ID: 1443933
Sample Name: 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
Cookbook: default.jbs
Time: 06:00:08
Date: 19/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

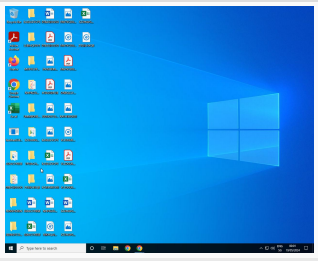
Windows Analysis Report

4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe

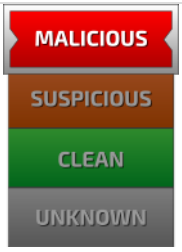
Overview

General Information

Sample name:	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
Analysis ID:	1443933
MD5:	a2c08a55b2b2…
SHA1:	1a12cd9455c3…
SHA256:	f7b1909a121a8..
Tags:	exe
Infos:	



Detection



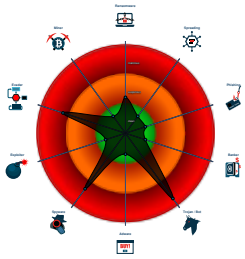
RedLine

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Yara detected RedLine Stealer
- C2 URLs / IPs found in malware con…
- Connects to many ports of the same…
- Found many strings related to Crypt…
- Machine Learning detection for sam…
- Queries sensitive disk information (v…
- Queries sensitive video device infor…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe (PID: 4564 cmdline: "C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe" MD5: A2C08A55B2B269965A786A352398596D)
  - conhost.exe (PID: 5084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
RedLine Stealer	RedLine Stealer is a malware available on underground forums for sale apparently as standalone ($100/$150 depending on the version) or also on a subscription basis ($100/month). This malware harvests information from browsers such as saved credentials, autocomplete data, and credit card information. A system inventory is also taken when running on a target machine, to include details such as the username, location data, hardware configuration, and information regarding installed security software. More recent versions of RedLine added the ability to steal cryptocurrency. FTP and IM clients are also apparently targeted by this family, and this malware has the ability to upload and download files, execute commands, and periodically send back information about the infected computer.	No Attribution	http://https://any.run/cybersecurity-blog/crackedcantil-breakdown/https://apophis133.medium.com/redline-technical-analysis-report-5034e16ad152https://asec.ahnlab.com/en/30445/https://asec.ahnlab.com/en/35981/https://asec.ahnlab.com/ko/25837/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "94.156.8.28:65012"
  ],
  "Bot Id": "3"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x135ca:$a4: get_ScannedWallets • 0x12428:$a5: get_ScanTelegram • 0x1324e:$a6: get_ScanGeckoBrowsersPaths • 0x1106a:$a7: <Processes>k__BackingField • 0xef7c:$a8: <GetWindowsVersion>g__HKLM_GetString\|11_0 • 0x1099e:$a9: <ScanFTP>k__BackingField
4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1048a:$u7: RunPE • 0x13b41:$u8: DownloadAndEx • 0x9130:$pat14: , CommandLine: • 0x13079:$v2_1: ListOfProcesses • 0x1068b:$v2_2: get_ScanVPN • 0x1072e:$v2_2: get_ScanFTP • 0x1141e:$v2_2: get_ScanDiscord • 0x1240c:$v2_2: get_ScanSteam • 0x12428:$v2_2: get_ScanTelegram • 0x124ce:$v2_2: get_ScanScreen • 0x13216:$v2_2: get_ScanChromeBrowsersPaths • 0x1324e:$v2_2: get_ScanGeckoBrowsersPaths • 0x13509:$v2_2: get_ScanBrowsers • 0x135ca:$v2_2: get_ScannedWallets • 0x135f0:$v2_2: get_ScanWallets • 0x13610:$v2_3: GetArguments • 0x11cd9:$v2_4: VerifyUpdate • 0x165de:$v2_4: VerifyUpdate • 0x139ca:$v2_5: VerifyScanRequest • 0x130c6:$v2_6: GetUpdates • 0x165bf:$v2_6: GetUpdates

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.1623079443.0000000000102000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000000.1623079443.0000000000102000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000000.1623079443.0000000000102000.00000002.00000001.01000000.00000003.sdmp	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x133ca:$a4: get_ScannedWallets • 0x12228:$a5: get_ScanTelegram • 0x1304e:$a6: get_ScanGeckoBrowsersPaths • 0x10e6a:$a7: <Processes>k__BackingField • 0xed7c:$a8: <GetWindowsVersion>g__HKLM_GetString\|11_0 • 0x1079e:$a9: <ScanFTP>k__BackingField
Process Memory Space: 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe PID: 4564	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe PID: 4564	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe.100000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.0.4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe.100000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.0.4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe.100000.0.unpack	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x135ca:$a4: get_ScannedWallets • 0x12428:$a5: get_ScanTelegram • 0x1324e:$a6: get_ScanGeckoBrowsersPaths • 0x1106a:$a7: <Processes>k__BackingField • 0xef7c:$a8: <GetWindowsVersion>g__HKLM_GetString\|11_0 • 0x1099e:$a9: <ScanFTP>k__BackingField
0.0.4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe.100000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1048a:$u7: RunPE • 0x13b41:$u8: DownloadAndEx • 0x9130:$pat14: , CommandLine: • 0x13079:$v2_1: ListOfProcesses • 0x1068b:$v2_2: get_ScanVPN • 0x1072e:$v2_2: get_ScanFTP • 0x1141e:$v2_2: get_ScanDiscord • 0x1240c:$v2_2: get_ScanSteam • 0x12428:$v2_2: get_ScanTelegram • 0x124ce:$v2_2: get_ScanScreen • 0x13216:$v2_2: get_ScanChromeBrowsersPaths • 0x1324e:$v2_2: get_ScanGeckoBrowsersPaths • 0x13509:$v2_2: get_ScanBrowsers • 0x135ca:$v2_2: get_ScannedWallets • 0x135f0:$v2_2: get_ScanWallets • 0x13610:$v2_3: GetArguments • 0x11cd9:$v2_4: VerifyUpdate • 0x165de:$v2_4: VerifyUpdate • 0x139ca:$v2_5: VerifyScanRequest • 0x130c6:$v2_6: GetUpdates • 0x165bf:$v2_6: GetUpdates

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

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

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Malware Analysis System Evasion

