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\passwords.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3229AF	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\information.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3229AF	CreateFileW
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	3C6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\Cookies\Chrome_Default.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3229AF	CreateFileW
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	3C6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EBA0A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	3C6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	3C6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EBAD4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EBD0A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EC0CE	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EC198	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EC577	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2ED29C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2ED6FA	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EDAD9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EDF3E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EE6FC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EF45D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	345C36	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EF527	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EF935	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EFC57	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2EFEF3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2F0F14	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2F1906	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2F1E70	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	2F1FC0	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	33E1C4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	33E908	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\9wBRx7ST9VOnJqni_JpioUs.zip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3229AF	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Ei8DrAmaYu9Ksignons.sqlite	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\8ghN89CsjOW1signons.sqlite	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\D87fZN3R3jFeplaces.sqlite	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\02zdBXl47cvzcookies.sqlite	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\S1kWLfoUHhbSLogin Data	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ZhaKbTXVRlMcLogin Data For Account	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\DOGuPW8VgXDwWeb Data	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\iCl1DNg_vvFNHistory	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Z82s7O924lLeWeb Data	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\POQox6AEGKfdCookies	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\suF4nwudmtWhCookies	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\BhPLdlMH4HviHistory	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ycP9pvgLeKxDWeb Data	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\yabQsRD6rxEWLogin Data	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\1gXU59PpK6kvLogin Data For Account	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\0bTBLNjSXQ3WWeb Data	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\uxiBTU0fcTloHistory	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ruxveYYrnNxbWeb Data	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\YkLhqolvvz3HCookies	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Ss_aLcG4kfDuHistory	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Hveaex_QIWEUWeb Data	success or wait	1	32B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\9wBRx7ST9VOnJqni_JpioUs.zip	success or wait	1	3A7071	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rage131MP.tmp	0	13	31 37 31 35 30 32 32 36 34 30 36 32 35	1715022640625	success or wait	1	329914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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	SQLite format 3@ .&K.j- a>~|0{ dzzz"yy3xxKwvuuGtt;sAs qpqp{ooh nnemn,m9lklPjjhhgdcc6b baa>	success or wait	10	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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	SQLite format 3@ .j}}	success or wait	1	3B69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\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	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAsqpqp{ooh nnemn,m9lklPjjhhgdcc6bbaa>	success or wait	10	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\S1kWLfoUHhbSLogin 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	SQLite format 3@ .j	success or wait	1	3B69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ZhaKbTXVRlMcLogin Data For Account	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\DOGuPW8VgXDwWeb 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	SQLite format 3@ 4!.j1	success or wait	1	3B69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\iCl1DNg_vvFNHistory	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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Z82s7O924lLeWeb 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	3B69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\suF4nwudmtWhCookies	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 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\BhPLdlMH4HviHistory	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	