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

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

Stealing of Sensitive Information

Yara detected RedLine Stealer

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

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

Tries to steal Crypto Currency Wallets

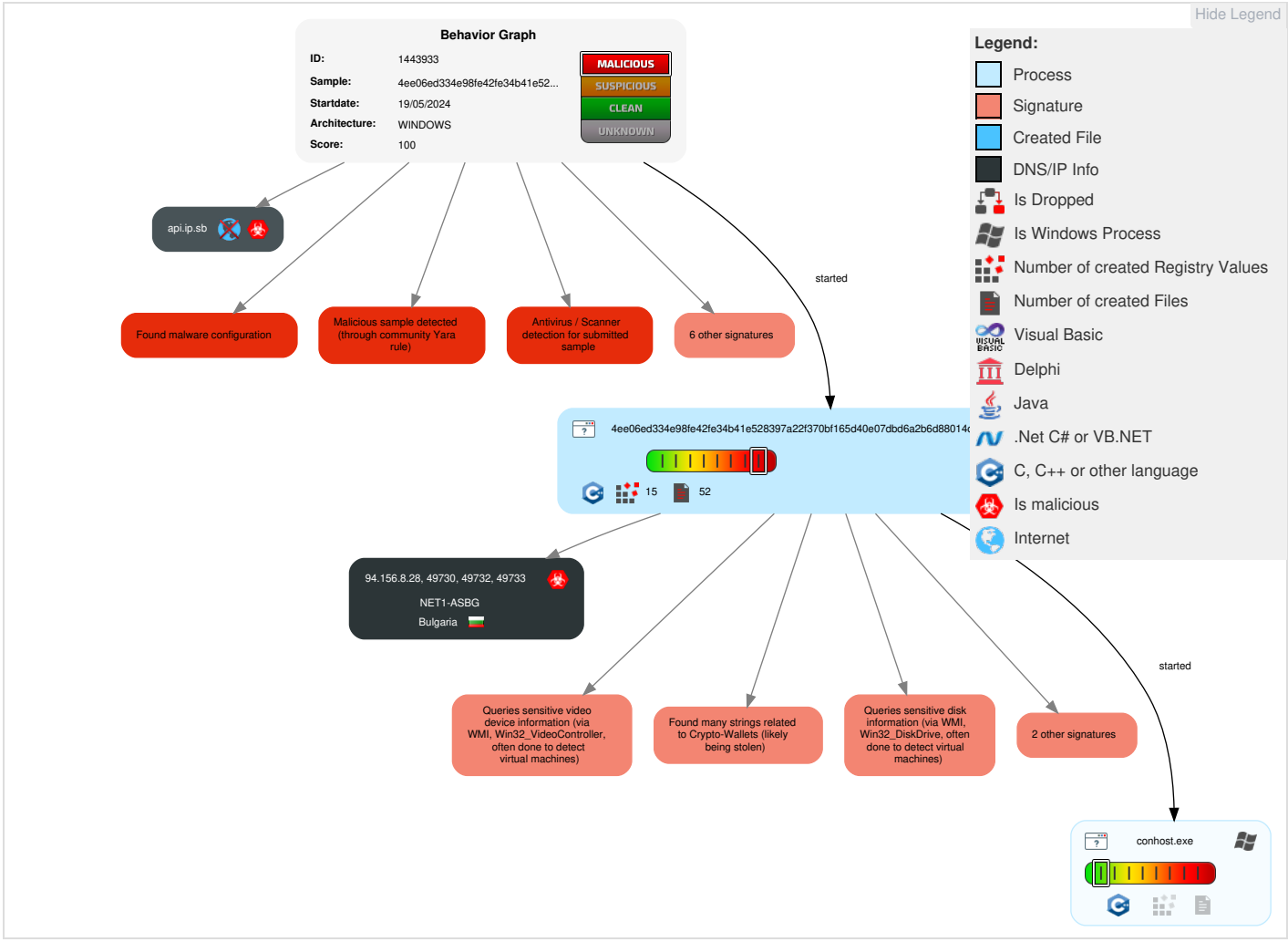
Remote Access Functionality

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	2 2 1 Windows Management Instrumentation	1 DLL Side-Loading	1 Process Injection	1 Masquerading	1 OS Credential Dumping	2 3 1 Security Software Discovery	Remote Services	1 Archive Collected Data	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	3 Data from Local System	1 1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	2 4 1 Virtualization/Sandbox Evasion	Security Account Manager	2 4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	2 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	1 2 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	1 1 3 System Information Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 DLL Side-Loading	Cached Domain Credentials	Wi-Fi Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

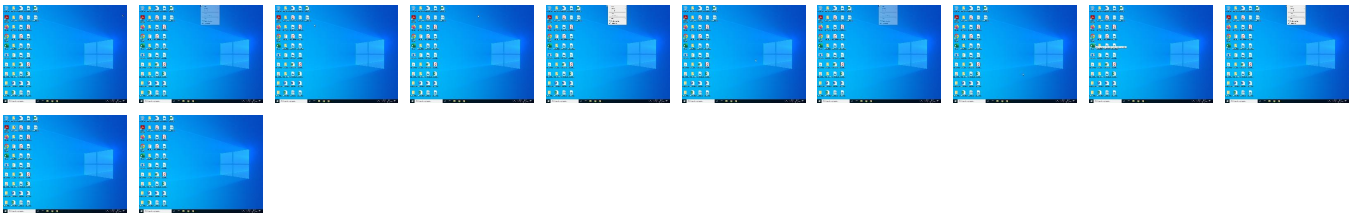
Behavior Graph



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
4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	79%	Virustotal		Browse
4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	100%	Avira	HEUR/AGEN.1305500	
4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
api.ip.sb	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ipinfo.io/ip%appdata%	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultX	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://api.ip.sb	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/soap/envelope/	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	URL Reputation	safe	
http://https://www.ecosia.org/newtab/	0%	URL Reputation	safe	
http://https://ac.ecosia.org/autocomplete?q=	0%	URL Reputation	safe	
http://https://api.ipify.orgcookies//settinString.Removeg	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/ws/2004/08/addressing	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0%	URL Reputation	safe	
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/soap/actor/next	0%	URL Reputation	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/CheckConnectResponse	0%	Avira URL Cloud	safe	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
94.156.8.28:65012	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Virustotal		Browse
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Virustotal		Browse
http://tempuri.org/Endpoint/EnvironmentSettings	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/VerifyUpdateResponse	1%	Virustotal		Browse
http://94.156.8.28:65012/	1%	Virustotal		Browse
http://tempuri.org/Endpoint/CheckConnect	2%	Virustotal		Browse
http://tempuri.org/Endpoint/EnvironmentSettings	2%	Virustotal		Browse
http://tempuri.org/Endpoint/CheckConnectResponse	1%	Virustotal		Browse
http://https://duckduckgo.com/ac/?q=	0%	Virustotal		Browse
94.156.8.28:65012	1%	Virustotal		Browse
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Virustotal		Browse
http://tempuri.org/Endpoint/CheckConnect	0%	Avira URL Cloud	safe	
http://94.156.8.28:65012/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnviron	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/VerifyUpdateResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	Avira URL Cloud	safe	
http://94.156.8.28:65012t-	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdates	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdatesResponse	0%	Avira URL Cloud	safe	
http://94.156.8.28:65012	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnviron	1%	Virustotal		Browse
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	1%	Virustotal		Browse
http://tempuri.org/Endpoint/SetEnvironment	1%	Virustotal		Browse
http://tempuri.org/0	0%	Avira URL Cloud	safe	
http://94.156.8.28:65012	1%	Virustotal		Browse
http://94.156.8.28:6	0%	Avira URL Cloud	safe	
http://tempuri.org/0	0%	Virustotal		Browse
http://tempuri.org/Endpoint/GetUpdatesResponse	1%	Virustotal		Browse
http://tempuri.org/Endpoint/GetUpdates	1%	Virustotal		Browse
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	1%	Virustotal		Browse
http://94.156.8.28:6	1%	Virustotal		Browse
http://tempuri.org/Endpoint/VerifyUpdate	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ip.sb	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
94.156.8.28:65012	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://94.156.8.28:65012/	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

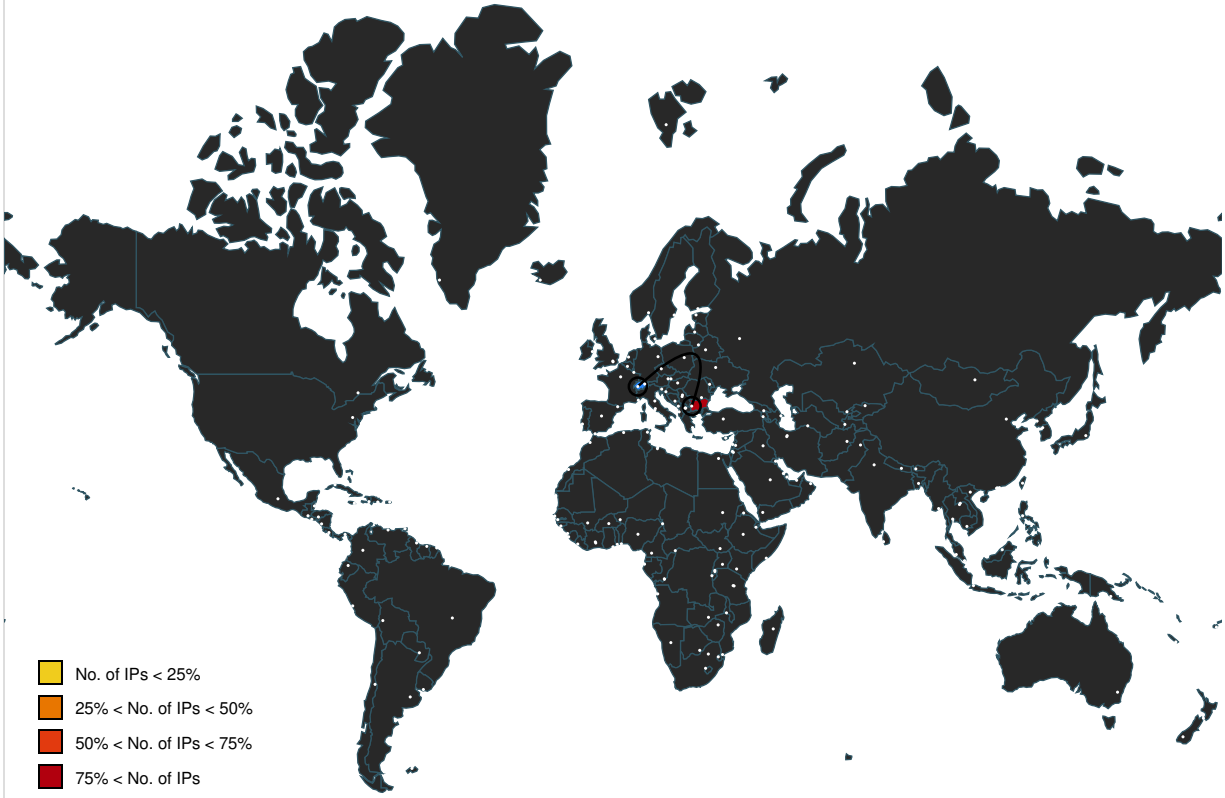
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/ip%appdata%	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/chrome_newtab	tmp771B.tmp.0.dr, tmp773D.tmp.0.dr, tmpAF68.tmp.0.dr, tmpAF58.tmp.0.dr, tmpAF79.tmp.0.dr, tmpE726.tmp.0.dr, tmpAFAA.tmp.0.dr, tmp772D.tmp.0.dr, tmpAF8A.tmp.0.dr, tmpAF47.tmp.0.dr, tmp775E.tmp.0.dr, tmp771C.tmp.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	tmp771B.tmp.0.dr, tmp773D.tmp.0.dr, tmpAF68.tmp.0.dr, tmpAF58.tmp.0.dr, tmpAF79.tmp.0.dr, tmpE726.tmp.0.dr, tmpAFAA.tmp.0.dr, tmp772D.tmp.0.dr, tmpAF8A.tmp.0.dr, tmpAF47.tmp.0.dr, tmp775E.tmp.0.dr, tmp771C.tmp.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	tmp771B.tmp.0.dr, tmp773D.tmp.0.dr, tmpAF68.tmp.0.dr, tmpAF58.tmp.0.dr, tmpAF79.tmp.0.dr, tmpE726.tmp.0.dr, tmpAFAA.tmp.0.dr, tmp772D.tmp.0.dr, tmpAF8A.tmp.0.dr, tmpAF47.tmp.0.dr, tmp775E.tmp.0.dr, tmp771C.tmp.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/CheckConnectResponse	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.datacontract.org/2004/07/	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000024EF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultX	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/EnvironmentSettings	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023F0000.00000004.00000800.00020000.00000000.sdmp, 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	false	• URL Reputation: safe	unknown
http://https://api.ip.sb	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023F0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ip.sb/geoip	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023F0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.0000000002412000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	tmp771B.tmp.0.dr, tmp773D.tmp.0.dr, tmpAF68.tmp.0.dr, tmpAF58.tmp.0.dr, tmpAF79.tmp.0.dr, tmpE726.tmp.0.dr, tmpAFAA.tmp.0.dr, tmp772D.tmp.0.dr, tmpAF8A.tmp.0.dr, tmpAF47.tmp.0.dr, tmp775E.tmp.0.dr, tmp771C.tmp.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.0000000002412000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/CheckConnect	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	tmp771B.tmp.0.dr, tmp773D.tmp.0.dr, tmpAF68.tmp.0.dr, tmpAF58.tmp.0.dr, tmpAF79.tmp.0.dr, tmpE726.tmp.0.dr, tmpAFAA.tmp.0.dr, tmp772D.tmp.0.dr, tmpAF8A.tmp.0.dr, tmpAF47.tmp.0.dr, tmp775E.tmp.0.dr, tmp771C.tmp.0.dr	false	• URL Reputation: safe	unknown
http://https://www.ecosia.org/newtab/	tmp771B.tmp.0.dr, tmp773D.tmp.0.dr, tmpAF68.tmp.0.dr, tmpAF58.tmp.0.dr, tmpAF79.tmp.0.dr, tmpE726.tmp.0.dr, tmpAFAA.tmp.0.dr, tmp772D.tmp.0.dr, tmpAF8A.tmp.0.dr, tmpAF47.tmp.0.dr, tmp775E.tmp.0.dr, tmp771C.tmp.0.dr	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdateResponse	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/SetEnviron	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.000000000254D000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/SetEnvironment	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.000000000254D000.00000004.00000800.00020000.00000000.sdmp, 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp, 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.0000000002431000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/SetEnvironmentResponse	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://94.156.8.28:65012t-	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000024EF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/GetUpdates	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.0000000002545000.00000004.00000800.00020000.00000000.sdmp, 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	tmp771B.tmp.0.dr, tmp773D.tmp.0.dr, tmpAF68.tmp.0.dr, tmpAF58.tmp.0.dr, tmpAF79.tmp.0.dr, tmpE726.tmp.0.dr, tmpAFAA.tmp.0.dr, tmp772D.tmp.0.dr, tmpAF8A.tmp.0.dr, tmpAF47.tmp.0.dr, tmp775E.tmp.0.dr, tmp771C.tmp.0.dr	false	• URL Reputation: safe	unknown
http://https://api.ipify.orgcookies//settinString.Removeg	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/GetUpdatesResponse	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	tmp771B.tmp.0.dr, tmp773D.tmp.0.dr, tmpAF68.tmp.0.dr, tmpAF58.tmp.0.dr, tmpAF79.tmp.0.dr, tmpE726.tmp.0.dr, tmpAFAA.tmp.0.dr, tmp772D.tmp.0.dr, tmpAF8A.tmp.0.dr, tmpAF47.tmp.0.dr, tmp775E.tmp.0.dr, tmp771C.tmp.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://94.156.8.28:65012	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000024EF000.00000004.00000800.00020000.00000000.sdmp, 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdate	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/0	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://94.156.8.28:6	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.000000000254D000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	tmp771B.tmp.0.dr, tmp773D.tmp.0.dr, tmpAF68.tmp.0.dr, tmpAF58.tmp.0.dr, tmpAF79.tmp.0.dr, tmpE726.tmp.0.dr, tmpAFAA.tmp.0.dr, tmp772D.tmp.0.dr, tmpAF8A.tmp.0.dr, tmpAF47.tmp.0.dr, tmp775E.tmp.0.dr, tmp771C.tmp.0.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/actor/next	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe, 00000000.00000002.1769960998.00000000023A1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.156.8.28	unknown	Bulgaria		43561	NET1-ASBG	true