3B69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ycP9pvgLeKxDWeb 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	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\yabQsRD6rxEWLogin 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	3B69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\S1kWLfoUHhbSLogin 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 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 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	SQLite format 3@ .j	success or wait	1	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\uxiBTU0fcTIoHistory	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 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 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	3B69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ruxveYYrnNxbWeb 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	SQLite format 3@ 8$.O}4	success or wait	1	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Ss_aLcG4kfDuHistory	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	SQLite format 3@ .O}	success or wait	1	3B69A6	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Hveaex_QIWEUWeb 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	SQLite format 3@ 8$.O}4	success or wait	1	3B69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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/rK1XOX2BXUq6pY2LBCOzoXODiJnrrvDbDsPWiYwKZowg9PxHqkTm37HpwC52rXpnuUFrQMpV3iKtdSHegOm+XguZZ6tGaCY2hGVyR8JgIqQma1WLXyhCiWqjou7/c3qSeaKyNoUKHa4TULX4ZnNNtXFoCuZcBAAy4tYcz+0BF4j/0Pg+MgV+s7367kYcjO4q3zwc	success or wait	1	329914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	cationsTelemetryDeviceI dENC893 *_djEw/EPksTnBmMBEQ qS0rmqlx6ZY bbpImMscmfukl8V2fyhGf 6CsRyOrQA RnlruNucWLn8bXbu7+rM wrxEjHAI73 Xw==_b3i0u6LLcKCMUa F/UlQgEPSL9 PtLZ21CuT1dJkfCzME=* .c.bing.co mFALSE/TRUE17301092 81SRM_BENC8 93*_djEw7mVFtY5cZBm cSId9o+LO6pYxZGfe	success or wait	1	329914	WriteFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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 00 00 00 00 00 00 00 00		success or wait	1	329914	WriteFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\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	329914	WriteFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\information.txt	0	4096	42 75 69 6c 64 3a 20 64 6f 6d 65 6e 0d 0a 56 65 72 73 69 6f 6e 3a 20 32 2e 30 0d 0a 0d 0a 44 61 74 65 3a 20 4d 6f 6e 20 4d 61 79 20 20 36 20 32 30 3a 30 38 3a 34 37 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 37 65 35 35 38 33 34 62 63 38 32 64 62 30 34 31 31 30 39 39 38 38 63 65 39 63 36 62 35 32 39 33 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: domenVersion: 2.0Date: Mon May 6 20:08:47 2024Machin eID: 9e146be9-c76a- 4720-bcdb-5 3011b87bd06GUID: {a33c7340-61ca-11ee- 8c18- 806e6f6e6963}HWID: 7e55834bc82db04110998 8ce9c6b5293Path: C:\ProgramData\MPGPH 1 31\MPGPH131.exeWork Dir: C:\	success or wait	1	329914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\information.txt	4096	2296	66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 32 34 30 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 32 36 34 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 32 38 38 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 33 31 36 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 33 33 36 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 33 36 30 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 33 38 38 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78	flJqnBFxosBVJsIfxhS.exe [6240] OLflJqnBFxosBVJsIfxhS.exe [6264]OLflJqnBFxosBVJsIfxhS.exe [6288]OLflJqnBFxosBVJsIfxhS.exe [6316]OLflJqnBFxosBVJsIfxhS.exe [6336]OLflJqnBFxosBVJsIfxhS.exe [6360]OLflJqnBFxosBVJsIfxhS.exe [6388]OLflJqnBFxosBVJsIfx	success or wait	1	329914	WriteFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\information.txt	0	4096	42 75 69 6c 64 3a 20 64 6f 6d 65 6e 0d 0a 56 65 72 73 69 6f 6e 3a 20 32 2e 30 0d 0a 0d 0a 44 61 74 65 3a 20 4d 6f 6e 20 4d 61 79 20 20 36 20 32 30 3a 30 38 3a 34 37 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 37 65 35 35 38 33 34 62 63 38 32 64 62 30 34 31 31 30 39 39 38 38 63 65 39 63 36 62 35 32 39 33 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: domenVersion: 2.0Date: Mon May 6 20:08:47 2024MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06GUID: {a33c7340-61ca-11ee-8c18-806e6f6e6963}HWID: 7e55834bc82db041109988ce9c6b5293Path: C:\ProgramData\MPGPH131\MPGPH131.exeWork Dir: C:\	success or wait	1	329914	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\information.txt	4096	2296	66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 32 34 30 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 32 36 34 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 32 38 38 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 33 31 36 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 33 33 36 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 33 36 30 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78 68 53 2e 65 78 65 20 5b 36 33 38 38 5d 0d 0a 4f 4c 66 6c 4a 71 6e 42 46 78 6f 73 42 56 4a 73 49 66 78	flJqnBFxosBVJsIfxhS.exe [6240] OLflJqnBFxosBVJsIfxhS.exe [6264]OLflJqnBFxosBVJsIfxhS.exe [6288]OLflJqnBFxosBVJsIfxhS.exe [6316]OLflJqnBFxosBVJsIfxhS.exe [6336]OLflJqnBFxosBVJsIfxhS.exe [6360]OLflJqnBFxosBVJsIfxhS.exe [6388]OLflJqnBFxosBVJsIfx	success or wait	1	329914	WriteFile
C:\Users\user\AppData\Local\Temp\9wBRx7ST9VOnJqni_JpioUs.zip	0	40	50 4b 03 04 14 00 00 08 08 00 17 fd fd 58 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 43 6f 6f 6b 69 65 73 5c 03 00	PKXCookies\	success or wait	4	329914	WriteFile