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1443933
Start date and time:	2024-05-19 06:00:08 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 4m 11s
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:	5
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:	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@2/47@1/1
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SIHClient.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.67.75.172, 104.26.12.31, 104.26.13.31
- Excluded domains from analysis (whitelisted): api.ip.sb.cdn.cloudflare.net, ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:01:03	API Interceptor	49x Sleep call for process: 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe.log

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2666
Entropy (8bit):	5.345804351520589
Encrypted:	false
SSDEEP:	48:MOfHK5HKxHKdHK8THaAHKzecYHKh3oPtHo6nmHKtXooBHKoHzHZHxLHG1qHjHKd2:vq5qxqdqolqztYqh3oPtl6mq7qoT5RL9
MD5:	3D3B62B70DF65C6D62C6B068D7256706
SHA1:	03CCEE715BD3299367368426E025742C869155B0
SHA-256:	7373A8D46BC57A95D1C80A2FCD34FF0238B7A0981147FBEA9C28F32F46C653BB
SHA-512:	E259F86B1107BCBFA7F72AB3D199F13AF10644848398DD02D22012B626F353A9EE6865A16E5EA39A7657727D3DA6384F7EA424D8ADEA8F4162C106E90737D559
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\a3127677749631df61e96a8400ddcb87\System.Runtime.Serialization.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral,

C:\Users\user\AppData\Local\Temp\tmp1E9A.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Temp\tmp1EAA.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Temp\tmp1EBB.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Temp\tmp1ECB.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Temp\tmp1EDC.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp1EED.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp1EFD.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp1EFE.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp3E62.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp3E72.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp55A0.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp55B0.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp55C1.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp55D2.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp55E2.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp76E8.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp76E9.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp76FA.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp770B.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp771B.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp771C.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp772D.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp773D.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmp775E.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpAF47.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpAF58.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpAF68.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpAF79.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpAF8A.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpAFAA.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpE726.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpE746.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4454
Malicious:	false
Preview:	SQLite format 3.....@ .....O}.....

C:\Users\user\AppData\Local\Temp\tmpE757.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4454
Malicious:	false
Preview:	SQLite format 3.....@ .....O}.....

C:\Users\user\AppData\Local\Temp\tmpE768.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpE769.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpE779.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpE77A.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpE78B.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.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\tmpF80F.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.690067217069288
Encrypted:	false
SSDEEP:	12:wSQanHEC73FqjThUbJwuUn5qPyd2whRZfZOaH5KrqXzJl/y5bjbVMmRYAPL8fx7T:wHu73FWhUNwzqq2OfX82JdHRNPLcxdl
MD5:	4E32787C3D6F915D3CB360878174E142
SHA1:	57FF84FAEDF66015F2D79E1BE72A29D7B5643F47
SHA-256:	2BCD2A46D2DCED38DE96701E6D3477D8C9F4456FFAE5135C0605C8434BA60269
SHA-512:	CEC75D7CCFA70705732826C202D144A8AC913E7FCFE0D9B54F6A0D1EEC3253B6DEFFB91E551586DA15F56BA4DE8030AC23EE28B16BB80D1C5F1CB6BECF9C21BE
Malicious:	false
Preview:	AIXACVYBSBCZDJMZUDVNECMFSGJSAOAIXCJFDPHQJVUANUFFPQXVYJRUGYPJGKEJNXCBTXARAETAKFTJKVLIZEXLMOAPVEZRZZUIRDUKSPZRBP INNEKLCLXBHFZMBRJTUJZTRCGQGFRQCEVPUBAAPBHBTYYHDJZHHPMFAKXVJPQRQCRUFYPMNUCRRQOYXYEHXQEHWHFLZSBMLRRZFLLYUQLADTKE DXVDLKLPZTTCNAXMXPSTCHQKWMSRPNRZGULFHOTUOYUSIVJEHUYPRYGESSFFMBWDPFRMTVBZEHTJSPRMDJISAZPMEWNGPGIXXTDNHCOBSXAWEF WRZNECKZGORELWMEPSAPLSTZZPUKXURSKTFSUSFEZMXMAIMRJZNGCVKLOHPVMZEIXIISXVMQHQTSADYWZQSWYVJHHONOOSZPQVWIUFMVXBXYCJ OMERCQSVXERFAOOENLKARQGTECAIXOXEZPFDFJHYFCKLADMCWYOMCITRHMECVVVNPNTSRXYGYRKZUTOFNBMHDZWYHPYLTWEIGWOIGBTHWYGIXB CUDYMZMTZNYQMZLMXKPNFZDUEXXQLFJZZZVOPBEZKTKTJCTNUPRCNNGCPTIHKPTGBJLGUENNUGTZVMZJGQGUVBRLOJZECBLINEKGSIRFWZPWMV YJNEPWGYIAHKMJRBZMRVIBPONMHBDQZYFBHDDMYBZZAFEPAQFFUPIGGYNSPVXUWNNCWAUZXAGCATPNHNNYICDCRMTKRODUCDDFZKHLISLVOIFZ PDTOSIEREFHYEWUBJKJRWXMZUGCPUXCPEXUQPWTSKEYSDPEICDQMMKUKJLDNQEHQQCYKRMWOUSJVTVSZJTFZCDVNUMEIZFWDNWCN CSCHBYNKRUSXPVMRIHGXDUPKXMZUIELSRXMZAEUNCCYZTEYLUYYRNSFUTHFESJOLGKJVGGNVJKSFSETAIHYOMLBOPRYAHSCATJUXNTWVZPEMEC BVVHKHDELQRTQBEBXPJJ

C:\Users\user\AppData\Local\Temp\tmpF81F.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.705615236042988
Encrypted:	false
SSDEEP:	24:B65nSK3I37xD9qo21p9G7ILc3pkowOeuiyJRdt7fXzyxu3f7Lj8X2:B65SK3Xx1OXpkowOeMJR/fzeYX8X2
MD5:	159C7BA9D193731A3AAE589183A63B3F
SHA1:	81FDFC9C96C5B4F9C7730127B166B778092F114A
SHA-256:	1FD7067403DCC66C9C013C2F21001B91C2C6456762B05BDC5EDA2C9E7039F41D
SHA-512:	2BC7C0FCEB65E41380FE2E41AE8339D381C226D74C9B510512BD6D2BAFAEB7211FF489C270579804E9C36440F047B65AF1C315D6C20AC10E52147CE388ED858A
Malicious:	false

Preview:	DTBZGIOOSOGIXCBMGZZTWMBQXGHIBDIDBNCACFDFVBOXTDUUJMUMBAKZSHFEIWNQHEECYVTVTSOTORNQIPIDARMCQDPQAFMDPEUWMOYTBCDCAY VFJLXBCNSKBDWMSQYEQYRUTREAZDRNQIZYXPRJXUJXDYZYLJWOVPCEZSCSUSREYDMTRVOKIKSVPBPVQFMFFQNUDCCBDNGIIDGYMQHFPEMCFEOS EKVDEHVQZBXIBJURBZFVTYETURFSVIYLBMHJKBCAPGOAJJFKOTEXRMHREBNTBJGLLRAKZHXKTTSKEXODMEVVGUJOGNLYLFYGHQIBHAFRVYETMD PLEXBQXLVWYLIMFCJAKPFWSQSVSWYINAAOPMCAAVTIWDFRPKUBYLVKYRNUDCLWZJHLKSXWPDEXGEVUQVEJQWTUUYNTOIRLKQTXRWJHCSMGZWWP GPBFZQLOSDMHAPKSMVNNMIVJAORPRFUXPDROELZMLHAIBRVVWUMSDWFAHIBDVMGGFRISFYQZZSESXHMSUQCQPXBCPTAZBJXKKLRBWEZYGWRXBB TYWRRUXCBJIWCOYQKBQCGCZCPFVLGETTTZLEFZDQMQFHJVERUYLQUPVYRNXQJRLPUBWWQHPTYNORTRKKOMLWKAQZNHZQUJGTIYVIKGAWLHSALT ZENHAAJKNKUBSQXDVFQRUFJLDFZAQUPCRNDOOEIALNCMGYLCEZSLPOPYEKIEYDRXSDONBFKQKQMAWBJULDADUHXOQGQLIDEPZRHMCBVTLCJUGO ZRYCGXCXPEOJTGJORAEJKASXKARQEVOHMITSWHQEWOJXNOGSKWUQQTSOSWSCCMOUDMMHPYKEAJECJSGTBNPSFVWSGFBKGSKEHVLW ONOMPOOJEJHDMKGRPCSBYWCZNHTWZCKQNEGEYABJZETYLVHROKZJAIGKJDHLJBRYOVDHNANLCJBHTDDRPXIXDIHNWDDQDHPSAKZRRXOFYYXZWQ WZFESELWVMUIBHMCLVZP

C:\Users\user\AppData\Local\Temp\tmpF820.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.70435191336402
Encrypted:	false
SSDEEP:	24:q83Oua2II99Dm5Xcf7kmp5fFjUTZF/+akoYY9fBpCtJ6Wi5v:7OD2ISi5Xcz9l8RkcFCJ6Wix
MD5:	8C1F71001ABC7FCE68B3F15299553CE7
SHA1:	382285FB69081EB79C936BC4E1BFFC9D4697D881
SHA-256:	DCC1D5A624022EFCE4D4A919041C499622A1213FD62B848C36E6252EE29B5CAE
SHA-512:	8F2124445F7856BFFBB3E7067135CFA70BFB657F8CEAEE89312CF15CFA127CACF28C2F1F9CD1CC64E56A8D8C248E237F2E97F968D244C457AD95D0AD5144E2 A7
Malicious:	false
Preview:	NHPKIZUUSGERQSLBGSEAVXGNDWXNHRIMGKQZIYGMNAKLDSDLMZTSHWNQSMRLTOXKIQVZWPTPMYGCCCTOQMOFGPYVVCCUDORIXMMX DHKCETULBHLJENABEIJPTFOHFPIUUSFPUHSBHENDANFMOYZRZAXYVFEZIKDKUEVZAWEFKRTUJZPFUDMEZZQVBGYMMIHKEBYJMJMTTXSDTDQAUA TXLABLBEJUBBPSXZPXMHVNHOHYPKCYLDVGJSBPEXWGYVPHWPWLYJIOFFNQHAOBSRORLXUKIHEETKPFDPHQAGTKOMEWPBYGMTXHOQFINPIQARIV GCFUFIETTFUMCUDHRHCSTIZWRDJEHWOLAFOSWAVIGSWONBSKFWHCQAGHLWBKAFUQUULJRVZNUGGVOCCVTTWZEZFPJKZDJMHDYXQKDPLRECPAAE ZVBXFDGZJIUGNMOEAISGBSPVTDRADHODLAXUFWZVTJPIGKERLENNAJHHHNNAPBWXCOGJSNVQJJEEPSMESQKGYOHXVMZQNSMSJHQHSGCJZCBZJX MLGNQQKZRIQSQCAWXZFCRMGMMLKHZDWNQTXPTYWGWNQQEQWEZJPQVPOASQIIJYWPUVLHFSLMGHWITYEKRNYGXYTAJZSRGYUWTMRN OICIEPMAYUOIDDOUSYSPAILYQQLYDTBOTEDGSCNXDRRQMOBWCQMDCQXTPEXDKPLVRMFZSKERSAULAYLSOJGDMFTZECKZYYLQVVDOMXISCOBUPP SAYUFOWOCBDJALHRAXDIKEMRYGQMEYTENAHXKWSVJEDEJTIUWZDHLIBKQRVMQLSAYIIOZDWWOLHCJUVJVRYJLTIENWCTYDOSJVSFUHOQPOXCMF GTAWFRCZJNYBCRPUFRUMZIBQDOVOBMFCHMMFHSSJZDCZNMWNCNSQMZWHCOEYNCAFONSABBQCKAPFWJIGKNUCUJZWUKRWIOFVWQWF SYAHDWXEMJKFZYMRVIRAMPVKBXONBJFTXIBDAYIE