C:\Users\user\AppData\Local\Temp\9wBRx7ST9VOnJqni_JpioUs.zip	14	12	00 00 00 00 02 00 00 00 00 00 00 00		success or wait	4	329914	WriteFile
C:\Users\user\AppData\Local\Temp\9wBRx7ST9VOnJqni_JpioUs.zip	5212	314	50 4b 01 02 00 0b 14 00 00 08 08 00 17 fd 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 17 fd 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 17 fd fd 58 fd fd 2e 69 fd 06 00 00 fd 18 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 17 fd 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 30 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	PKXCookies\PKXQn+(Cookies\Chrome_Default.txtPKX.iUinformation.txtPKXF!0passwords.txtPK	success or wait	1	329914	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\MPGPH131\MPGPH131.exe	0	64	success or wait	1	4EE562	NtReadFile
C:\ProgramData\MPGPH131\MPGPH131.exe	0	20	success or wait	1	4EE562	NtReadFile
C:\ProgramData\MPGPH131\MPGPH131.exe	0	1998848	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Ei8DrAmaYu9Ksignons.sqlite	0	100	end of file	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\8ghN89CsjOW1signons.sqlite	0	100	end of file	1	425968	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\D87fZN3R3jFeplaces.sqlite	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\D87fZN3R3jFeplaces.sqlite	0	32768	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\D87fZN3R3jFeplaces.sqlite	0	16	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\02zdBXl47cvzcookies.sqlite	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\02zdBXl47cvzcookies.sqlite	0	32768	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\02zdBXl47cvzcookies.sqlite	0	16	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\3b6N2Xdh3CYwplaces.sqlite	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\3b6N2Xdh3CYwplaces.sqlite	0	32768	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\S1kWLfoUHhbSLogin Data	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\S1kWLfoUHhbSLogin Data	0	2048	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	2	328BE4	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	2	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ZhaKbTXVRlMcLogin Data For Account	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ZhaKbTXVRlMcLogin Data For Account	0	2048	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\DOGuPW8VgXDwWeb Data	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\DOGuPW8VgXDwWeb Data	0	2048	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\iCl1DNg_vvFNHistory	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\iCl1DNg_vvFNHistory	0	4096	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\iCl1DNg_vvFNHistory	0	4096	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Z82s7O924lLeWeb Data	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Z82s7O924lLeWeb Data	0	2048	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\POQox6AEGKfdCookies	0	100	end of file	1	425968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\suF4nwudmtWhCookies	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\suF4nwudmtWhCookies	0	4096	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\suF4nwudmtWhCookies	0	4096	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\BhPLdlMH4HviHistory	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\BhPLdlMH4HviHistory	0	4096	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\BhPLdlMH4HviHistory	0	4096	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ycP9pvgLeKxDWeb Data	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	65536	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	0	4096	success or wait	1	328BE4	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	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\yabQsRD6rx EWLogin Data	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\yabQsRD6rx EWLogin Data	0	2048	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\1gXU59PpK6 kvLogin Data For Account	0	100	end of file	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\0bTBLNjSXQ 3WWeb Data	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\0bTBLNjSXQ 3WWeb Data	0	2048	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\uxiBTU0fcT loHistory	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\uxiBTU0fcT loHistory	0	4096	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\ruxveYYrnN xbWeb Data	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\YkLhqolvvz 3HCookies	0	100	end of file	1	425968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Ss_aLcG4kf DuHistory	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Ss_aLcG4kf DuHistory	0	4096	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM\Hveaex_QIW EUWeb Data	0	100	success or wait	1	425968	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\information.txt	0	4096	success or wait	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\Cookies\C hrome_Default.txt	0	4096	success or wait	2	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\Cookies\C hrome_Default.txt	0	4096	end of file	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\information.txt	0	4096	success or wait	2	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\information.txt	0	4096	end of file	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\passwords.txt	0	4096	success or wait	2	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\trixyVDXBLDHnzSSM\passwords.txt	0	4096	end of file	1	328BE4	ReadFile
C:\Users\user\AppData\Local\Temp\9wBRx7ST9VOnJqni_JpioUs.zip	0	4096	success or wait	1	328BE4	ReadFile