C:\Users\user\AppData\Local\Temp\tmpF821.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.69156792375111
Encrypted:	false
SSDEEP:	24:wT4Ye6841ff8PdGjcDOa8AtDLSoarbrGxYsrxpuzu:/Ye68AIGjiOaDDc4uzu
MD5:	A4E170A8033E4DAE501B5FD3D8AC2B74
SHA1:	589F92029C10058A7B281AA9F2BBFA8C822B5767
SHA-256:	E3F62A514D12A3F7D0EB2FF2DA31113A72063AE2E96F816E9AD4185FF8B15C91
SHA-512:	FB96A5E674AE29C3AC9FC495E9C75B103AE4477E2CA370235ED8EA831212AC9CB1543CB3C3F61FD00C8B380836FE1CA679F40739D01C5DDE782C7297C31F4F A
Malicious:	false
Preview:	XZXHAVGRAGWUZPDZUEGAYKLOJAATOVXJVRJCLWZVJFOFPZNHYWDUACWAEZMWROZFSNVNLUZTIGQHRPFNIXZWAQNKEFFVMFVJEYHESHQWKICFNA ONPPGGSABXPCYNBZITQCMUVOCKUUGGEKLAFNXLBOWPVKEOIBLWWAPOYVIECYONJSQKQQDXGYONJXNAQTSMYDMXZYXYEGULUXOLZALCFDXCFNFK PZDKANUFUXWMRLBIQALSWLXEXAFGLOYIFRMFQEZVUTIKXYTPJYCVKCQFZXEECZIXEIHQZQQYTVHKAQLEKMWMZZULQXNCKIJZACKDTKVLWIVBKF QXXOMIGVNYLPAXZFSMAZJTXJUXMZPVKWUQVNXGFUJUQLXWUJWXXGWFDEHIUZKLUQKWAGSXVVNNFXCYWQGRDZCZRLRYXTMLQRGEHR FDGZJOZZKKYLKBWQOZXHGQWMYFROUTIBGKPARBJPOEDNOQMKUEALEVNBPCUIKVTPAWCUIHGVFJWDYFDWTASWSIDDELYILSJEFAACQCZMSARBUA QIRFFLJJMHBVZYFUUTOLDYGUUVIYGJYNXGWJCYUYVJKCVNACSGWHTSOCDOFFPNNHQEMEAXXRINULLPFMNSQUWWIGEJQABGOQLKIXTZYHHQQTOZ YLTNJMMWELZZPDIDHXRBCJGZUDMDGVMAEUIWFYWGIHBTOBLWXIEGHJRIDDBTOXKXOOIAAJUPCJRNMROGCUNSCGQYEEZLWOYIYMJPGKLDXEOGUA UHNUJCEFMGEKRBWDAHWRXWVSFQCURHTSGJQWPJHWEAHXCEQVKJRECGPJBGCDBEGBIRMVXHGYHMWJXIXMQHTKSZFVSATJKNAJOYAJ NKDTKZMBHRENBCAYUBASQOTKKVNCTZIOGOUVVDNXYVJFHXTPSZMOWWCPPMBMLCTTPGONDVJOVLCMTWRESLSDGLNGAGTIXVYAJZVB YYHWAMERRRQXMWVCYELNGPYXOGOPHWVXCTQIKXSK

C:\Users\user\AppData\Local\Temp\tmpF832.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.690067217069288
Encrypted:	false

SSDEEP:	12:wSQanHEC73FqjThUbJwuUn5qPyd2whRZfZOaH5KrqXzJl/y5bjbVMmRYAPL8fx7T:wHu73FWhUNwzqq2OfX82JdHRNPLcxdl
MD5:	4E32787C3D6F915D3CB360878174E142
SHA1:	57FF84FAEDF66015F2D79E1BE72A29D7B5643F47
SHA-256:	2BCD2A46D2DCED38DE96701E6D3477D8C9F4456FFAE5135C0605C8434BA60269
SHA-512:	CEC75D7CCFA70705732826C202D144A8AC913E7FCFE0D9B54F6A0D1EEC3253B6DEFFB91E551586DA15F56BA4DE8030AC23EE28B16BB80D1C5F1CB6BECF9C21BE
Malicious:	false
Preview:	AIXACVYBSBCZDJMZUDVNECMFSGJSAOAIXCJFDPHQJVUANUFFPQXVYJRUGYPJGKEJNXCBTXARAETAKFTJKVLIZEXLMOAPVEZRZZUIRDUKSPZRBP INNEKLCLXBHFZMBRJTUJZTRCGQGFRQCEVPUBAAPBHBTYYHDJZHHPMFAKXVJPQRQCRUFYPMNUCRRQOYXYEHXQEHWHFLZSBMLRRZFLLYUQLADTKE DXVDLKLPZTTCNAXMXPSTCHQKWMSRPNRZGULFHOTUOYUSIVJEHUYPRYGESSFFMBWDPFRMTVBZEHTJSPRMDJISAZPMEWNGPGIXXTDNHCOBSXAWEF WRZNECKZGORELWMEPSAPLSTZZPUKXURSKTFSUSFEZMXMAIMRJZNGCVKLOHPVMZEIXIISXVMQHQTSADYWZQSWYVJHHONOOSZPQVWIUFMVXBXYCJ OMERCQSVXERFAOOENLKARQGTECAIXOXEZPFDFJHYFCKLADMCWYOMCITRHMECVVVNPNTSRXYGYRKZUTOFNBMHDZWYHPYLTWEIGWOIGBTHWYGIXB CUDYMZMTZNYQMZLMXKPNFZDUEXXQLFJZZZVOPBEZKTKTJCTNUPRCNNGCPTIHKPTGBJLGUENNUGTZVMZJGQGUVBRLOJZECBLINEKGSIRFWZPWMV YJNEPWGYIAHKMJRBZMRVIBPONMHBDQZYFBHDDMYBZZAFEPAQFFUPIGGYNSPVXUWNNCWAUZXAGCATPNHNNYICDCRMTKRODUCDDFZKHLISLVOIFZ PDTOSIEREFHYEWUBJKJRWXMZUGCPUXCPEXUQPWTSKEYSDPEICDQMMKUKJLDNQEHQQCYKRMWOUSJVTVSZJTFZCDVNUMEIZFWDNWCN CSCHBYNKRUSXPVMRIHGXDUPKXMZUIELSRXMZAEUNCCYZTEYLUYYRNSFUTHFESJOLGKJVGGNVJKSFSETAIHYOMLBOPRYAHSCATJUXNTWVZPEMEC BVVHKHDELQRTQBEBXPJJ

C:\Users\user\AppData\Local\Temp\tmpF833.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.705615236042988
Encrypted:	false
SSDEEP:	24:B65nSK3I37xD9qo21p9G7ILc3pkowOeuiyJRdt7fXzyxu3f7Lj8X2:B65SK3Xx1OXpkowOeMJR/fzeYX8X2
MD5:	159C7BA9D193731A3AAE589183A63B3F
SHA1:	81FDFC9C96C5B4F9C7730127B166B778092F114A
SHA-256:	1FD7067403DCC66C9C013C2F21001B91C2C6456762B05BDC5EDA2C9E7039F41D
SHA-512:	2BC7C0FCEB65E41380FE2E41AE8339D381C226D74C9B510512BD6D2BAFAEB7211FF489C270579804E9C36440F047B65AF1C315D6C20AC10E52147CE388ED858A
Malicious:	false
Preview:	DTBZGIOOSOGIXCBMGZZTWMBQXGHIBDIDBNCACFDFVBOXTDUUJMUMBAKZSHFEIWNQHEECYVTVTSOTORNQIPIDARMCQDPQAFMDPEUWMOYTBCDCAY VFJLXBCNSKBDWMSQYEQYRUTREAZDRNQIZYXPRJXUJXDYZYLJWOVPCEZSCSUSREYDMTRVOKIKSVPBPVQFMFFQNUDCCBDNGIIDGYMQHFPEMCFEOS EKVDEHVQZBXIBJURBZFVTYETURFSVIYLBMHJKBCAPGOAJJFKOTEXRMHREBNTBJGLLRAKZHXKTTSKEXODMEVVGUJOGNLYLFYGHQIBHAFRVYETMD PLEXBQXLVWYLIMFCJAKPFWSQSVSWYINAAOPMCAAVTIWDFRPKUBYLVKYRNUDCLWZJHLKSXWPDEXGEVUQVEJQWTUUYNTOIRLKQTXRWJHCSMGZWWP GPBFZQLOSDMHAPKSMVNNMIVJAORPRFUXPDROELZMLHAIBRVVWUMSDWFAHIBDVMGGFRISFYQZZSESXHMSUQCQPXBCPTAZBJXKKLRBWEZYGWRXBB TYWRRUXCBJIWCOYQKBQCGCZCPFVLGETTTZLEFZDQMQFHJVERUYLQUPVYRNXQJRLPUBWWQHPTYNORTRKKOMLWKAQZNHZQUJGTIYVIKGAWLHSALT ZENHAAJKNKUBSQXDVFQRUFJLDFZAQUPCRNDOOEIALNCMGYLCEZSLPOPYEKIEYDRXSDONBFKQKQMAWBJULDADUHXOQGQLIDEPZRHMCBVTLCJUGO ZRYCGXCXPEOJTGJORAEJKASXKARQEVOHMITSWHQEWOJXNOGSKWUQQTSOSWSCCMOUDMMHPYKEAJECJSGTBNPSFVWSGFBKGSKEHVLW ONOMPOOJEJHDMKGRPCSBYWCZNHTWZCKQNEGEYABJZETYLVHROKZJAIGKJDHLJBRYOVDHNANLCJBHTDDRPXIXDIHNWDDQDHPSAKZRRXOFYYXZWQ WZFESELWVMUIBHMCLVZP

C:\Users\user\AppData\Local\Temp\tmpF844.tmp

Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.70435191336402
Encrypted:	false
SSDEEP:	24:q83Oua2II99Dm5Xcf7kmp5fFjUTZF/+akoYY9fBpCtJ6Wi5v:7OD2ISi5Xcz9l8RkcFCJ6Wix
MD5:	8C1F71001ABC7FCE68B3F15299553CE7
SHA1:	382285FB69081EB79C936BC4E1BFFC9D4697D881
SHA-256:	DCC1D5A624022EFCE4D4A919041C499622A1213FD62B848C36E6252EE29B5CAE
SHA-512:	8F2124445F7856BFFBB3E7067135CFA70BFB657F8CEAEE89312CF15CFA127CACF28C2F1F9CD1CC64E56A8D8C248E237F2E97F968D244C457AD95D0AD5144E2A7
Malicious:	false
Preview:	NHPKIZUUSGERQSLBGSEAVXGNDWXNHRIMGKQZIYGMNAKLDSDLMZTSHWNQSMRLTOXKIQVZWPTPMYGCCCTOQMOFGPYVVCCUDORIXMMX DHKCETULBHLJENABEIJPTFOHFPIUUSFPUHSBHENDANFMOYZRZAXYVFEZIKDKUEVZAWEFKRTUJZPFUDMEZZQVBGYMMIHKEBYJMJMTTXSDTDQAUA TXLABLBEJUBBPSXZPXMHVNHOHYPKCYLDVGJSBPEXWGYVPHWPWLYJIOFFNQHAOBSRORLXUKIHEETKPFDPHQAGTKOMEWPBYGMTXHOQFINPIQARIV GCFUFIETTFUMCUDHRHCSTIZWRDJEHWOLAFOSWAVIGSWONBSKFWHCQAGHLWBKAFUQUULJRVZNUGGVOCCVTTWZEZFPJKZDJMHDYXQKDPLRECPAAE ZVBXFDGZJIUGNMOEAISGBSPVTDRADHODLAXUFWZVTJPIGKERLENNAJHHHNNAPBWXCOGJSNVQJJEEPSMESQKGYOHXVMZQNSMSJHQHSGCJZCBZJX MLGNQQKZRIQSQCAWXZFCRMGMMLKHZDWNQTXPTYWGWNQQEQWEZJPQVPOASQIIJYWPUVLHFSLMGHWITYEKRNYGXYTAJZSRGYUWTMRN OICIEPMAYUOIDDOUSYSPAILYQQLYDTBOTEDGSCNXDRRQMOBWCQMDCQXTPEXDKPLVRMFZSKERSAULAYLSOJGDMFTZECKZYYLQVVDOMXISCOBUPP SAYUFOWOCBDJALHRAXDIKEMRYGQMEYTENAHXKWSVJEDEJTIUWZDHLIBKQRVMQLSAYIIOZDWWOLHCJUVJVRYJLTIENWCTYDOSJVSFUHOQPOXCMF GTAWFRCZJNYBCRPUFRUMZIBQDOVOBMFCHMMFHSSJZDCZNMWNCNSQMZWHCOEYNCAFONSABBQCKAPFWJIGKNUCUJZWUKRWIOFVWQWF SYAHDWXEMJKFZYMRVIRAMPVKBXONBJFTXIBDAYIE

C:\Users\user\AppData\Local\Temp\tmpF845.tmp	
Process:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.69156792375111
Encrypted:	false
SSDEEP:	24:wT4Ye6841ff8PdGjcDOa8AtDLSoarbrGxYsrxpuzu:/Ye68AIGjiOaDDc4uzu
MD5:	A4E170A8033E4DAE501B5FD3D8AC2B74
SHA1:	589F92029C10058A7B281AA9F2BBFA8C822B5767
SHA-256:	E3F62A514D12A3F7D0EB2FF2DA31113A72063AE2E96F816E9AD4185FF8B15C91
SHA-512:	FB96A5E674AE29C3AC9FC495E9C75B103AE4477E2CA370235ED8EA831212AC9CB1543CB3C3F61FD00C8B380836FE1CA679F40739D01C5DDE782C7297C31F4FA
Malicious:	false
Preview:	XZXHAVGRAGWUZPDZUEGAYKLOJAATOVXJVRJCLWZVJFOFPZNHYWDUACWAEZMWROZFSNVNLUZTIGQHRPFNIXZWAQNKEFFVMFVJEYHESHQWKICFNA ONPPGGSABXPCYNBZITQCMUVOCKUUGGEKLAFNXLBOWPVKEOIBLWWAPOYVIECYONJSQKQQDXGYONJXNAQTSMYDMXZYXYEGULUXOLZALCFDXCFNFK PZDKANUFUXWMRLBIQALSWLXEXAFGLOYIFRMFQEZVUTIKXYTPJYCVKCQFZXEECZIXEIHQZQQYTVHKAQLEKMWMZZULQXNCKIJZACKDTKVLWIVBKF QXXOMIGVNYLPAXZFSMAZJTXJUXMZPVKWUQVNXGFUJUQLXWUJWXXGWFDEHIUZKLUQKWAGSXVVNNFXCYWQGRDZCZRLRYXTMLQRGEHR FDGZJOZZKKYLKBWQOZXHGQWMYFROUTIBGKPARBJPOEDNOQMKUEALEVNBPCUIKVTPAWCUIHGVFJWDYFDWTASWSIDDELYILSJEFAACQCZMSARBUA QIRFFLJJMHBVZYFUUTOLDYGUUVIYGJYNXGWJCYUYVJKCVNACSGWHTSOCDOFFPNNHQEMEAXXRINULLPFMNSQUWWIGEJQABGOQLKIXTZYHHQQTOZ YLTNJMMWELZZPDIDHXRBCJGZUDMDGVMAEUIWFYWGIHBTOBLWXIEGHJRIDDBTOXKXOOIAAJUPCJRNMROGCUNSCGQYEEZLWOYIYMJPGKLDXEOGUA UHNUJCEFMGEKRBWDAHWRXWVSFQCURHTSGJQWPJHWEAHXCEQVKJRECGPJBGCDBEGBIRMVXHGYHMWJXIXMQHTKSZFVSATJKNAJOYAJ NKDTKZMBHRENBCAYUBASQOTKKVNCTZIOGOUVVDNXYVJFHXTPSZMOWWCPPMBMLCTTPGONDVJOVLCMTWRESLSDGLNGAGTIXVYAJZVB YYHWAMERRRQXMWVCYELNGPYXOGOPHWVXCTQIKXSK

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.960015598587119
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
File size:	97'792 bytes
MD5:	a2c08a55b2b269965a786a352398596d
SHA1:	1a12cd9455c3cb7b0b9b49c35f7c2deb1e1c316a
SHA256:	f7b1909a121a8ae8df6f3c54043a14a3726fb0cbdcfdab1f273b26458b318910
SHA512:	704f9d67ea229f4d1dbeff83110c2237f3c847c3dbe3e40caff180a8bccee083eeebecd0b806c65db7a0ad1bd776b080578abc68eda4ae6b94c391eabf7012e1
SSDEEP:	1536:Jqskqq+zlbG6jejoigIT43Ywzi0Zb78ivombfexv0ujXyyed2jteulgS6pt:nPpZYT+zi0ZbYe1g0ujyzdft
TLSH:	82A35D2067AC9F19EAFD1B74B4B2012043F1E08A9091FB4A4DC164E71FA7B865957FF2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..t..... .....@.. .....@.....