Analysis Process: MPGPH131.exe PID: **7592**, Parent PID: **1044**

General

Target ID:	6
Start time:	20:07:53
Start date:	06/05/2024
Path:	C:\ProgramData\MPGPH131\MPGPH131.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\MPGPH131\MPGPH131.exe
Imagebase:	0x2e0000
File size:	3'188'736 bytes
MD5 hash:	51014F1C86736D8F91D432548062EBBF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
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\trixyVDXBLDHnzSSM	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	33A4D7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\spanVDXBLDHnzSSM	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	33A4FD	CreateDirectoryA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rage131MP.tmp	0	13	31 37 31 35 30 32 32 36 34 30 36 32 35	1715022640625	success or wait	1	329914	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\MPGPH131\MPGPH131.exe	0	64	success or wait	1	4EE562	NtReadFile
C:\ProgramData\MPGPH131\MPGPH131.exe	0	20	success or wait	1	4EE562	NtReadFile
C:\ProgramData\MPGPH131\MPGPH131.exe	0	1998848	success or wait	1	328BE4	ReadFile
C:\ProgramData\MPGPH131\MPGPH131.exe	0	4096	success or wait	1	328BE4	ReadFile

Analysis Process: RageMP131.exe PID: **7672**, Parent PID: **2580**

General

Target ID:	7
Start time:	20:08:00
Start date:	06/05/2024
Path:	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\RageMP131\RageMP131.exe"
Imagebase:	0x610000
File size:	3'188'736 bytes
MD5 hash:	51014F1C86736D8F91D432548062EBBF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000007.00000002.2022464307.000000000191E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000007.00000002.2022464307.00000000019F4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs • Detection: 40%, 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\trixysEwF_O0f6T2F	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	66A4D7	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	66A4FD	CreateDirectoryA
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\z6bny8rn.default\signons.sqlite	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	754E09	CreateFileW
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\signons.sqlite	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	754E09	CreateFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\D87fZN3R3jFeplaces.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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\h7vTUP6ilQXbLogin 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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\cCZagzzOxnzSLogin 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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\V9veGYQ701aZWeb 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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\ELASOvMcSsNrHistory	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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\42h4yDt09kAFWeb 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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	754E09	CreateFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\kGWzVJBhnyHSCookies	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	6E69A6	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\OAwfuvRJ7Zo3History	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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\pTWMc6sLNinTWeb 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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\pSuV50rXNRR3Login 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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Login Data For Account	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	754E09	CreateFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\OrF8rFJrkbX9Web 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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\UaBkH_1UtTljHistory	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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\ne2K7r4K6MmbWeb 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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Cookies	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	754E09	CreateFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\l9WMfadWVY3RHistory	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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\HQFayTHWA4CIWeb 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	6E69A6	CopyFileA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\passwords.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6529AF	CreateFileW
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\information.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6529AF	CreateFileW
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	6F6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61BA0A	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61BAD4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	6F6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	6F6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61BD0A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\Cookies\Chrome_Default.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6529AF	CreateFileW
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	6F6BDB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61C0CE	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61C198	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61C577	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61D29C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61D6FA	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61DAD9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61DF3E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61E6FC	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61F45D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61F527	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61F935	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61FC57	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	61FEF3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	620F14	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	621906	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	621E70	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	621FC0	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	66E1C4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	66E908	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\trixysEwF_O0f6T2F\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	675C36	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\tC131VXqxqwXyoqOe7muh9i.zip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6529AF	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\D87fZN3R3jFeplaces.sqlite	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\02zdBXl47cvzcookies.sqlite	success or wait	1	65B9DE	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\h7vTUP6ilQXbLogin Data	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\cCZagzzOxnzSLogin Data For Account	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\V9veGYQ701aZWeb Data	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\ELASOvMcSsNrHistory	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\42h4yDt09kAFWeb Data	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\kGWzVJBhnyHSCookies	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\OAwfuvRJ7Zo3History	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\pTWMc6sLNinTWeb Data	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\pSuV50rXNRR3Login Data	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\OrF8rFJrkbX9Web Data	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\UaBkH_1UtTljHistory	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\ne2K7r4K6MmbWeb Data	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\l9WMfadWVY3RHistory	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\spansEwF_O0f6T2F\HQFayTHWA4ClWeb Data	success or wait	1	65B9DE	DeleteFileW
C:\Users\user\AppData\Local\Temp\tC131VXqxqwXyoqOe7muh9i.zip	success or wait	1	6D7071	DeleteFileA

Analysis Process: RageMP131.exe PID: **7784**, Parent PID: **2580**

General

Target ID:	8
Start time:	20:08:08
Start date:	06/05/2024
Path:	C:\Users\user\AppData\Local\RageMP131\RageMP131.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\RageMP131\RageMP131.exe"
Imagebase:	0x610000
File size:	3'188'736 bytes
MD5 hash:	51014F1C86736D8F91D432548062EBBF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.2015798047.00000000019D2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000008.00000002.2015798047.0000000001A18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000008.00000002.2015798047.0000000001938000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

Analysis Process: WerFault.exe PID: **8136**, Parent PID: **7672**

General

Target ID:	12
Start time:	20:08:16
Start date:	06/05/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7672 -s 1944
Imagebase:	0x530000
File size:	483'680 bytes
MD5 hash:	C31336C1EFC2CCB44B4326EA793040F2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: WerFault.exe PID: **6536**, Parent PID: **7784**

General	
Target ID:	16
Start time:	20:08:19
Start date:	06/05/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7784 -s 1908
Imagebase:	0x530000
File size:	483'680 bytes
MD5 hash:	C31336C1EFC2CCB44B4326EA793040F2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: WerFault.exe PID: **7324**, Parent PID: **7428**

General	
Target ID:	18
Start time:	20:08:20
Start date:	06/05/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7428 -s 1980
Imagebase:	0x530000
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: **2816**, Parent PID: **7584**

General	
Target ID:	20
Start time:	20:08:43
Start date:	06/05/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7584 -s 1960
Imagebase:	0x530000
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

Disassembly

No disassembly