File Icon

Icon Hash:	90cececece8e8eb0

Static PE Info

General

Entrypoint:	0x41932e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE

Time Stamp:	0xF00CA9A2 [Wed Aug 14 23:34:58 2097 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x192d4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a000	0x4de	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x17334	0x17400	5c8313ca62b34586154966bf1d23bc54	False	0.4486307123655914	data	6.015064086426226	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x1a000	0x4de	0x600	e3145af1e7dfa1e41fe7799ae002b612	False	0.3756510416666667	data	3.723940100220831	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1c000	0xc	0x200	5d15b3ed438a3ab0253bd60fcc035f5d	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

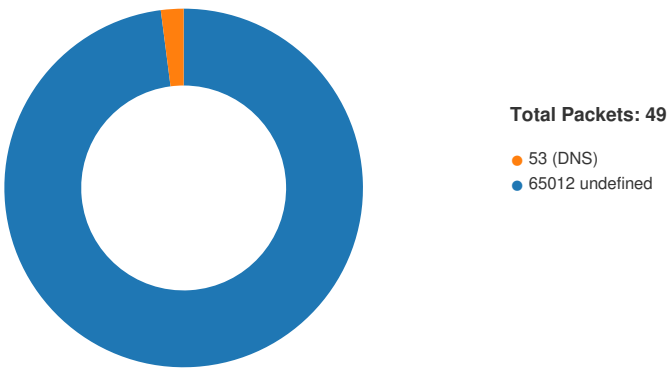
Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_VERSION	0x1a0a0	0x254	data			0.4597315436241611
RT_MANIFEST	0x1a2f4	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.5489795918367347

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2024 06:00:56.425894022 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:00:56.431197882 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:00:56.431329966 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:00:56.449484110 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:00:56.483715057 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:00:56.798177958 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:00:56.803571939 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:00:57.207339048 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:00:57.248821020 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:02.309808969 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:02.309885025 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:02.315361023 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:02.320954084 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:02.550378084 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:02.592565060 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:03.363182068 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:03.364418983 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:03.364629030 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:03.367120028 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:03.367166996 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:03.367312908 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:03.370002031 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:03.370037079 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:03.370181084 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.433940887 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.434721947 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.439693928 CEST	65012	49730	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.439800978 CEST	49730	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.444442034 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.444531918 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.445303917 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.495578051 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.796045065 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.801430941 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.801598072 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.806200981 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.806260109 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.806293011 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.806297064 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.806325912 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.806341887 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.806355000 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.806382895 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.806390047 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.806410074 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.806427002 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.806437969 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.806462049 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.806466103 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.806504965 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.806529999 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.811012030 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.811117887 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.815706968 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.815737963 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.815764904 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.815804958 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.815813065 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.815833092 CEST	65012	49732	94.156.8.28	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2024 06:01:06.815845013 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.815865993 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.815942049 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.854878902 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.855273962 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.902883053 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.903117895 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.951004982 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.951200962 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.987786055 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.988104105 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.993386030 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.993463993 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998147011 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998193026 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998222113 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998246908 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998250961 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998271942 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998281002 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998290062 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998310089 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998317957 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998337984 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998346090 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998366117 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998378992 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998394966 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998409986 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998421907 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998430014 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998450041 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998460054 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998477936 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998485088 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998505116 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998518944 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998533964 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998542070 CEST	49732	65012	192.168.2.4	94.156.8.28
May 19, 2024 06:01:06.998563051 CEST	65012	49732	94.156.8.28	192.168.2.4
May 19, 2024 06:01:06.998588085 CEST	49732	65012	192.168.2.4	94.156.8.28

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2024 06:01:03.412743092 CEST	62993	53	192.168.2.4	1.1.1.1

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 19, 2024 06:01:03.412743092 CEST	192.168.2.4	1.1.1.1	0x16c4	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false

DNS Answers

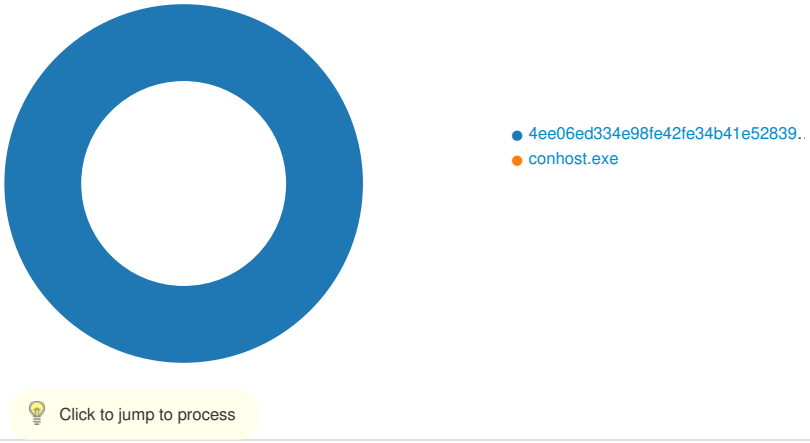
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 19, 2024 06:01:03.420180082 CEST	1.1.1.1	192.168.2.4	0x16c4	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- 94.156.8.28:65012

Statistics

Behavior



System Behavior

Analysis Process: 4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe

PID: **4564**, Parent PID: **2580**

General

Target ID:	0
Start time:	00:00:54
Start date:	19/05/2024
Path:	C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\4ee06ed334e98fe42fe34b41e528397a22f370bf165d40e07dbd6a2b6d88014d_payload.exe"
Imagebase:	0x100000
File size:	97'792 bytes
MD5 hash:	A2C08A55B2B269965A786A352398596D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.1623079443.0000000000102000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000000.1623079443.0000000000102000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000000.00000000.1623079443.0000000000102000.00000002.00000001.01000000.00000003.sdmp, Author: unknown
Reputation:	low
Has exited:	true

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\RASMANCS	success or wait	1	70DAFC58	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\RASMANCS	EnableFileTracing	dword	0	success or wait	1	70DAFC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	70DAFC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	70DAFC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\RASMANCS	FileTracingMask	dword	-65536	success or wait	1	70DAFC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	70DAFC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\RASMANCS	MaxFileSize	dword	1048576	success or wait	1	70DAFC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	70DAFC58	unknown

Analysis Process: conhost.exe PID: **5084**, Parent PID: **4564**

General

Target ID:	1
Start time:	00:00:54
Start date:	19/05/2024
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

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly