ID: 1457840
Sample Name: w4XFffGDz1.exe
Cookbook: default.jbs
Time: 20:21:09
Date: 15/06/2024
Version: 40.0.0 Tourmaline

Table of Contents

C:\Users\user\AppData\Local\Temp\tmp10A5.tmp	22
C:\Users\user\AppData\Local\Temp\tmp10C5.tmp	22
C:\Users\user\AppData\Local\Temp\tmp10D6.tmp	22
C:\Users\user\AppData\Local\Temp\tmp10F6.tmp	23
C:\Users\user\AppData\Local\Temp\tmp1107.tmp	23
C:\Users\user\AppData\Local\Temp\tmp21E5.tmp	23
C:\Users\user\AppData\Local\Temp\tmp2BA8.tmp	24
C:\Users\user\AppData\Local\Temp\tmp2BB9.tmp	24
C:\Users\user\AppData\Local\Temp\tmp2BD9.tmp	24
C:\Users\user\AppData\Local\Temp\tmp2BDA.tmp	24
C:\Users\user\AppData\Local\Temp\tmp2BFA.tmp	25
C:\Users\user\AppData\Local\Temp\tmp2F6.tmp	25
C:\Users\user\AppData\Local\Temp\tmp306.tmp	25
C:\Users\user\AppData\Local\Temp\tmp327.tmp	26
C:\Users\user\AppData\Local\Temp\tmp337.tmp	26
C:\Users\user\AppData\Local\Temp\tmp348.tmp	26
C:\Users\user\AppData\Local\Temp\tmp358.tmp	27
C:\Users\user\AppData\Local\Temp\tmp369.tmp	27
C:\Users\user\AppData\Local\Temp\tmp3799.tmp	27
C:\Users\user\AppData\Local\Temp\tmp37AA.tmp	27
C:\Users\user\AppData\Local\Temp\tmp37BB.tmp	28
C:\Users\user\AppData\Local\Temp\tmp37CB.tmp	28
C:\Users\user\AppData\Local\Temp\tmp37DC.tmp	28
C:\Users\user\AppData\Local\Temp\tmp37FC.tmp	29
C:\Users\user\AppData\Local\Temp\tmp380D.tmp	29
C:\Users\user\AppData\Local\Temp\tmp4825.tmp	29
C:\Users\user\AppData\Local\Temp\tmp4836.tmp	29
C:\Users\user\AppData\Local\Temp\tmp4856.tmp	30
C:\Users\user\AppData\Local\Temp\tmp4876.tmp	30
C:\Users\user\AppData\Local\Temp\tmp4887.tmp	30
C:\Users\user\AppData\Local\Temp\tmp61B0.tmp	31
C:\Users\user\AppData\Local\Temp\tmp621E.tmp	31
C:\Users\user\AppData\Local\Temp\tmp623F.tmp	31
C:\Users\user\AppData\Local\Temp\tmp624F.tmp	32
C:\Users\user\AppData\Local\Temp\tmp6270.tmp	32
C:\Users\user\AppData\Local\Temp\tmp6280.tmp	32
C:\Users\user\AppData\Local\Temp\tmp6291.tmp	32
C:\Users\user\AppData\Local\Temp\tmp7F38.tmp	33
C:\Users\user\AppData\Local\Temp\tmp7F58.tmp	33
C:\Users\user\AppData\Local\Temp\tmp7F78.tmp	33
C:\Users\user\AppData\Local\Temp\tmp7F89.tmp	34
C:\Users\user\AppData\Local\Temp\tmp7F8A.tmp	34
C:\Users\user\AppData\Local\Temp\tmp7F9B.tmp	34
C:\Users\user\AppData\Local\Temp\tmp8574.tmp	35
C:\Users\user\AppData\Local\Temp\tmp9838.tmp	35
C:\Users\user\AppData\Local\Temp\tmp9858.tmp	35
C:\Users\user\AppData\Local\Temp\tmp9869.tmp	35
C:\Users\user\AppData\Local\Temp\tmp9889.tmp	36
C:\Users\user\AppData\Local\Temp\tmp989A.tmp	36
C:\Users\user\AppData\Local\Temp\tmp98BA.tmp	36
C:\Users\user\AppData\Local\Temp\tmp9F36.tmp	37
C:\Users\user\AppData\Local\Temp\tmp9F46.tmp	37
C:\Users\user\AppData\Local\Temp\tmp9F47.tmp	37
C:\Users\user\AppData\Local\Temp\tmp9F58.tmp	38
C:\Users\user\AppData\Local\Temp\tmp9F59.tmp	38
C:\Users\user\AppData\Local\Temp\tmp9F5A.tmp	39
C:\Users\user\AppData\Local\Temp\tmpA0AE.tmp	39
C:\Users\user\AppData\Local\Temp\tmpA0BE.tmp	39
C:\Users\user\AppData\Local\Temp\tmpB5DE.tmp	39
C:\Users\user\AppData\Local\Temp\tmpB5EF.tmp	40
C:\Users\user\AppData\Local\Temp\tmpB600.tmp	40
C:\Users\user\AppData\Local\Temp\tmpB610.tmp	40
C:\Users\user\AppData\Local\Temp\tmpB621.tmp	41
C:\Users\user\AppData\Local\Temp\tmpB631.tmp	41
C:\Users\user\AppData\Local\Temp\tmpB642.tmp	41
C:\Users\user\AppData\Local\Temp\tmpBA4F.tmp	42
C:\Users\user\AppData\Local\Temp\tmpBA60.tmp	42
C:\Users\user\AppData\Local\Temp\tmpBA61.tmp	42
C:\Users\user\AppData\Local\Temp\tmpBA71.tmp	43
C:\Users\user\AppData\Local\Temp\tmpBA72.tmp	43
C:\Users\user\AppData\Local\Temp\tmpBA73.tmp	43
C:\Users\user\AppData\Local\Temp\tmpCDE5.tmp	44
C:\Users\user\AppData\Local\Temp\tmpCDF5.tmp	44
C:\Users\user\AppData\Local\Temp\tmpCE06.tmp	44
C:\Users\user\AppData\Local\Temp\tmpCE16.tmp	45
C:\Users\user\AppData\Local\Temp\tmpCE27.tmp	45
C:\Users\user\AppData\Local\Temp\tmpCE38.tmp	45

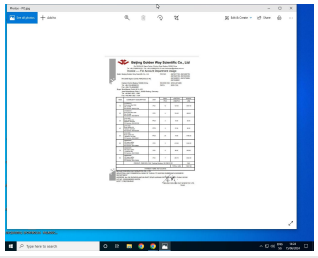
Windows Analysis Report

w4XFffGDz1.exe

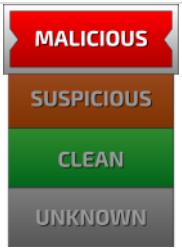
Overview

General Information

Sample name:	w4XFffGDz1.exerenamed because original name is a hash value
Original sample name:	2185ecde5380…
Analysis ID:	1457840
MD5:	2185ecde5380…
SHA1:	caa1b832574fc..
SHA256:	e1a01751d2ea…
Tags:	exe RedLineStealer
Infos:	



Detection



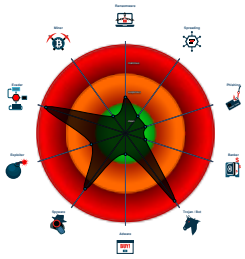
RedLine

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

Signatures

- Found malware configuration
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp fil…
- Yara detected AntiVM3
- Yara detected RedLine Stealer
- .NET source code contains potentia…
- AI detected suspicious sample
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…
- Found many strings related to Crypt…

Classification



Process Tree

- **System is w10x64**
- w4XFffGDz1.exe (PID: 6412 cmdline: "C:\Users\user\Desktop\w4XFffGDz1.exe" MD5: 2185ECDE5380054AD075B7A25AE0EA51)
  - PO.exe (PID: 7532 cmdline: "C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe" MD5: 86F98523CEB67DF5CC3431A839F63134)
    - powershell.exe (PID: 7780 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe" MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
      - conhost.exe (PID: 7788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - powershell.exe (PID: 7812 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\AJzHYZtQlb.exe" MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
      - conhost.exe (PID: 7856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
      - WmiPrvSE.exe (PID: 5020 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: 60FF40CFD7FB8FE41EE4FE9AE5FE1C51)
    - schtasks.exe (PID: 7908 cmdline: "C:\Windows\System32\schtasks.exe" /Create /TN "Updates\AJzHYZtQlb" /XML "C:\Users\user\AppData\Local\Temp\tmp61B0.tmp" MD5: 48C2FE20575769DE916F48EF0676A965)
      - conhost.exe (PID: 7960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - PO.exe (PID: 8068 cmdline: "C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe" MD5: 86F98523CEB67DF5CC3431A839F63134)
      - conhost.exe (PID: 8080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- AJzHYZtQlb.exe (PID: 8164 cmdline: C:\Users\user\AppData\Roaming\AJzHYZtQlb.exe MD5: 86F98523CEB67DF5CC3431A839F63134)
  - schtasks.exe (PID: 8028 cmdline: "C:\Windows\System32\schtasks.exe" /Create /TN "Updates\AJzHYZtQlb" /XML "C:\Users\user\AppData\Local\Temp\tmp8574.tmp" MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 7960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - AJzHYZtQlb.exe (PID: 5404 cmdline: "C:\Users\user\AppData\Roaming\AJzHYZtQlb.exe" MD5: 86F98523CEB67DF5CC3431A839F63134)
    - conhost.exe (PID: 7848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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": [
    "45.137.22.67:55615"
  ],
  "Bot Id": "cheat"
}
```


Yara Signatures

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
0000000E.00000002.2274416687.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000E.00000002.2274416687.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000E.00000002.2274416687.0000000000402000.00000040.00000400.00020000.00000000.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
00000015.00000002.2357626482.0000000002FF0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000010.00000002.2247047739.0000000004AFD000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.PO.exe.3c18d70.3.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
7.2.PO.exe.3c18d70.3.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
7.2.PO.exe.3c00f50.4.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
7.2.PO.exe.3c18d70.3.unpack	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x117ca:$a4: get_ScannedWallets • 0x10628:$a5: get_ScanTelegram • 0x1144e:$a6: get_ScanGeckoBrowsersPaths • 0xf26a:$a7: <Processes>k__BackingField • 0xd17c:$a8: <GetWindowsVersion>g__HKLM_GetString\|11_0 • 0xeb9e:$a9: <ScanFTP>k__BackingField
7.2.PO.exe.3c00f50.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 15 entries				

Sigma Signatures

System Summary

Sigma detected: Powershell Base64 Encoded MpPreference Cmdlet

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: Powershell Defender Exclusion

Sigma detected: Suspicious Add Scheduled Task Parent

Sigma detected: Suspicious Schtasks From Env Var Folder

Sigma detected: Non Interactive PowerShell Process Spawned

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

AI detected suspicious sample

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Loading BitLocker PowerShell Module

Uses known network protocols on non-standard ports

Malware Analysis System Evasion

Yara detected AntiVM3

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)

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

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

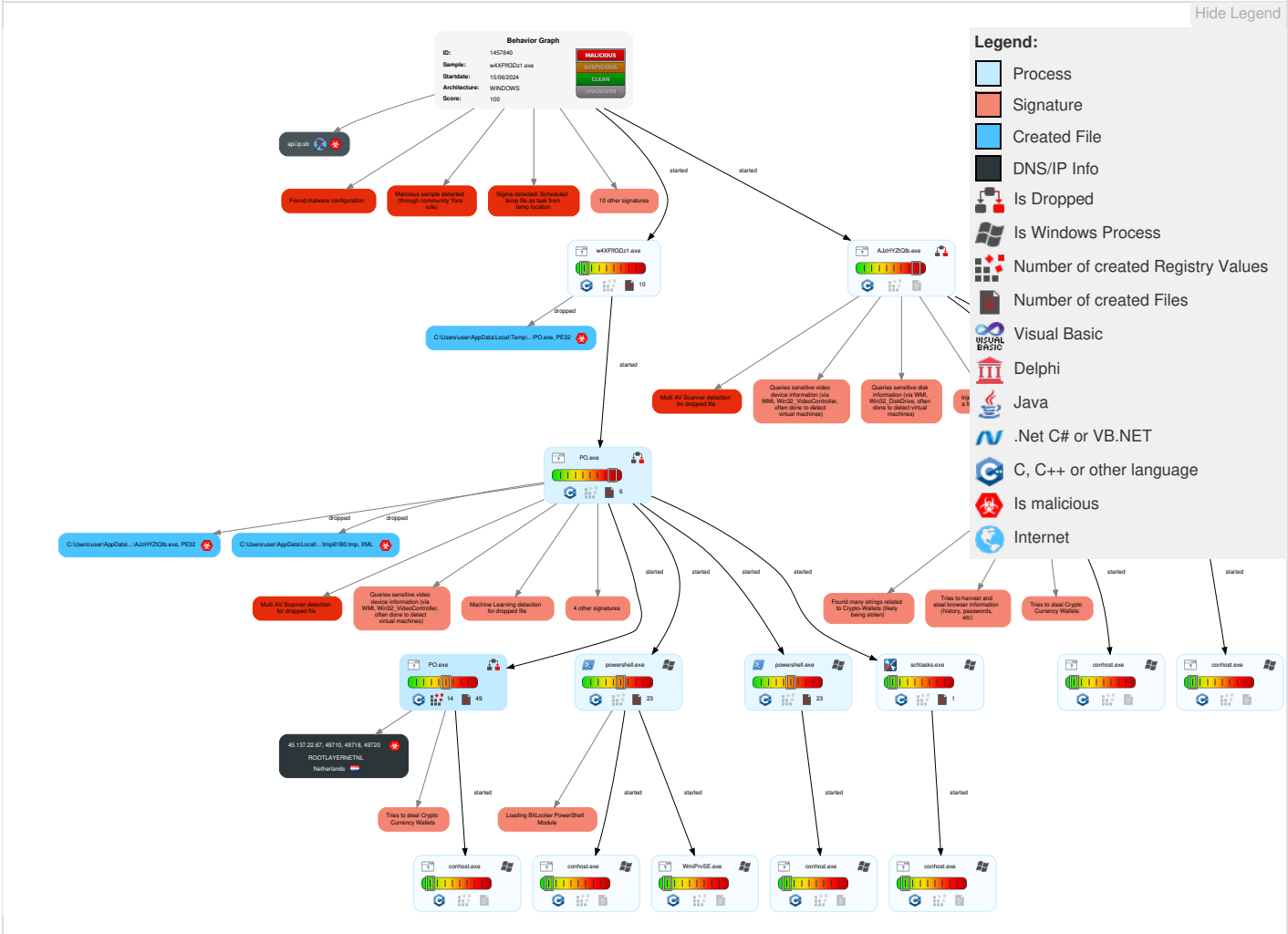
Yara detected RedLine Stealer

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 DLL Side-Loading	1 1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	2 Command and Scripting Interpreter	1 Scheduled Task/Job	1 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	3 File and Directory 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	1 Scheduled Task/Job	Logon Script (Windows)	1 Scheduled Task/Job	4 Obfuscated Files or Information	Security Account Manager	1 3 7 System Information Discovery	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 3 Software Packing	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	1 2 Application Layer Protocol	Traffic Duplication	Data Destruction

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	3 5 1 Security Software 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 Masqueradi ng	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Multiband Communicat ion	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	2 4 1 Virtualizatio n/Sandbox Evasion	DCSync	2 4 1 Virtualizatio n/Sandbox Evasion	Windows Remote Managemen t	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependenci es	Serverless	Drive-by Compromis e	Container Orchestratio n Job	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	1 Application Window Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

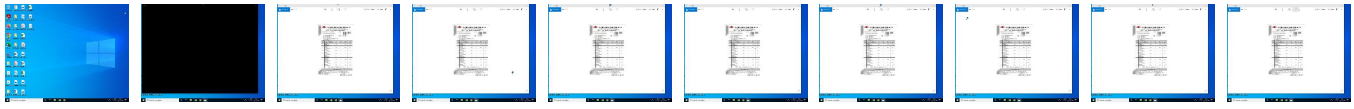
Behavior Graph

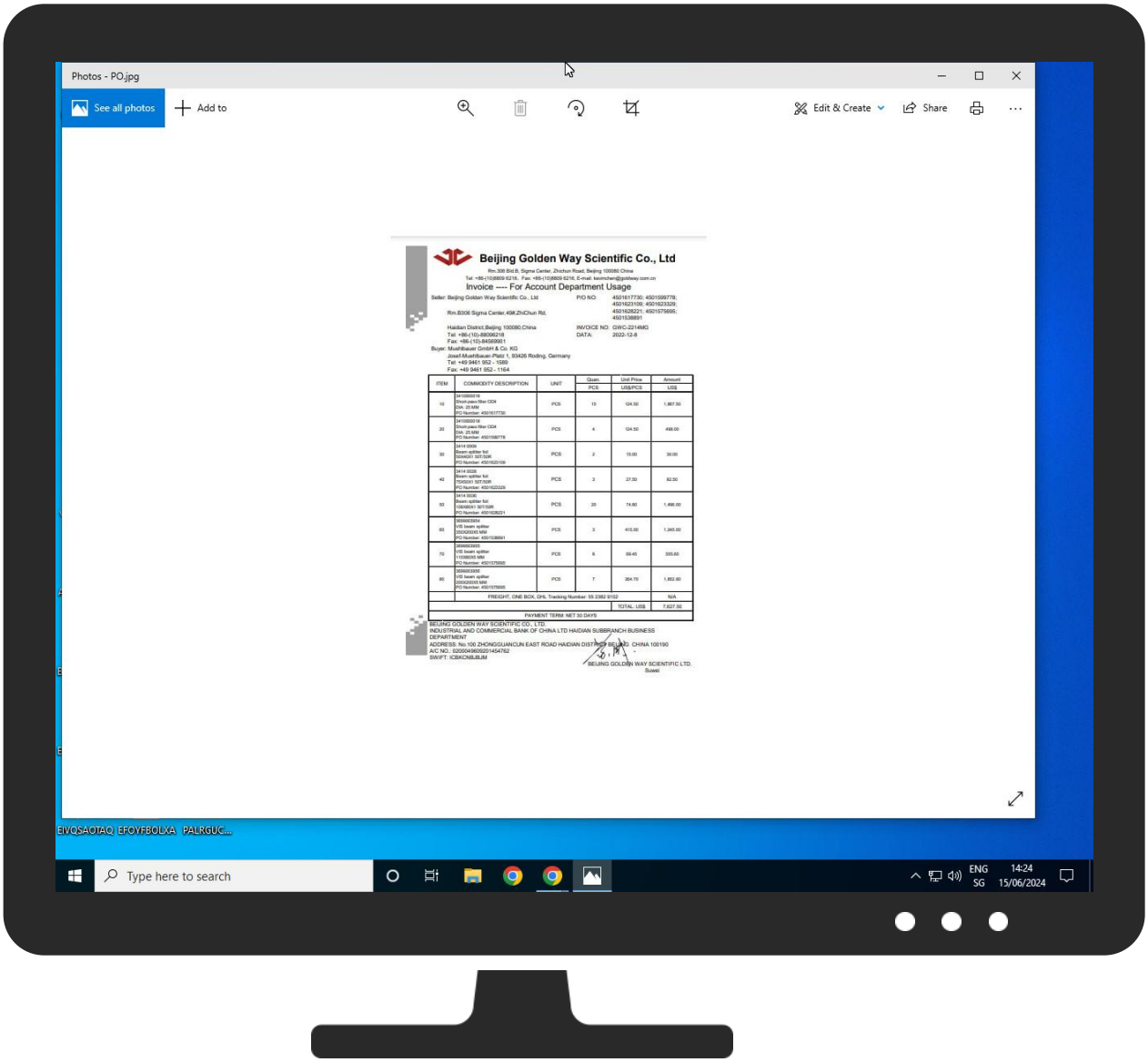


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
w4XFffGDz1.exe	68%	ReversingLabs	ByteCode-MSIL.Trojan.SpyNoon	
w4XFffGDz1.exe	67%	Virustotal		Browse
w4XFffGDz1.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe	88%	ReversingLabs	ByteCode-MSIL.Trojan.SpyNoon	
C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe	58%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe	88%	ReversingLabs	ByteCode-MSIL.Trojan.SpyNoon	
C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe	58%	Virustotal		Browse

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://schemas.xmlsoap.org/soap/envelope/	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://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://45.137.22.67:55615	0%	Avira URL Cloud	safe	
http://https://ipinfo.io/ip%appdata%	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://45.137.22.67:55615/	0%	Avira URL Cloud	safe	
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	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%	Avira URL Cloud	safe	
http://45.137.22.67:55615/	3%	Virustotal		Browse
http://45.137.22.67:55615	3%	Virustotal		Browse
http://schemas.datacontract.org/2004/07/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/CheckConnectResponse	0%	Avira URL Cloud	safe	
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultX	0%	Avira URL Cloud	safe	
http://https://ipinfo.io/ip%appdata%	0%	Virustotal		Browse
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Virustotal		Browse
http://schemas.datacontract.org/2004/07/	0%	Virustotal		Browse
http://tempuri.org/Endpoint/EnvironmentSettings	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Virustotal		Browse
http://https://api.ip.sb/geoip	0%	Virustotal		Browse
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	Virustotal		Browse
http://tempuri.org/Endpoint/EnvironmentSettings	2%	Virustotal		Browse
http://https://api.ip.sb	0%	Virustotal		Browse
http://tempuri.org/Endpoint/CheckConnectResponse	1%	Virustotal		Browse
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	0%	Virustotal		Browse
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultX	0%	Virustotal		Browse
http://https://api.ip.sb/geoip	0%	Avira URL Cloud	safe	
http://https://api.ip.sb	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/CheckConnect	0%	Avira URL Cloud	safe	
http://www.w3.or	0%	Avira URL Cloud	safe	
http://tempuri.org/	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://https://www.chiark.greenend.org.uk/~sgtatham/putty/0	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://tempuri.org/	0%	Virustotal		Browse
http://tempuri.org/Endpoint/VerifyUpdateResponse	1%	Virustotal		Browse
http://tempuri.org/Endpoint/GetUpdates	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/CheckConnect	2%	Virustotal		Browse
http://https://api.ipify.orgcookies//settinString.Removeg	0%	Avira URL Cloud	safe	
http://https://www.chiark.greenend.org.uk/~sgtatham/putty/0	0%	Virustotal		Browse
http://schemas.xmlsoap.org/ws/2004/08/addressing	0%	Avira URL Cloud	safe	
45.137.22.67:55615	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdatesResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	Avira URL Cloud	safe	
45.137.22.67:55615	3%	Virustotal		Browse
http://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdates	1%	Virustotal		Browse
http://tempuri.org/Endpoint/GetUpdatesResponse	1%	Virustotal		Browse
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	1%	Virustotal		Browse
http://schemas.xmlsoap.org/ws/2004/08/addressing	0%	Virustotal		Browse
http://tempuri.org/0	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironment	1%	Virustotal		Browse
http://45.137.22.67:55615t-	0%	Avira URL Cloud	safe	
http://schemas.xmlsoap.org/soap/actor/next	0%	Avira URL Cloud	safe	
http://www.aforgenet.com/framework/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	1%	Virustotal		Browse
http://tempuri.org/0	0%	Virustotal		Browse
http://schemas.xmlsoap.org/soap/actor/next	0%	Virustotal		Browse
http://tempuri.org/Endpoint/VerifyUpdate	1%	Virustotal		Browse
http://www.aforgenet.com/framework/	0%	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
http://45.137.22.67:55615/	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
45.137.22.67:55615	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

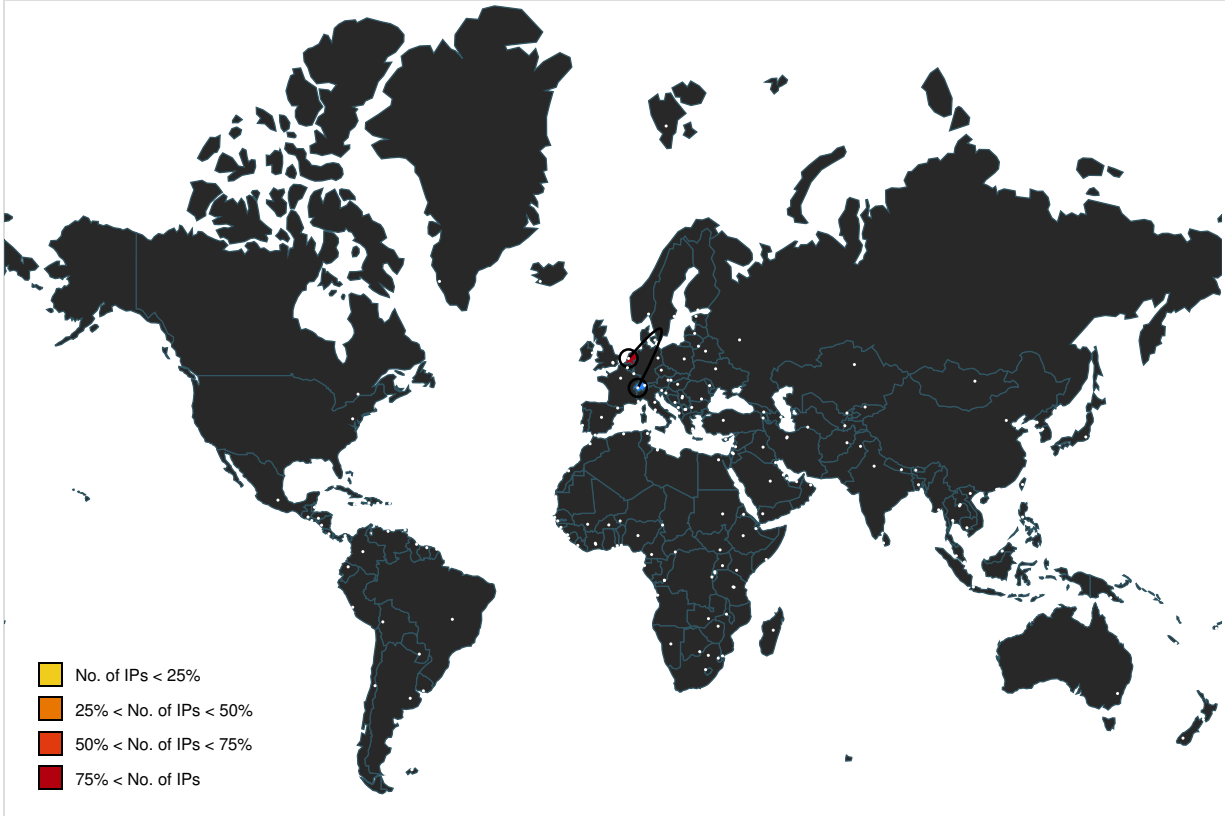
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/ip%appdata%	PO.exe, PO.exe, 0000000E.00000002.2274416687.0000000000402000.00000040.00000400.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000010.00000002.2247047739.0000000004AFD000.00000004.00000800.00020000.00000000.sdmp	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://45.137.22.67:55615	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, PO.exe, 0000000E.00000002.2276292357.000000000347E000.00000004.00000800.00020000.00000000.sdmp, PO.exe, 0000000E.00000002.2276292357.00000000033D8000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000015.00000002.2357626482.00000000030A3000.00000004.00000800.00020000.00000000.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	tmp4887.tmp.21.dr, tmp4825.tmp.21.dr, tmp7F38.tmp.21.dr, tmp10D6.tmp.21.dr, tmp989A.tmp.14.dr, tmp10A5.tmp.21.dr, tmp4836.tmp.21.dr, tmp6270.tmp.14.dr, tmp98BA.tmp.14.dr, tmp4876.tmp.21.dr, tmp6291.tmp.14.dr, tmp4856.tmp.21.dr, tmp6280.tmp.14.dr, tmp9889.tmp.14.dr, tmp624F.tmp.14.dr, tmp1107.tmp.21.dr, tmp10C5.tmp.21.dr, tmp9838.tmp.14.dr, tmp9858.tmp.14.dr, tmp10F6.tmp.21.dr, tmp623F.tmp.14.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	tmp4887.tmp.21.dr, tmp4825.tmp.21.dr, tmp7F38.tmp.21.dr, tmp10D6.tmp.21.dr, tmp989A.tmp.14.dr, tmp10A5.tmp.21.dr, tmp4836.tmp.21.dr, tmp6270.tmp.14.dr, tmp98BA.tmp.14.dr, tmp4876.tmp.21.dr, tmp6291.tmp.14.dr, tmp4856.tmp.21.dr, tmp6280.tmp.14.dr, tmp9889.tmp.14.dr, tmp624F.tmp.14.dr, tmp1107.tmp.21.dr, tmp10C5.tmp.21.dr, tmp9838.tmp.14.dr, tmp9858.tmp.14.dr, tmp10F6.tmp.21.dr, tmp623F.tmp.14.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	tmp4887.tmp.21.dr, tmp4825.tmp.21.dr, tmp7F38.tmp.21.dr, tmp10D6.tmp.21.dr, tmp989A.tmp.14.dr, tmp10A5.tmp.21.dr, tmp4836.tmp.21.dr, tmp6270.tmp.14.dr, tmp98BA.tmp.14.dr, tmp4876.tmp.21.dr, tmp6291.tmp.14.dr, tmp4856.tmp.21.dr, tmp6280.tmp.14.dr, tmp9889.tmp.14.dr, tmp624F.tmp.14.dr, tmp1107.tmp.21.dr, tmp10C5.tmp.21.dr, tmp9838.tmp.14.dr, tmp9858.tmp.14.dr, tmp10F6.tmp.21.dr, tmp623F.tmp.14.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/CheckConnectResponse	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.datacontract.org/2004/07/	PO.exe, 0000000E.00000002.2276292357.00000000033D8000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.00000000030A3000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultX	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/EnvironmentSettings	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, PO.exe, 0000000E.00000002.2276292357.00000000031D0000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FF0000.00000004.00000800.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	PO.exe, PO.exe, 0000000E.00000002.2274416687.0000000000402000.00000040.00000400.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000010.00000002.2247047739.0000000004AFD000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.ip.sb	AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FFA000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.ip.sb/geoip	AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FFA000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/	AJzHYZtQIb.exe, 00000015.00000002.2357626482.000000000300B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.w3.or	AJzHYZtQIb.exe, 00000010.00000002.2245706074.0000000002F69000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	tmp4887.tmp.21.dr, tmp4825.tmp.21.dr, tmp7F38.tmp.21.dr, tmp10D6.tmp.21.dr, tmp989A.tmp.14.dr, tmp10A5.tmp.21.dr, tmp4836.tmp.21.dr, tmp6270.tmp.14.dr, tmp98BA.tmp.14.dr, tmp4876.tmp.21.dr, tmp6291.tmp.14.dr, tmp4856.tmp.21.dr, tmp6280.tmp.14.dr, tmp9889.tmp.14.dr, tmp624F.tmp.14.dr, tmp1107.tmp.21.dr, tmp10C5.tmp.21.dr, tmp9838.tmp.14.dr, tmp9858.tmp.14.dr, tmp10F6.tmp.21.dr, tmp623F.tmp.14.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/	AJzHYZtQlb.exe, 00000015.00000002.2357626482.000000000300B000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/CheckConnect	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	tmp4887.tmp.21.dr, tmp4825.tmp.21.dr, tmp7F38.tmp.21.dr, tmp10D6.tmp.21.dr, tmp989A.tmp.14.dr, tmp10A5.tmp.21.dr, tmp4836.tmp.21.dr, tmp6270.tmp.14.dr, tmp98BA.tmp.14.dr, tmp4876.tmp.21.dr, tmp6291.tmp.14.dr, tmp4856.tmp.21.dr, tmp6280.tmp.14.dr, tmp9889.tmp.14.dr, tmp624F.tmp.14.dr, tmp1107.tmp.21.dr, tmp10C5.tmp.21.dr, tmp9838.tmp.14.dr, tmp9858.tmp.14.dr, tmp10F6.tmp.21.dr, tmp623F.tmp.14.dr	false	• URL Reputation: safe	unknown
http://https://www.ecosia.org/newtab/	tmp4887.tmp.21.dr, tmp4825.tmp.21.dr, tmp7F38.tmp.21.dr, tmp10D6.tmp.21.dr, tmp989A.tmp.14.dr, tmp10A5.tmp.21.dr, tmp4836.tmp.21.dr, tmp6270.tmp.14.dr, tmp98BA.tmp.14.dr, tmp4876.tmp.21.dr, tmp6291.tmp.14.dr, tmp4856.tmp.21.dr, tmp6280.tmp.14.dr, tmp9889.tmp.14.dr, tmp624F.tmp.14.dr, tmp1107.tmp.21.dr, tmp10C5.tmp.21.dr, tmp9838.tmp.14.dr, tmp9858.tmp.14.dr, tmp10F6.tmp.21.dr, tmp623F.tmp.14.dr	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdateResponse	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.chiark.greenend.org.uk/~sgtatham/putty/0	PO.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/SetEnvironment	AJzHYZtQlb.exe, 00000015.00000002.2357626482.00000000030A3000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/SetEnvironmentResponse	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/GetUpdates	AJzHYZtQlb.exe, 00000015.00000002.2357626482.00000000030A3000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000015.00000002.2357626482.0000000002FF0000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000015.00000002.2357626482.0000000003019000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	tmp4887.tmp.21.dr, tmp4825.tmp.21.dr, tmp7F38.tmp.21.dr, tmp10D6.tmp.21.dr, tmp989A.tmp.14.dr, tmp10A5.tmp.21.dr, tmp4836.tmp.21.dr, tmp6270.tmp.14.dr, tmp98BA.tmp.14.dr, tmp4876.tmp.21.dr, tmp6291.tmp.14.dr, tmp4856.tmp.21.dr, tmp6280.tmp.14.dr, tmp9889.tmp.14.dr, tmp624F.tmp.14.dr, tmp1107.tmp.21.dr, tmp10C5.tmp.21.dr, tmp9838.tmp.14.dr, tmp9858.tmp.14.dr, tmp10F6.tmp.21.dr, tmp623F.tmp.14.dr	false	• URL Reputation: safe	unknown
http://https://api.ipify.orgcookies//settinString.Removeg	PO.exe, PO.exe, 0000000E.00000002.2274416687.0000000000402000.00000040.00000400.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000010.00000002.2247047739.0000000004AFD000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000015.00000002.2357626482.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/GetUpdatesResponse	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQlb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	tmp4887.tmp.21.dr, tmp4825.tmp.21.dr, tmp7F38.tmp.21.dr, tmp10D6.tmp.21.dr, tmp989A.tmp.14.dr, tmp10A5.tmp.21.dr, tmp4836.tmp.21.dr, tmp6270.tmp.14.dr, tmp98BA.tmp.14.dr, tmp4876.tmp.21.dr, tmp6291.tmp.14.dr, tmp4856.tmp.21.dr, tmp6280.tmp.14.dr, tmp9889.tmp.14.dr, tmp624F.tmp.14.dr, tmp1107.tmp.21.dr, tmp10C5.tmp.21.dr, tmp9838.tmp.14.dr, tmp9858.tmp.14.dr, tmp10F6.tmp.21.dr, tmp623F.tmp.14.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdate	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://tempuri.org/0	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO.exe, 00000007.00000002.2160002789.0000002A55000.00000004.00000800.00020000.00000000.sdmp, PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000010.00000002.2245706074.0000000003018000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	tmp4887.tmp.21.dr, tmp4825.tmp.21.dr, tmp7F38.tmp.21.dr, tmp10D6.tmp.21.dr, tmp989A.tmp.14.dr, tmp10A5.tmp.21.dr, tmp4836.tmp.21.dr, tmp6270.tmp.14.dr, tmp98BA.tmp.14.dr, tmp4876.tmp.21.dr, tmp6291.tmp.14.dr, tmp4856.tmp.21.dr, tmp6280.tmp.14.dr, tmp9889.tmp.14.dr, tmp624F.tmp.14.dr, tmp1107.tmp.21.dr, tmp10C5.tmp.21.dr, tmp9838.tmp.14.dr, tmp9858.tmp.14.dr, tmp10F6.tmp.21.dr, tmp623F.tmp.14.dr	false	• URL Reputation: safe	unknown
http://45.137.22.67:55615t-	AJzHYZtQIb.exe, 00000015.00000002.2357626482.00000000030A3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/actor/next	PO.exe, 0000000E.00000002.2276292357.0000000003181000.00000004.00000800.00020000.00000000.sdmp, AJzHYZtQIb.exe, 00000015.00000002.2357626482.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.aforgenet.com/framework/	PO.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.137.22.67	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1457840
Start date and time:	2024-06-15 20:21:09 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 8m 46s
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:	24
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:	w4XFffGDz1.exerenamed because original name is a hash value
Original Sample Name:	2185ecde5380054ad075b7a25ae0ea51.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@22/104@2/1
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, WMIADAP.exe, Microsoft.Photos.exe, SIHClient.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 104.26.12.31, 104.26.13.31, 172.67.75.172
- Excluded domains from analysis (whitelisted): api.ip.sb.cdn.cloudflare.net, fs.microsoft.com, 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 exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateKey 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
14:22:03	API Interceptor	34x Sleep call for process: PO.exe modified
14:22:09	API Interceptor	37x Sleep call for process: powershell.exe modified
14:22:13	API Interceptor	45x Sleep call for process: AJzHYZtQIb.exe modified
14:22:13	API Interceptor	1x Sleep call for process: w4XFffGDz1.exe modified
20:22:11	Task Scheduler	Run new task: AJzHYZtQIb path: C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe

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\AJzHYZtQIb.exe.log

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.34331486778365
Encrypted:	false
SSDEEP:	24:MLUE4K5E4KH1qE4qXKDE4KhKiKhPKIE4oKNzKoZAE4Kze0E4x84j:MIHK5HKH1qHiYHKh3oPtHo6hAHKze0HJ
MD5:	1330C80CAAC9A0FB172F202485E9B1E8
SHA1:	86BAFDA4E4AE68C7C3012714A33D85D2B6E1A492
SHA-256:	B6C63ECE799A8F7E497C2A158B1FFC2F5CB4F745A2F8E585F794572B7CF03560
SHA-512:	75A17AB129FE97BBAB36AA2BD66D59F41DB5AFF44A705EF3E4D094EC5FCD056A3ED59992A0AC96C9D0D40E490F8596B07DCA9B60E606B67223867B061D9D0B2
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02

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

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.34331486778365
Encrypted:	false
SSDEEP:	24:MLUE4K5E4KH1qE4qXKDE4KhKiKhPKIE4oKNzKoZAE4Kze0E4x84j:MIHK5HKH1qHiYHKh3oPtHo6hAHKze0HJ
MD5:	1330C80CAAC9A0FB172F202485E9B1E8
SHA1:	86BAFDA4E4AE68C7C3012714A33D85D2B6E1A492

SHA-256:	B6C63ECE799A8F7E497C2A158B1FFC2F5CB4F745A2F8E585F794572B7CF03560
SHA-512:	75A17AB129FE97BBAB36AA2BD66D59F41DB5AFF44A705EF3E4D094EC5FCD056A3ED59992A0AC96C9D0D40E490F8596B07DCA9B60E606B67223867B061D9D0E B2
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df07665 68\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll",0..3 ,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Conf iguration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c56193 4e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	2232
Entropy (8bit):	5.379552885213346
Encrypted:	false
SSDEEP:	48:fWSU4xympjgZ9tz4RIoUl8NPZHUl7u1iMugeC/ZM0Uyus:fLHxvCZfIfSKRHmOugw1s
MD5:	236CE6553B5DB20FA0B07F9FEA88F4A4
SHA1:	AEB5B156162EC5CD4E0BC3A0BA0F0D4739D40DBD
SHA-256:	3849E9437770B9804D942D293FFAB3C6449B82BA23C0CD3D48DE2C318938FCAD
SHA-512:	90B07AFD72EE353BEA8E2C7ECBB8CDAFB965C91E1B32C5FFE971F60C69004FDEBF5BA429B4DD455210772D2494A8AD60930A8F01C289D0199998A7CC36050F D6
Malicious:	false
Preview:	@...e.....@.....P.....1]...E.....j.....(.Microsoft.PowerShell.Commands.ManagementH.....o..b~.D.poM..... .Microsoft.PowerShell.C onsoleHost0.....C.I]..7.s.....System..4.....D...{..|f.....System.Core.D.....4..7..D.#V.....System.Management.Automation<.....i..VdqF.. .|.....System.Configuration4.....%...K... .....System.Xml..4.....@.[8]'.\.....System.Data.<.....t.,.IG....M.....System.Management...@..... .....z.U..G...5.f.1.....System.DirectoryServicesH.....WY..2.M.&..g*(g.....Microsoft.PowerShell.Security...<.....V.}...@...i.....System.Transactions.L.... .....*gQ?O.....x5.....#.Microsoft.Management.Infrastructure.8.....1...L..U;V.<}.....System.Numerics.P.....8..{...@.e..."4.....%.Microsoft.PowerShell.Com

C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe

Process:	C:\Users\user\Desktop\w4XFffGDz1.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	743944
Entropy (8bit):	7.615457036874597
Encrypted:	false
SSDEEP:	12288:Sxtg61jjk0LAta9A15fraDI+Jpaf6F+CfdGoZ8LFCSz4vtwD/zxmkR:wg61jjk0LAta9A+DIMaf6MCF18LXz
MD5:	86F98523CEB67DF5CC3431A839F63134
SHA1:	160A60824E1ADC4C0FFD5959341C6DAE4DA2E76B
SHA-256:	0E43D560502493DFADE28C5822081232EE47FD42C233F9FF473C467E51297E27
SHA-512:	CD6D79DBF6E8EC3663570F584760DB9AC50E190B4CC6E12630CB31796A88912B26556B08E01E803D3EC06874263FBDEB9AC73C8C5CD67E2749D32EBA7A23C7 B7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 88% • Antivirus: Virustotal, Detection: 58%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.gf.....0.....#... ...@....@.. ....@.....".O....@..L.....$...6...`..... ..... ..H.....text..... ..... ..`.rsrc...L....@.....@..@.rel oc.....`.....".....@..B.....".....H.....P....".....P...p+.....0..\.....(.....(.....{....r...po.....{....r...p(.....(.....(....rC..p(....o.....{....r...po....*br.. .p(...&.{.....o!...*..("...*z.,..{....,..{....o#.....($...*.0.....s%...}.....s&...}.....s'...}.....s(...}.....s%...}.....{....o)....(*....{.....o+....{....r-..p"..@A.. ....s,...o-....{.... .....s....o/....{....r?..po0....{ .....9..s1...o2....{.....o3....{....rU..po.....{.....o+....{....r-..p"

C:\Users\user\AppData\Local\Temp\RarSFX0\PO.jpg

Process:	C:\Users\user\Desktop\w4XFffGDz1.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 390x552, components 3
Category:	dropped
Size (bytes):	49161
Entropy (8bit):	7.9640442162988965
Encrypted:	false
SSDEEP:	768:LWTHytOtCeYfsfd8HAeA5Sz8Q3X1taN5adCKWEnMAyk8n/syo:qTj7Yfsfd8Ha5Sz/nHaN5adrlYsf
MD5:	E83CCB51EE74EFD2A221BE293D23C69A
SHA1:	4365CA564F7CDD7337CF0F83AC5FD64317FB4C32

SHA-256:	DA931852A19A707D01C3EDF138622B8601056C42525F8AC40CB48AF43A7410CC
SHA-512:	0252E629FBDAFDB66FF63EF76D18F25D1CA46AC3EFF019F012361DB45EBD34D1A7A9AD35F7A2FC5830676C771997633F3ABF1DC3224BD8F6BD55456B0A554A6
Malicious:	false
Preview:	......JFIF.....`.`.....C.....C.....(...."..... `...4....0 CI.#..!..i..`..!..i..`..!..i..`..!..i..`....f.....8q.+..k...8.....\4..V^...._....o.....S..6.....C?...../.;..G.~...J}fw..o.).B..S~..!..o...?|.]...'/...@...7...+.....>..}#..7.....n....+4_.....c].;....J%Ye}....c.3...-..O..[y.!../@.....f.....0....#p....|u.2.Yc[.%v.[.?..P.=K..D.,z.zN.....(...._Qv..i.....7...+..!.doY.z.E...%7..._.6..sU.;k-.:K.H.i.Y.....B...Q...IZ..SR..R.....U..0y. &I^.}...X.3Q.s3..#=.....].6&...Z6..i...e"K..&C...<...>....?.....-%...\;p.....7_.....:r..B.8....p...4...[.eN..e.P...+.^.....bB..Y...>?l.wllr.KG.L..`.....$z..FTu....`....u.{.@.....4.iK. OQ.....R-.(.g?%.....>;F.....L+d.....m.S.+`...h3.v#.a.P.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2fxchldq.gpv.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_c5dgxrmw.020.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jj5kt24d.bgw.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ncpykx4c.cxo.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped

Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ojbysllk.cf1.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ucbzawq5.ay1.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vvrkyg5q.p2h.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vxmgtnbz.hkb.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp\tmp10A5.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmp10C5.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmp10D6.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF

SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp10F6.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp1107.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp21E5.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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\tmp2BA8.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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\tmp2BB9.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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\tmp2BD9.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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\tmp2BDA.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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\tmp2BFA.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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\tmp2F6.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp306.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2

SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp327.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp337.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp348.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp358.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp369.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp3799.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp37AA.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false

SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp37BB.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp37CB.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmp37DC.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false

Preview:	SQLite format 3.....@ .....Y.....6.....j.....W.....

C:\Users\user\AppData\Local\Temp\tmp37FC.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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\tmp380D.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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\tmp4825.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp4836.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp4856.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp4876.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp4887.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84

MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....l.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmp61B0.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1583
Entropy (8bit):	5.11800490128808
Encrypted:	false
SSDEEP:	24:2di4+S2qhlZ1Muy1my3UnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtkxvn:cgergYrFdOFzOzN33ODOiDdKrsuT0v
MD5:	1CA22DCFBADB6107577BDA22B32BD86C
SHA1:	69BE9304F80294A061CB43DDDD505BB4C09ABBA9
SHA-256:	F3B7B692FA1DA9406F506EA7728E20E9094D6CE13F829D361F78189BCEDAA573
SHA-512:	36D5DB6D5A980A1C60D98A12C9407FB7B28B95FCB285D10D9DA3222C72C5BF4523E864FD394371320A13185D1F1A96A0A1F33B9610169E233F05A9ECD595CC5
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <RunOnlyIfNetwor

C:\Users\user\AppData\Local\Temp\tmp621E.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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\tmp623F.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false

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

C:\Users\user\AppData\Local\Temp\tmp624F.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmp6270.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmp6280.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmp6291.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp7F38.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp7F58.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7IwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....

C:\Users\user\AppData\Local\Temp\tmp7F78.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7IwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80

SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmp7F89.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7IwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmp7F8A.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7IwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmp7F9B.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7IwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false

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

C:\Users\user\AppData\Local\Temp\tmp8574.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1583
Entropy (8bit):	5.11800490128808
Encrypted:	false
SSDEEP:	24:2di4+S2qhlZ1Muy1my3UnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtkxvn:cgergYrFdOFzOzN33ODOiDdKrsuT0v
MD5:	1CA22DCFBADB6107577BDA22B32BD86C
SHA1:	69BE9304F80294A061CB43DDDD505BB4C09ABBA9
SHA-256:	F3B7B692FA1DA9406F506EA7728E20E9094D6CE13F829D361F78189BCEDAA573
SHA-512:	36D5DB6D5A980A1C60D98A12C9407FB7B28B95FCB285D10D9DA3222C72C5BF4523E864FD394371320A13185D1F1A96A0A1F33B9610169E233F05A9ECD595CC5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <RunOnlyIfNetwor

C:\Users\user\AppData\Local\Temp\tmp9838.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp9858.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp9869.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp9889.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp989A.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmp98BA.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84

MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....l.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmp9F36.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.704346314649071
Encrypted:	false
SSDEEP:	24:XPzUwxdkbbeZScSZIv3ZoJNWhjcfzkabZsHx:fzUwx4bK+W/+fzuR
MD5:	8B66CD8FCBCEB253D75DB5CDE6291FA2
SHA1:	6CE0386190B9753849299B268AA7B8D15F9F72E2
SHA-256:	51AD0E037F53D8EEDFEBC58112BDFA30796A0A56FBD31B65384B41896489BDB4
SHA-512:	7C46027769E82ACD4E3ACB038FB80E34792E81B0527AE318194FE22BD066699A86E9B3E55AC5A1BCAC005FE0E8B7FB70B041656DF78BF84983A97CEDAA8861DC
Malicious:	false
Preview:	BJZFPPWAPTZISGUNDSDXEATFCUXAGEFCTTZKBNFYFVKDZEMPHZAJNCAVKZWYYNTVOWAJJLGAAUTHJTXJTGQLSVTGXPQIMVSAZAKJXHFSFGEVOJ UYTICTQZLJZDQYBUBYFSZSBIOBVSAJCHKIQYCAYMMOZZQCCHGYUFOUMXHXCPNMUMVVZRXZCGPDXYDBBMVMWVPHNHLTQKLDBALGGHIVJYUKXJWA FDLMMQQUEQFWPXRQQODUGQSALTDJTROBSIRXEJYUMIWWHBCANDJZNUJGIKFXUWXKPWKATRJSISRBLFZRNYVGGJJMECDAMBUVQBAZGLVITWWCNZ FHKZSKXZCMBCAKDDJCKKLPSOZVUJSWOYBBVEUPDSCKJRFEYGLDGCUHDWDNXCLOHDPVAIFYDTEOJCHJMFFBYBQICVVKCFBQZTCRCDMDLPWOJNYP COZSCAPIZTHRAONKKSINEYBBWDVGRURGHBALLNKTXIGFWNKLQZPCTSMBRQYVMGXEIBGKILOUERUQSZIKLJQNKDPZJVSDIANCPNMTCRACOINNDA MOQOPAIVLAVJQWKZFANIEXSROWVPTCRRWMWEOIFZXRTNMYBGRZIKPJCTJYJQFKGVOKPTJYXUDCYYOIPMURGGXZGVLUDYKKODERMFIEIWKVSJAR DMDMBGKRQHSUCNHMIFNOOKAZIJQSDSIGSBRMCBLXMKFSZZUAJROFXWXYRGSBMDTXFEMBZEMCYBLNRDJBWBOCUMLSOLNUPTETGCYW ROACYQSFXBWNHGWPJVQNWAWKUVISCLHXAODXHGTGYBIVDGQQULRMEJMCYHRYXYWXLQTNEIINUCYEPKOEPHTQOQWVAZSBUDRHGYAF VQYNMYCERIVKOVOQNJLBIXTRBDBHNTZPWPYCVFUNIEAVJGCCWWHQQNTFCFYJDTKIZERPJVHSNNBWBOTMBMGRTKDWRLWPSEQAWSWD OFSPSEHOQRGFTQGBAGLJEZFNAHFMRNONCLEXLHXV

C:\Users\user\AppData\Local\Temp\tmp9F46.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696178193607948
Encrypted:	false
SSDEEP:	24:/X8jyAbnZdGxzRopIlg0xlAqLR61W80Ic9ALjzEk1CceqZQ:gyYnjGxdKL8NlMAzEk0EK
MD5:	960ECA5919CC00E1B4542A6E039F413E
SHA1:	2079091F1BDF5B543413D549EF9C47C5269659BA
SHA-256:	A103755C416B99D910D0F9B374453FADF614C0C87307A63DB0591D47EBBD14F4
SHA-512:	57D6AD727BEB9ADB7DED05BC0FCE84B43570492DA4E7A0CCAB42FFF2D4EEF6410AEDC446F2D2F07D9CE524C4640B0FB6E13DCD819051E7B233B35F8672A5ADB7
Malicious:	false
Preview:	EFOYFBOLXACUDYURQVAYVJXHJUGEEDPZADUOAPPOQQWQWQUHVVNJESQUUMLWZGSPUVGMFUNVUAJZVMUXELMWQMQASSSGGGJJGKEX ZJITZCZHBFNFKPSAPJIYNYUGZHKNTNXKHXTBXQPWUVNOKJUTUOXNNMDSUPTQRWVDMMOHKVXWMJEBHSPNNEQFXTJSRJUQDTTDGEDEKBKLUEAXKK KWXKHTVKNTWBHTZOKZNDMJXKTTGHRNAWWIBUILXUMWZIMCXVXLGVWBIWAGGRITYGTHZCIUGGSPBVQPVSAMZBKHRKSRUKMYEZBGFASYOHNDHDAZ ICVMOQUNZQXFSSSWJJUJLOPCNSUDNPJGXSQCNLKWNAYAVAFMTSLCNOUBHQKHOIALXKEFDFFQBAGKRNRBIWVREZJOOFMLXAZTWLEAOZRHRBFSBO NLILGVTOFKSPDKLHKEYWTXRPOWVHUMWWBBJNKSDDHCZCEZBDSJNMTTRGVZQVZUMECWAMCSNGCNYLUINFNXYCBEUKXUHVXAVTHIPURBBNFYVJTF MOLRZVAXLTLVSXETAIDBKHKCPFZAFQDPCXVFIVQQGEEICSHLCAYFSNSDHOELLSCZOGAAUENDMPCOCUFYZDMLPBNKDUGRDZRARSOMIJFRZRZUIH DMSAFFCNVKSOSQISTWGPAEHFMPZCCZNXMQBAWCBEUPECUJREOJQIHRSWCZZFJMFLJKICDWHXVLIXNXPRQGJYJUOGNEDHQPGFRLOHFADQRBTSXN GFAZNOZBJCPSPRRNIVIHFGIRZACAKFSLJETQMVKRUZJTTQSUXQEUOQNSNEMJADFUZUYAEXCLKPKWEYZNEOFNRPIUJKDSUTOXHDBKNTEVKKRRKW GOAZKYTICBSAEESHOCGXXGAWBZZLXBQCOVSSJALBIGTSKJTMZXGQLEURKHCIHHNDAYOKUXKAVYIWQFZVMPKEXXMPJUYHRWAIPFWTLCJRNQCRDE NEBUALFGVEULSBFIKWOO

C:\Users\user\AppData\Local\Temp\tmp9F47.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697358951122591

Encrypted:	false
SSDEEP:	24:GllFjmGrUw8wsY1UbsUhBRShwdYjDuvHNeGXNei:WFewtsZZp8DkHzNL
MD5:	244A1B624BD2C9C3A0D660425CB1F3C6
SHA1:	FB6C19991CC49A27F0277F54D88B4522F479BE5F
SHA-256:	E8C5EAACF4D2C4A65761719C311785A7873F0B25D849418ED86BBFE9D7F55C96
SHA-512:	9875E6DE2ACC859CACC2873F537DDE6ED4EC8CA00CBA3D28535E0440D76FFD475B66C52B6217D311D301C4B9A097619CF29A26B2FD54D03CD27A20A17EC9C A31
Malicious:	false
Preview:	GRXZDKKVDBUGJWVAVQNLKHTVWJFMWUAIFGXJYDZTDDYOZYAHDDDHNXHNVSFVZJEMKSJXGDABHWXKQZCQXBMLFZCFZRGZPZWYYNETLMDWOLDLPI FOVKRDMQEWUEHKITHNGNRTRZWQHFMBDECTTQKFDEVNVHBAPCNMCJNWWITPVACWBIUNPCYFZKGJXCMBWDNHDCVDCGEKHYPPPEGKPC PMYZEKRCOGRHDFANVZFDZEKZWOKLRIOUPCTJCKQPECVEEGNTLJWZOKHSKZRNLJEDQLEQNRWIYLSXHSNVGFTCDJOFJSSGANZFCFSTDUPYBCCAPQ WVVVHWQMAMBVDQNABQSQOSDYDMOVPXENCAXSTPDCENIQOWPCOQHPSISEOWFKMBLGAZRALPTAYHDZLKJTCHXGTPXNIVUMCOJRZXPU VUFPCWEAEZMMLATLTGHPJIMHWFBUWIATNBBPFGVFXNULJLRYLAGRNCKVAJADSLQGVLGIYOHDIWUERAQSCTFBMXCMLCXSHZGTWPBCVHUYPVAFSB ZNBGAGMHGULJYULEEHPGNBGEQRAOPBXXMZIUIPJMFAOVNMZZTOZGOZOJPKWCEFTTAVUBAADATZYJDWSZEZPLDTGYCYWTSDQTIMZHCKMQLZFEYS YUUWFJSYEFNDDKQMZVTBOZLQBDKFHMMKIYQPFKZLTSHIJVNPHPCTWBWPTTKDHDZEMDVWXXBLPWLCSSBMTLIVOVYOKQCJKTYJWGJUBQUGQVBYJQ QLLGTHWSPFLDMDWBTOQUISHXBCHIJKAJFIPBNKMWVQGUSJVNKXAXFDNOBYJXMWRDAZWUJSRMMFQXDPYYKOFBEROBQMDZHDZZHOEI OKDOCHQQDQQRHOROOIFAGQEJZJFZIGPJIRWVNQYZAJAHAWIEFFNXLXQWIUWYSGZDFYPCCGWYBBFQQMSMJBRIUPFBWIHWJWVCYOBNNXKIIWTIXO WRVLFBGPGWFQTGPUNWKWUUMQXIKNCLTTGYHBMKXJ

C:\Users\user\AppData\Local\Temp\tmp9F58.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.704346314649071
Encrypted:	false
SSDEEP:	24:XPzUwxdkbbeZScSZIv3ZoJNWhjcfzkabZsHx:fzUwx4bK+W/+fzuR
MD5:	8B66CD8FCBCEB253D75DB5CDE6291FA2
SHA1:	6CE0386190B9753849299B268AA7B8D15F9F72E2
SHA-256:	51AD0E037F53D8EEDFEBC58112BDFA30796A0A56FBD31B65384B41896489BDB4
SHA-512:	7C46027769E82ACD4E3ACB038FB80E34792E81B0527AE318194FE22BD066699A86E9B3E55AC5A1BCAC005FE0E8B7FB70B041656DF78BF84983A97CEDAA8861 DC
Malicious:	false
Preview:	BJZFPPWAPTZISGUNDSDXEATFCUXAGEFCTTZKBNFYFVKDZEMPHZAJNCAVKZWYYNTVOWAJJLGAAUTHJTXJTGQLSVTGXPQIMVSAZAKJXHFSFGEVOJ UYTICTQZLJZDQYBUBYFSZSBIOBVSAJCHKIQYCAYMMOZZQCCHGYUFOUMXHXCPNMUMVVZRXZCGPDXYDBBMVMWVPHNHLTQKLDBALGGHIVJYUKXJWA FDLMMQQUEQFWPXRQQODUGQSALTDJTROBSIRXEJYUMIWWHBCANDJZNUJGIKFXUWXKPWKATRJSISRBLFZRNYVGGJJMECDAMBUVQBAZGLVITWWCNZ FHKZSKXZCMBCAKDDJCKKLPSOZVUJSWOYBBVEUPDSCKJRFEYGLDGCUHDWDNXCLOHDPVAIFYDTEOJCHJMFFBYBQICVVKCFBQZTCRCDMDLPWOJNYP COZSCAPIZTHRAONKKSINEYBBWDVGRURGHBALLNKTXIGFWNKLQZPCTSMBRQYVMGXEIBGKILOUERUQSZIKLJQNKDPZJVSDIANCPNMTCRACOINNDA MOQOPAIVLAVJQWKZFANIEXSROWVPTCRRWMWEOIFZXRTNMYBGRZIKPJCTJYJQFKGVOKPTJYXUDCYYOIPMURGGXZGVLUDYKKODERMFIEIWKVSJAR DMDMBGKRQHSUCNHMIFNOOKAZIJQSDSIGSBRMCBLXMKFSZZUAJROFXWXYRGSBMDTXFEMBZEMCYBLNRDJBWBOCUMLSOLNUPTETGCYW ROACYQSFXBWNHGWPJVQNWAWKUVISCLHXAODXHGTGYBIVDGQQULRMEJMCYHRYXYWXLQTNEIINUCYEPKOEPHTQOQWVAZSBUDRHGYAF VQYNMYCERIVKOVOQNJLBIXTRBDBHNTZPWPYCVFUNIEAVJGCCWWHQQNTFCFYJDTKIZERPJVHSNNBWBOTMBMGRTKDWRLWPSEQAWSWD OFSPSEHOQRGFTQGBAGLJEZFNAHFMRNONCLEXLHXV

C:\Users\user\AppData\Local\Temp\tmp9F59.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696178193607948
Encrypted:	false
SSDEEP:	24:/X8jyAbnZdGxzRopIlg0xlAqLR61W80Ic9ALjzEk1CceqZQ:gyYnjGxdKL8NlMAzEk0EK
MD5:	960ECA5919CC00E1B4542A6E039F413E
SHA1:	2079091F1BDF5B543413D549EF9C47C5269659BA
SHA-256:	A103755C416B99D910D0F9B374453FADF614C0C87307A63DB0591D47EBBD14F4
SHA-512:	57D6AD727BEB9ADB7DED05BC0FCE84B43570492DA4E7A0CCAB42FFF2D4EEF6410AEDC446F2D2F07D9CE524C4640B0FB6E13DCD819051E7B233B35F8672A5 ADB7
Malicious:	false
Preview:	EFOYFBOLXACUDYURQVAYVJXHJUGEEDPZADUOAPPOQQWQWQUHVVNJESQUUMLWZGSPUVGMFUNVUAJZVMUXELMWQMQASSSGGGJJGKEX ZJITZCZHBFNFKPSAPJIYNYUGZHKNTNXKHXTBXQPWUVNOKJUTUOXNNMDSUPTQRWVDMMOHKVXWMJEBHSPNNEQFXTJSRJUQDTTDGEDEKBKLUEAXKK KWXKHTVKNTWBHTZOKZNDMJXKTTGHRNAWWIBUILXUMWZIMCXVXLGVWBIWAGGRITYGTHZCIUGGSPBVQPVSAMZBKHRKSRUKMYEZBGFASYOHNDHDAZ ICVMOQUNZQXFSSSWJJUJLOPCNSUDNPJGXSQCNLKWNAYAVAFMTSLCNOUBHQKHOIALXKEFDFFQBAGKRNRBIWVREZJOOFMLXAZTWLEAOZRHRBFSBO NLILGVTOFKSPDKLHKEYWTXRPOWVHUMWWBBJNKSDDHCZCEZBDSJNMTTRGVZQVZUMECWAMCSNGCNYLUINFNXYCBEUKXUHVXAVTHIPURBBNFYVJTF MOLRZVAXLTLVSXETAIDBKHKCPFZAFQDPCXVFIVQQGEEICSHLCAYFSNSDHOELLSCZOGAAUENDMPCOCUFYZDMLPBNKDUGRDZRARSOMIJFRZRZUIH DMSAFFCNVKSOSQISTWGPAEHFMPZCCZNXMQBAWCBEUPECUJREOJQIHRSWCZZFJMFLJKICDWHXVLIXNXPRQGJYJUOGNEDHQPGFRLOHFADQRBTSXN GFAZNOZBJCPSPRRNIVIHFGIRZACAKFSLJETQMVKRUZJTTQSUXQEUOQNSNEMJADFUZUYAEXCLKPKWEYZNEOFNRPIUJKDSUTOXHDBKNTEVKKRRKW GOAZKYTICBSAEESHOCGXXGAWBZZLXBQCOVSSJALBIGTSKJTMZXGQLEURKHCIHHNDAYOKUXKAVYIWQFZVMPKEXXMPJUYHRWAIPFWTLCJRNQCRDE NEBUALFGVEULSBFIKWOO

C:\Users\user\AppData\Local\Temp\tmp9F5A.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697358951122591
Encrypted:	false
SSDEEP:	24:GllFjmGrUw8wsY1UbsUhBRShwdYjDuvHNeGXNei:WFewtsZZp8DkHzNL
MD5:	244A1B624BD2C9C3A0D660425CB1F3C6
SHA1:	FB6C19991CC49A27F0277F54D88B4522F479BE5F
SHA-256:	E8C5EAACF4D2C4A65761719C311785A7873F0B25D849418ED86BBFE9D7F55C96
SHA-512:	9875E6DE2ACC859CACC2873F537DDE6ED4EC8CA00CBA3D28535E0440D76FFD475B66C52B6217D311D301C4B9A097619CF29A26B2FD54D03CD27A20A17EC9 A31
Malicious:	false
Preview:	GRXZDKKVDBUGJWVAVQNLKHTVWJFMWUAIFGXJYDZTDDYOZYAHDDDHNXHNVSFVZJEMKSJXGDABHWXKQZCQXBMLFZCFZRGZPZWYYNETLMDWOLDLPI FOVKRDMQEWUEHKITHNGNRTRZWQHFMBDECTTQKFDEVNVHBAPCNMCJNWWITPVACWBIUNPCYFZKGJXCMBWDNHDCVDCGEKHYPPPEGKPC PMYZEKRCOGRHDFANVZFDZEKZWOKLRIOUPCTJCKQPECVEEGNTLJWZOKHSKZRNLJEDQLEQNRWIYLSXHSNVGFTCDJOFJSSGANZFCFSTDUPYBCCAPQ WVVVHWQMAMBVDQNABQSQOSDYDMOVPXENCAXSTPDCENIQOWPCOQHPSISEOWFKMBLGAZRALPTAYHDZLKJTCHXGTPXNIVUMCOJRZXPU VUFPCWEAEZMMLATLTGHPJIMHWFBUWIATNBBPFGVFXNULJLRYLAGRNCKVAJADSLQGVLGIYOHDIWUERAQSCTFBMXCMLCXSHZGTWPBCVHUYPVAFSB ZNBGAGMHGULJYULEEHPGNBGEQRAOPBXXMZIUIPJMFAOVNMZZTOZGOZOJPKWCEFTTAVUBAADATZYJDWSZEZPLDTGYCYWTSDQTIMZHCKMQLZFEYS YUUWFJSYEFNDDKQMZVTBOZLQBDKFHMMKIYQPFKZLTSHIJVNPHPCTWBWPTTKDHDZEMDVWXXBLPWLCSSBMTLIVOVYOKQCJKTYJWGJUBQUGQVBYJQ QLLGTHWSPFLDMDWBTOQUISHXBCHIJKAJFIPBNKMWVQGUSJVNKXAXFDNOBYJXMWRDAZWUJSRMMFQXDPYYKOFBEROBQMDZHDZZHOEI OKDOCHQQDQQRHOROOIFAGQEJZJFZIGPJIRWVNQYZAJAHAWIEFFNXLXQWIUWYSGZDFYPCCGWYBBFQQMSMJBRIUPFBWIHWJWVCYOBNNXKIIWTIXO WRVLFBGPGWFQTGPUNWKWUUMQXIKNCLTTGYHBMKXJ

C:\Users\user\AppData\Local\Temp\tmpA0AE.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88 F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpA0BE.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88 F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpB5DE.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7lwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpB5EF.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmpB600.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmpB610.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow

MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmpB621.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmpB631.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmpB642.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false

Preview:	SQLite format 3.....@ .....Y.....6.....j.....W.....

C:\Users\user\AppData\Local\Temp\tmpBA4F.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.704346314649071
Encrypted:	false
SSDEEP:	24:XPzUwxdkbbeZScSZIv3ZoJNWhjcfzkabZsHx:fzUwx4bK+W/+fzuR
MD5:	8B66CD8FCBCEB253D75DB5CDE6291FA2
SHA1:	6CE0386190B9753849299B268AA7B8D15F9F72E2
SHA-256:	51AD0E037F53D8EEDFEBC58112BDFA30796A0A56FBD31B65384B41896489BDB4
SHA-512:	7C46027769E82ACD4E3ACB038FB80E34792E81B0527AE318194FE22BD066699A86E9B3E55AC5A1BCAC005FE0E8B7FB70B041656DF78BF84983A97CEDAA8861DC
Malicious:	false
Preview:	BJZFPPWAPTZISGUNDSDXEATFCUXAGEFCTTZKBNFYFVKDZEMPHZAJNCAVKZWYYNTVOWAJJLGAAUTHJTXJTGQLSVTGXPQIMVSAZAKJXHFSFGEVOJ UYTICTQZLJZDQYBUBYFSZSBIOBVSAJCHKIQYCAYMMOZZQCCHGYUFOUMXHXCPNMUMVVZRXZCGPDXYDBBMVMWVPHNHLTQKLDBALGGHIVJYUKXJWA FDLMMQQUEQFWPXRQQODUGQSALTDJTROBSIRXEJYUMIWWHBCANDJZNUJGIKFXUWXKPWKATRJSISRBLFZRNYVGGJJMECDAMBUVQBAZGLVITWWCNZ FHKZSKXZCMBCAKDDJCKKLPSOZVUJSWOYBBVEUPDSCKJRFEYGLDGCUHDWDNXCLOHDPVAIFYDTEOJCHJMFFBYBQICVVKCFBQZTCRCDMDLPWOJNYP COZSCAPIZTHRAONKKSINEYBBWDVGRURGHBALLNKTXIGFWNKLQZPCTSMBRQYVMGXEIBGKILOUERUQSZIKLJQNKDPZJVSDIANCPNMTCRACOINNDA MOQOPAIVLAVJQWKZFANIEXSROWVPTCRRWMWEOIFZXRTNMYBGRZIKPJCTJYJQFKGVOKPTJYXUDCYYOIPMURGGXZGVLUDYKKODERMFIEIWKVSJAR DMDMBGKRQHSUCNHMIFNOOKAZIJQSDSIGSBRMCBLXMKFSZZUAJROFXWXYRGSBMDTXFEMBZEMCYBLNRDJBWBOCUMLSOLNUPTETGCYW ROACYQSFXBWNHGWPJVQNWAWKUVISCLHXAODXHGTGYBIVDGQQULRMEJMCYHRYXYWXLQTNEIINUCYEPKOEPHTQOQWVAZSBUDRHGYAF VQYNMYCERIVKOVOQNJLBIXTRBDBHNTZPWPYCVFUNIEAVJGCCWWHQQNTFCFYJDTKIZERPJVHSNNBWBOTMBMGRTKDWRLWPSEQAWSWD OFSPSEHOQRGFTQGBAGLJEZFNAHFMRNONCLEXLHXV

C:\Users\user\AppData\Local\Temp\tmpBA60.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696178193607948
Encrypted:	false
SSDEEP:	24:/X8jyAbnZdGxzRopIIg0xlAqLR61W80Ic9ALjzEk1CceqZQ:gyYnjGxdKL8NlMAzEk0EK
MD5:	960ECA5919CC00E1B4542A6E039F413E
SHA1:	2079091F1BDF5B543413D549EF9C47C5269659BA
SHA-256:	A103755C416B99D910D0F9B374453FADF614C0C87307A63DB0591D47EBBD14F4
SHA-512:	57D6AD727BEB9ADB7DED05BC0FCE84B43570492DA4E7A0CCAB42FFF2D4EEF6410AEDC446F2D2F07D9CE524C4640B0FB6E13DCD819051E7B233B35F8672A5ADB7
Malicious:	false
Preview:	EFOYFBOLXACUDYURQVAYVJXHJUGEEDPZADUOAPPOQQWQWQUHVVNJESQUUMLWZGSPUVGMFUNVUAJZVMUXELMWQMQASSSGGGJJGKEX ZJITZCZHBFNFKPSAPJIYNYUGZHKNTNXKHXTBXQPWUVNOKJUTUOXNNMDSUPTQRWVDMMOHKVXWMJEBHSPNNEQFXTJSRJUQDTTDGEDEKBKLUEAXKK KWXKHTVKNTWBHTZOKZNDMJXKTTGHRNAWWIBUILXUMWZIMCXVXLGVWBIWAGGRITYGTHZCIUGGSPBVQPVSAMZBKHRKSRUKMYEZBGFASYOHNDHDAZ ICVMOQUNZQXFSSSWJJUJLOPCNSUDNPJGXSQCNLKWNAYAVAFMTSLCNOUBHQKHOIALXKEFDFFQBAGKRNRBIWVREZJOOFMLXAZTWLEAOZRHRBFSBO NLILGVTOFKSPDKLHKEYWTXRPOWVHUMWWBBJNKSDDHCZCEZBDSJNMTTRGVZQVZUMECWAMCSNGCNYLUINFNXYCBEUKXUHVXAVTHIPURBBNFYVJTF MOLRZVAXLTLVSXETAIDBKHKCPFZAFQDPCXVFIVQQGEEICSHLCAYFSNSDHOELLSCZOGAAUENDMPCOCUFYZDMLPBNKDUGRDZRARSOMIJFRZRZUIH DMSAFFCNVKSOSQISTWGPAEHFMPZCCZNXMQBAWCBEUPECUJREOJQIHRSWCZZFJMFLJKICDWHXVLIXNXPRQGJYJUOGNEDHQPGFRLOHFADQRBTSXN GFAZNOZBJCPSPRRNIVIHFGIRZACAKFSLJETQMVKRUZJTTQSUXQEUOQNSNEMJADFUZUYAEXCLKPKWEYZNEOFNRPIUJKDSUTOXHDBKNTEVKKRRKW GOAZKYTICBSAEESHOCGXXGAWBZZLXBQCOVSSJALBIGTSKJTMZXGQLEURKHCIHHNDAYOKUXKAVYIWQFZVMPKEXXMPJUYHRWAIPFWTLCJRNQCRDE NEBUALFGVEULSBFIKWOO

C:\Users\user\AppData\Local\Temp\tmpBA61.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697358951122591
Encrypted:	false
SSDEEP:	24:GllFjmGrUw8wsY1UbsUhBRShwdYjDuvHNeGXNei:WFewtsZZp8DkHzNL
MD5:	244A1B624BD2C9C3A0D660425CB1F3C6
SHA1:	FB6C19991CC49A27F0277F54D88B4522F479BE5F
SHA-256:	E8C5EAACF4D2C4A65761719C311785A7873F0B25D849418ED86BBFE9D7F55C96

SHA-512:	9875E6DE2ACC859CACC2873F537DDE6ED4EC8CA00CBA3D28535E0440D76FFD475B66C52B6217D311D301C4B9A097619CF29A26B2FD54D03CD27A20A17EC9(A31
Malicious:	false
Preview:	GRXZDKKVDBUGJWVAVQNLKHTVWJFMWUAIFGXJYDZTDDYOZYAHDDDHNXHNVSFVZJEMKSJXGDABHWXKQZCQXBMLFZCFZRGZPZWYYNETLMDWOLDLPI FOVKRDMQEWUEHKITHNGNRTRZWQHFMBDECTTQKFDEVNVHBAPCNMCJNWWITPVACWBIUNPCYFZKGJXCMBWDNHDCVDCGEKHYPPPEGKPC PMYZEKRCOGRHDFANVZFDZEKZWOKLRIOUPCTJCKQPECVEEGNTLJWZOKHSKZRNLJEDQLEQNRWIYLSXHSNVGFTCDJOFJSSGANZFCFSTDUPYBCCAPQ WVVVHWQMAMBVDQNABQSQOSDYDMOVPXENCAXSTPDCENIQOWPCOQHPSISEOWFKMBLGAZRALPTAYHDZLKJTCHXGTPXNIVUMCOJRZXPU VUFPCWEAEZMMLATLTGHPJIMHWFBUWIATNBBPFGVFXNULJLRYLAGRNCKVAJADSLQGVLGIYOHDIWUERAQSCTFBMXCMLCXSHZGTWPBCVHUYPVAFSB ZNBGAGMHGULJYULEEHPGNBGEQRAOPBXXMZIUIPJMFAOVNMZZTOZGOZOJPKWCEFTTAVUBAADATZYJDWSZEZPLDTGYCYWTSDQTIMZHCKMQLZFEYS YUUWFJSYEFNDDKQMZVTBOZLQBDKFHMMKIYQPFKZLTSHIJVNPHPCTWBWPTTKDHDZEMDVWXXBLPWLCSSBMTLIVOVYOKQCJKTYJWGJUBQUGQVBYJQ QLLGTHWSPFLDMDWBTOQUISHXBCHIJKAJFIPBNKMWVQGUSJVNKXAXFDNOBYJXMWRDAZWUJSRMMFQXDPYYKOFBEROBQMDZHDZZHOEI OKDOCHQQDQQRHOROOIFAGQEJZJFZIGPJIRWVNQYZAJAHAWIEFFNXLXQWIUWYSGZDFYPCCGWYBBFQQMSMJBRIUPFBWIHWJWVCYOBNNXKIIWTIXO WRVLFBGPGWFQTGPUNWKWUUMQXIKNCLTTGYHBMKXJ

C:\Users\user\AppData\Local\Temp\tmpBA71.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.704346314649071
Encrypted:	false
SSDEEP:	24:XPzUwxdkbbeZScSZIv3ZoJNWhjcfzkabZsHx:fzUwx4bK+W/+fzuR
MD5:	8B66CD8FCBCEB253D75DB5CDE6291FA2
SHA1:	6CE0386190B9753849299B268AA7B8D15F9F72E2
SHA-256:	51AD0E037F53D8EEDFEBC58112BDFA30796A0A56FBD31B65384B41896489BDB4
SHA-512:	7C46027769E82ACD4E3ACB038FB80E34792E81B0527AE318194FE22BD066699A86E9B3E55AC5A1BCAC005FE0E8B7FB70B041656DF78BF84983A97CEDAA8861DC
Malicious:	false
Preview:	BJZFPPWAPTZISGUNDSDXEATFCUXAGEFCTTZKBNFYFVKDZEMPHZAJNCAVKZWYYNTVOWAJJLGAAUTHJTXJTGQLSVTGXPQIMVSAZAKJXHFSFGEVOJ UYTICTQZLJZDQYBUBYFSZSBIOBVSAJCHKIQYCAYMMOZZQCCHGYUFOUMXHXCPNMUMVVZRXZCGPDXYDBBMVMWVPHNHLTQKLDBALGGHIVJYUKXJWA FDLMMQQUEQFWPXRQQODUGQSALTDJTROBSIRXEJYUMIWWHBCANDJZNUJGIKFXUWXKPWKATRJSISRBLFZRNYVGGJJMECDAMBUVQBAZGLVITWWCNZ FHKZSKXZCMBCAKDDJCKKLPSOZVUJSWOYBBVEUPDSCKJRFEYGLDGCUHDWDNXCLOHDPVAIFYDTEOJCHJMFFBYBQICVVKCFBQZTCRCDMDLPWOJNYP COZSCAPIZTHRAONKKSINEYBBWDVGRURGHBALLNKTXIGFWNKLQZPCTSMBRQYVMGXEIBGKILOUERUQSZIKLJQNKDPZJVSDIANCPNMTCRACOINNDA MOQOPAIVLAVJQWKZFANIEXSROWVPTCRRWMWEOIFZXRTNMYBGRZIKPJCTJYJQFKGVOKPTJYXUDCYYOIPMURGGXZGVLUDYKKODERMFIEIWKVSJAR DMDMBGKRQHSUCNHMIFNOOKAZIJQSDSIGSBRMCBLXMKFSZZUAJROFXWXYRGSBMDTXFEMBZEMCYBLNRDJBWBOCUMLSOLNUPTETGCYW ROACYQSFXBWNHGWPJVQNWAWKUVISCLHXAODXHGTGYBIVDGQQULRMEJMCYHRYXYWXLQTNEIINUCYEPKOEPHTQOQWVAZSBUDRHGYAF VQYNMYCERIVKOVOQNJLBIXTRBDBHNTZPWPYCVFUNIEAVJGCCWWHQQNTFCFYJDTKIZERPJVHSNNBWBOTMBMGRTKDWRLWPSEQAWSWD OFSPSEHOQRGFTQGBAGLJEZFNAHFMRNONCLEXLHXV

C:\Users\user\AppData\Local\Temp\tmpBA72.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696178193607948
Encrypted:	false
SSDEEP:	24:/X8jyAbnZdGxzRopIlg0xlAqLR61W80Ic9ALjzEk1CceqZQ:gyYnjGxdKL8NlMAzEk0EK
MD5:	960ECA5919CC00E1B4542A6E039F413E
SHA1:	2079091F1BDF5B543413D549EF9C47C5269659BA
SHA-256:	A103755C416B99D910D0F9B374453FADF614C0C87307A63DB0591D47EBBD14F4
SHA-512:	57D6AD727BEB9ADB7DED05BC0FCE84B43570492DA4E7A0CCAB42FFF2D4EEF6410AEDC446F2D2F07D9CE524C4640B0FB6E13DCD819051E7B233B35F8672A5ADB7
Malicious:	false
Preview:	EFOYFBOLXACUDYURQVAYVJXHJUGEEDPZADUOAPPOQQWQWQUHVVNJESQUUMLWZGSPUVGMFUNVUAJZVMUXELMWQMQASSSGGGJJGKEX ZJITZCZHBFNFKPSAPJIYNYUGZHKNTNXKHXTBXQPWUVNOKJUTUOXNNMDSUPTQRWVDMMOHKVXWMJEBHSPNNEQFXTJSRJUQDTTDGEDEKBKLUEAXKK KWXKHTVKNTWBHTZOKZNDMJXKTTGHRNAWWIBUILXUMWZIMCXVXLGVWBIWAGGRITYGTHZCIUGGSPBVQPVSAMZBKHRKSRUKMYEZBGFASYOHNDHDAZ ICVMOQUNZQXFSSSWJJUJLOPCNSUDNPJGXSQCNLKWNAYAVAFMTSLCNOUBHQKHOIALXKEFDFFQBAGKRNRBIWVREZJOOFMLXAZTWLEAOZRHRBFSBO NLILGVTOFKSPDKLHKEYWTXRPOWVHUMWWBBJNKSDDHCZCEZBDSJNMTTRGVZQVZUMECWAMCSNGCNYLUINFNXYCBEUKXUHVXAVTHIPURBBNFYVJTF MOLRZVAXLTLVSXETAIDBKHKCPFZAFQDPCXVFIVQQGEEICSHLCAYFSNSDHOELLSCZOGAAUENDMPCOCUFYZDMLPBNKDUGRDZRARSOMIJFRZRZUIH DMSAFFCNVKSOSQISTWGPAEHFMPZCCZNXMQBAWCBEUPECUJREOJQIHRSWCZZFJMFLJKICDWHXVLIXNXPRQGJYJUOGNEDHQPGFRLOHFADQRBTSXN GFAZNOZBJCPSPRRNIVIHFGIRZACAKFSLJETQMVKRUZJTTQSUXQEUOQNSNEMJADFUZUYAEXCLKPKWEYZNEOFNRPIUJKDSUTOXHDBKNTEVKKRRKW GOAZKYTICBSAEESHOCGXXGAWBZZLXBQCOVSSJALBIGTSKJTMZXGQLEURKHCIHHNDAYOKUXKAVYIWQFZVMPKEXXMPJUYHRWAIPFWTLCJRNQCRDE NEBUALFGVEULSBFIKWOO

C:\Users\user\AppData\Local\Temp\tmpBA73.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped

Size (bytes):	1026
Entropy (8bit):	4.697358951122591
Encrypted:	false
SSDEEP:	24:GllFjmGrUw8wsY1UbsUhBRShwdYjDuvHNeGXNei:WFewtsZZp8DkHzNL
MD5:	244A1B624BD2C9C3A0D660425CB1F3C6
SHA1:	FB6C19991CC49A27F0277F54D88B4522F479BE5F
SHA-256:	E8C5EAACF4D2C4A65761719C311785A7873F0B25D849418ED86BBFE9D7F55C96
SHA-512:	9875E6DE2ACC859CACC2873F537DDE6ED4EC8CA00CBA3D28535E0440D76FFD475B66C52B6217D311D301C4B9A097619CF29A26B2FD54D03CD27A20A17EC9(A31
Malicious:	false
Preview:	GRXZDKKVDBUGJWVAVQNLKHTVWJFMWUAIFGXJYDZTDDYOZYAHDDDHNXHNVSFVZJEMKSJXGDABHWXKQZCQXBMLFZCFZRGZPZWYYNETLMDWOLDLPI FOVKRDMQEWUEHKITHNGNRTRZWQHFMBDECTTQKFDEVNVHBAPCNMCJNWWITPVACWBIUNPCYFZKGJXCMBWDNHDCVDCGEKHYPPPEGKPC PMYZEKRCOGRHDFANVZFDZEKZWOKLRIOUPCTJCKQPECVEEGNTLJWZOKHSKZRNLJEDQLEQNRWIYLSXHSNVGFTCDJOFJSSGANZFCFSTDUPYBCCAPQ WVVVHWQMAMBVDQNABQSQOSDYDMOVPXENCAXSTPDCENIQOWPCOQHPSISEOWFKMBLGAZRALPTAYHDZLKJTCHXGTPXNIVUMCOJRZXPU VUFPCWEAEZMMLATLTGHPJIMHWFBUWIATNBBPFGVFXNULJLRYLAGRNCKVAJADSLQGVLGIYOHDIWUERAQSCTFBMXCMLCXSHZGTWPBCVHUYPVAFSB ZNBGAGMHGULJYULEEHPGNBGEQRAOPBXXMZIUIPJMFAOVNMZZTOZGOZOJPKWCEFTTAVUBAADATZYJDWSZEZPLDTGYCYWTSDQTIMZHCKMQLZFEYS YUUWFJSYEFNDDKQMZVTBOZLQBDKFHMMKIYQPFKZLTSHIJVNPHPCTWBWPTTKDHDZEMDVWXXBLPWLCSSBMTLIVOVYOKQCJKTYJWGJUBQUGQVBYJQ QLLGTHWSPFLDMDWBTOQUISHXBCHIJKAJFIPBNKMWVQGUSJVNKXAXFDNOBYJXMWRDAZWUJSRMMFQXDPYYKOFBEROBQMDZHDZZHOEI OKDOCHQQDQQRHOROOIFAGQEJZJFZIGPJIRWVNQYZAJAHAWIEFFNXLXQWIUWYSGZDFYPCCGWYBBFQQMSMJBRIUPFBWIHWJWVCYOBNNXKIIWTIXO WRVLFBGPGWFQTGPUNWKWUUMQXIKNCLTTGYHBMKXJ

C:\Users\user\AppData\Local\Temp\tmpCDE5.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmpCDF5.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7IwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpCE06.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988

Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7lwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpCE16.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7lwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpCE27.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7lwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpCE38.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7lwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF

SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpCE48.tmp

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7lwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpD8D7.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88 F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpD8D8.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88 F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmpD8F8.tmp	
Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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\tmpD909.tmp	
Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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\tmpD919.tmp	
Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmpEC18.tmp	
Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped

Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmpEC29.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmpEC3A.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmpEC4A.tmp

Process:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA

SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.781604734274106
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	w4XFffGDz1.exe
File size:	920'266 bytes
MD5:	2185ecde5380054ad075b7a25ae0ea51
SHA1:	caa1b832574fc3050af5f97b6deabc21398b5c47
SHA256:	e1a01751d2ea4682e211983eb7d6d1f01876a1199ba8eb9f04e3b8594f2ee199
SHA512:	f31d6c4fc0b4533c0538975518a1ff703c9a62ffdb072570942245725d375b9ef27f0d65a37e3ed07cd52a11def9893c8c3e7d0edc884c5c9b602af61ad8e211
SSDEEP:	24576:bCdL4E+j8SmRREbtuLD4DIvu18fplg+zQWxu5y0:bcL4/ruqbtuLMDQh58
TLSH:	6E15122277D58832C2F322371975A3925A3CB8715F238ACB93E429ADEF359C19931753
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y...y....y....~..y....|.!y....}..y..+.r..y..+....y..+....y.....y.....y...y...x..%....y..%....y..%.p..y..%....y.

File Icon

Icon Hash:	3570b480858580c5

Static PE Info

General

Entrypoint:	0x41d000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x65DC537F [Mon Feb 26 09:01:51 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	10b73c5f7fc148e21f974da703236659

Entrypoint Preview

Instruction
call 00007F0D08DBDC21h
jmp 00007F0D08DBD58Dh
int3
int3

Instruction
int3
int3
int3
int3
push ecx
lea ecx, dword ptr [esp+08h]
sub ecx, eax
and ecx, 0Fh
add eax, ecx
sbb ecx, ecx
or eax, ecx
pop ecx
jmp 00007F0D08DBCCEFh
push ecx
lea ecx, dword ptr [esp+08h]
sub ecx, eax
and ecx, 07h
add eax, ecx
sbb ecx, ecx
or eax, ecx
pop ecx
jmp 00007F0D08DBCCD9h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F0D08DBC711h
push 0043BF68h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F0D08DBE447h
int3
jmp 00007F0D08DC3D4Ch
push ebp
mov ebp, esp
and dword ptr [0045B89Ch], 00000000h
sub esp, 24h
or dword ptr [0043E770h], 01h
push 0000000Ah
call dword ptr [0043218Ch]
test eax, eax
je 00007F0D08DBD8C2h
and dword ptr [ebp-10h], 00000000h
xor eax, eax
push ebx
push esi
push edi
xor ecx, ecx
lea edi, dword ptr [ebp-24h]
push ebx
cpuid
mov esi, ebx
pop ebx
nop
mov dword ptr [edi], eax
mov dword ptr [edi+04h], esi
mov dword ptr [edi+08h], ecx
xor ecx, ecx
mov dword ptr [edi+0Ch], edx

Instruction
mov eax, dword ptr [ebp-24h]
mov edi, dword ptr [ebp-20h]
mov dword ptr [ebp-0Ch], eax
xor edi, 756E6547h
mov eax, dword ptr [ebp-18h]
xor eax, 49656E69h
mov dword ptr [ebp-04h], eax
mov eax, dword ptr [ebp-1Ch]
xor eax, 6C65746Eh
mov dword ptr [ebp+00h], eax

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3cef0	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3cf24	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5d000	0x62f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x64000	0x2f38	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3a020	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x3a080	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x346f8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x32000	0x24c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3c4fc	0x100	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3023c	0x30400	eab8c49347b2363b3fdd36257b1df951	False	0.5767132852979274	data	6.682129404058095	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x32000	0xbc34	0xbe00	e5f2fdc4aee2f1a0726781d86b4f8c02	False	0.4407483552631579	data	5.126576177856284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3e000	0x1df78	0x1200	94ebd057e10782ee3aa0d3ba58c1a1bf	False	0.3856336805555556	DOS executable (block device driver w{\362ko\3050)	3.9129841433728263	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didat	0x5c000	0x17c	0x200	f6f8a7d940bc508fbb3b807359e5a063	False	0.42578125	data	3.261134286324671	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x5d000	0x62f8	0x6400	274f8184ed0865c3a4e3309a06e7038d	False	0.6695703125	data	6.732052947212191	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x64000	0x2f38	0x3000	83735fea8ebd9a3faee82aa0e6812001	False	0.7744140625	data	6.687384285279319	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
PNG	0x5d554	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States	1.0027729636048528
PNG	0x5e09c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States	0.9363390441839495
RT_ICON	0x5f648	0x162c	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced			0.906800563777308
RT_DIALOG	0x60c74	0x286	data	English	United States	0.5092879256965944
RT_DIALOG	0x60efc	0x13a	data	English	United States	0.60828025477707
RT_DIALOG	0x61038	0xec	data	English	United States	0.6991525423728814
RT_DIALOG	0x61124	0x12e	data	English	United States	0.5927152317880795
RT_DIALOG	0x61254	0x338	data	English	United States	0.45145631067961167
RT_DIALOG	0x6158c	0x252	data	English	United States	0.5757575757575758
RT_STRING	0x617e0	0x1e2	data	English	United States	0.3900414937759336
RT_STRING	0x619c4	0x1cc	data	English	United States	0.4282608695652174
RT_STRING	0x61b90	0x1b8	data	English	United States	0.45681818181818185
RT_STRING	0x61d48	0x146	data	English	United States	0.5153374233128835
RT_STRING	0x61e90	0x46c	data	English	United States	0.3454063604240283
RT_STRING	0x622fc	0x166	data	English	United States	0.49162011173184356
RT_STRING	0x62464	0x152	data	English	United States	0.5059171597633136
RT_STRING	0x625b8	0x10a	data	English	United States	0.49624060150375937
RT_STRING	0x626c4	0xbc	data	English	United States	0.6329787234042553
RT_STRING	0x62780	0x1c0	data	English	United States	0.5178571428571429
RT_STRING	0x62940	0x250	data	English	United States	0.44256756756756754
RT_GROUP_ICON	0x62b90	0x14	data			1.05
RT_MANIFEST	0x62ba4	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States	0.3957333333333333

Imports

DLL	Import
KERNEL32.dll	LocalFree, GetLastError, SetLastError, FormatMessageW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileTime, CloseHandle, CreateFileW, GetCurrentProcessId, CreateDirectoryW, RemoveDirectoryW, SetFileAttributesW, GetFileAttributesW, DeleteFileW, MoveFileW, FindClose, FindFirstFileW, FindNextFileW, InterlockedDecrement, GetVersionExW, GetModuleFileNameW, SetCurrentDirectoryW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, ExpandEnvironmentStringsW, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, GetTimeFormatW, GetDateFormatW, GetCurrentProcess, GetExitCodeProcess, WaitForSingleObject, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetNumberFormatW, GetProcessHeap, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetOEMCP, DecodePointer, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapReAlloc, HeapSize, SetStdHandle, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, SetEvent, ResetEvent, WaitForSingleObjectEx, CreateEventW, IsDebuggerPresent, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlUnwind, EncodePointer, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage
OLEAUT32.dll	VariantClear, SysFreeString, SysAllocString
gdiplus.dll	GdiplusStartup, GdipCreateHBITMAPFromBitmap, GdipCreateBitmapFromStreamICM, GdiplusShutdown, GdipCreateBitmapFromStream, GdipDisposeImage, GdipCloneImage, GdipFree, GdipAlloc

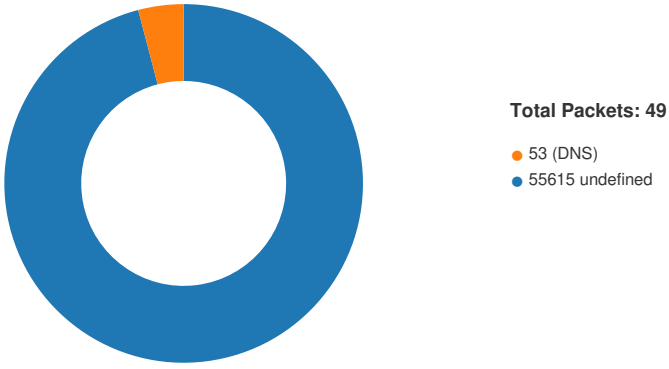
Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2024 20:22:13.592211962 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:13.597270966 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:13.597446918 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:13.614931107 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:13.619968891 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:13.962301016 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:13.968107939 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:14.436089039 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:14.477663040 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:19.484477043 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:19.484569073 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:19.489763975 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:19.489794970 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:19.746203899 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:19.746267080 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:19.746320963 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:19.746330023 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:19.746356964 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:19.746387005 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:19.746412992 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:19.790283918 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:20.549530029 CEST	49718	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:20.554758072 CEST	55615	49718	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:20.554884911 CEST	49718	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:20.564523935 CEST	49718	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:20.569586039 CEST	55615	49718	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:20.915374994 CEST	49718	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:20.920666933 CEST	55615	49718	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:21.384052038 CEST	55615	49718	45.137.22.67	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2024 20:22:21.430783987 CEST	49718	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.916909933 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.917320013 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.922207117 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.922521114 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.922700882 CEST	55615	49710	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.922755003 CEST	49710	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.923113108 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.923113108 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.928051949 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.928081989 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.928103924 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.928132057 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.928152084 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.928159952 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.928189039 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.928208113 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.928220987 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.928252935 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.928339005 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.928366899 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.928416967 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.932372093 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.932456970 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.932457924 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.932507992 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.933129072 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.933177948 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.933181047 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.933207989 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.933255911 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.933264017 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.933284998 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.933314085 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.933339119 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.933495045 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:22.974293947 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:22.974421024 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.022219896 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.022274017 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.070172071 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.070229053 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.118232965 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.118518114 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.166363001 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.166462898 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.214201927 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.220511913 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.270370960 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.270559072 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.318248034 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.318428040 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.366364002 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.366983891 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.418523073 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.418622017 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.466478109 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.466589928 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.518975973 CEST	55615	49720	45.137.22.67	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2024 20:22:23.519157887 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.524339914 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.524373055 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.524425983 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.524440050 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.524468899 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.524559021 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.524575949 CEST	49720	55615	192.168.2.5	45.137.22.67
Jun 15, 2024 20:22:23.524626970 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.524658918 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.524687052 CEST	55615	49720	45.137.22.67	192.168.2.5
Jun 15, 2024 20:22:23.524715900 CEST	55615	49720	45.137.22.67	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2024 20:22:19.792176008 CEST	61337	53	192.168.2.5	1.1.1.1
Jun 15, 2024 20:22:33.087971926 CEST	52659	53	192.168.2.5	1.1.1.1

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 15, 2024 20:22:19.792176008 CEST	192.168.2.5	1.1.1.1	0x57cb	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false
Jun 15, 2024 20:22:33.087971926 CEST	192.168.2.5	1.1.1.1	0x1de4	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
Jun 15, 2024 20:22:19.799233913 CEST	1.1.1.1	192.168.2.5	0x57cb	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Jun 15, 2024 20:22:33.103152990 CEST	1.1.1.1	192.168.2.5	0x1de4	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false

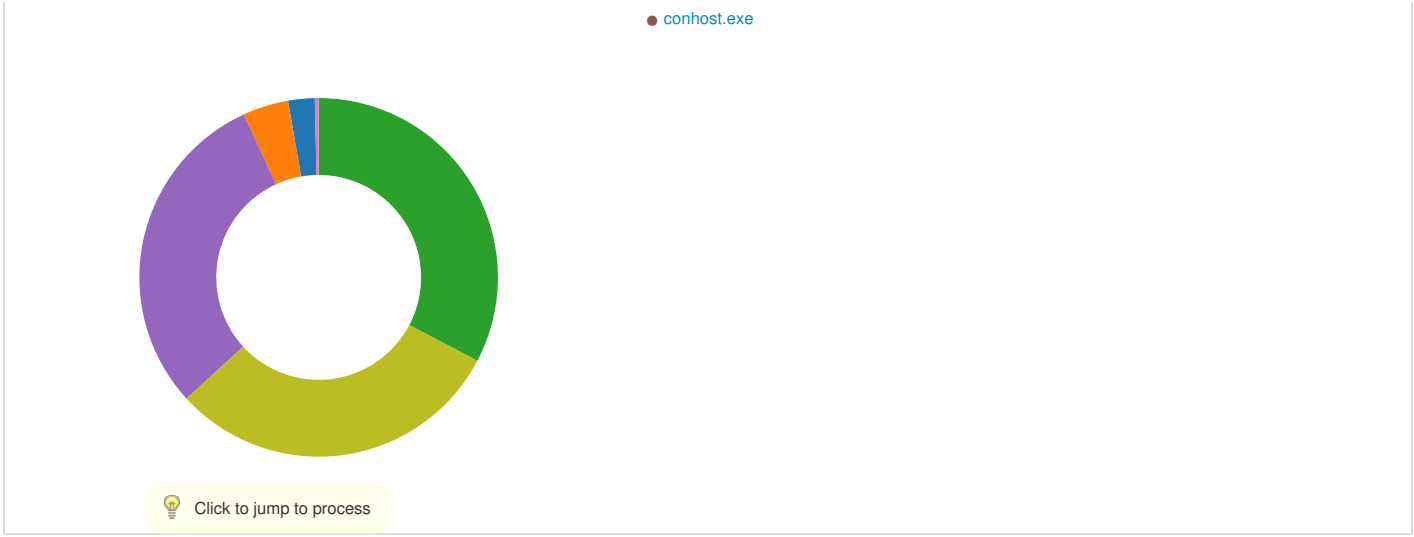
HTTP Request Dependency Graph

- 45.137.22.67:55615

Statistics

Behavior

- w4XFffGDz1.exe
- PO.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- PO.exe
- conhost.exe
- AJzHYZtQlb.exe
- WmiPrvSE.exe
- schtasks.exe
- conhost.exe
- AJzHYZtQlb.exe



System Behavior

Analysis Process: w4XFffGDz1.exe PID: 6412, Parent PID: 1028

General

Target ID:	0
Start time:	14:21:59
Start date:	15/06/2024
Path:	C:\Users\user\Desktop\w4XFffGDz1.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\w4XFffGDz1.exe"
Imagebase:	0x170000
File size:	920'266 bytes
MD5 hash:	2185ECDE5380054AD075B7A25AE0EA51
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Analysis Process: PO.exe PID: 7532, Parent PID: 6412

General

Target ID:	7
Start time:	14:22:01
Start date:	15/06/2024
Path:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe"
Imagebase:	0x600000
File size:	743'944 bytes
MD5 hash:	86F98523CEB67DF5CC3431A839F63134
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: 00000007.00000002.2160567285.000000000453C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000007.00000002.2160567285.000000000453C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000007.00000002.2160567285.000000000453C000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2160567285.0000000003C00000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000007.00000002.2160567285.0000000003C00000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000007.00000002.2160567285.0000000003C00000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 88%, ReversingLabs • Detection: 58%, Virustotal, Browse
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72BAF4C3	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72BAF4C3	unknown
C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71A813BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp61B0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7302A0B7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp61B0.tmp	success or wait	1	71A7E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AJzHYZtQlb.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 27 fd 67 66 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 04 0b 00 00 1e 00 00 00 00 00 00 12 23 0b 00 00 20 00 00 00 40 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'gf0# @@ @	success or wait	3	71A813BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp61B0.tmp	0	1583	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 46 4f 4e 53 2d 50 43 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 3c 54 72 69	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>user-PC\user</Author> </RegistrationInfo> <Tri	success or wait	1	71A79B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7302A147	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BACBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B50842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BC738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BC738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71A79B71	ReadFile

Analysis Process: powershell.exe PID: **7780**, Parent PID: **7532**

General

Target ID:	8
Start time:	14:22:08
Start date:	15/06/2024
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe"
Imagebase:	0x8d0000
File size:	433'152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ncpykx4c.cxo.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A78792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2fxchldq.gpv.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A78792	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72BAF4C3	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72BAF4C3	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	6AAA8290	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ucbzawq5.ay1.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A78792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ojbysllk.cf1.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A78792	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	7	6AAA8290	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ncpykx4c.cxo.ps1	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2fxchldq.gpv.psm1	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ucbzawq5.ay1.ps1	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ojbysllk.cf1.psm1	success or wait	1	71A7E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ncpykx4c.cxo.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A79B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2fxchldq.gpv.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A79B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ucbzawq5.ay1.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A79B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ojbysllk.cf1.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A79B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 00 00 00 14 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 14 00 fd 01 08 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	72F776C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	50 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 7f 31 5d 13 fd fd 45 fd 31 a4 86 08 6a 00 00 00 0e 00 28 00	P1]Ej(	success or wait	17	72F776C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	40	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6d 6d 61 6e 64 73 2e 4d 61 6e 61 67 65 6d 65 6e 74	Microsoft.PowerShell.Commands.Management	success or wait	17	72F776C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	262	2	00 00		success or wait	11	72F776C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	28 04 00 03	(	success or wait	1	72F776C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	1060	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0c fd 00 08 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 0d 0e fd 00 0e 0e fd 00 0f 0c fd 00 00 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 19 02 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 07 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 0a 40 00 fd 0a 40 00 fd 01 40 00 0d 02 40 00 10 0d fd 00 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 21 01 40 10 3c 01 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40	@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ @@@@!@<@@@@@@@@@@@	success or wait	1	72F776C2	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BACBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BC738A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BC738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BC738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BC738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Pb378ec07#\bc6fa6cbc82ba7e8e7f31ce87cd85b5f\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	72BBB174	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	1300	success or wait	1	72BBB27D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\1b8c564fd69668e6e62d136259980d9e\System.Data.ni.dll.aux	0	1540	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P6f792626#\fa050a0a5a69ea7573ca6cbffc254e14\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\d06877b5a0df441a8dc4c7b8d95b5d41\System.Numerics.ni.dll.aux	0	300	success or wait	1	72B50842	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	71A79B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	2	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	2	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	2	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	71A79B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectoryServices.ni.dll.aux	0	752	success or wait	3	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.A9acaf597#\28d73b1a02dd10f20826df677fab36e2\Microsoft.AppV.AppvClientComConsumer.ni.dll.aux	0	712	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	641	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	71A79B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P521220ea#\ee7238e0e97151da928155502d6b496b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Confe64a9051#\48ee4ec9441351bbe4d9095c96b8ea01\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	success or wait	74	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	104	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	309	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	160	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	767	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	767	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	417	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	4096	success or wait	16	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	950	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	488	end of file	1	71A79B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	8	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	986	end of file	2	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	4096	end of file	2	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	994	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	113	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	0	114	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	0	4096	end of file	1	71A79B71	ReadFile

Analysis Process: conhost.exe PID: **7788**, Parent PID: **7780**

General

Target ID:	9
Start time:	14:22:09
Start date:	15/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
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

Analysis Process: powershell.exe PID: **7812**, Parent PID: **7532**

General

Target ID:	10
Start time:	14:22:09
Start date:	15/06/2024
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe"
Imagebase:	0x8d0000

File size:	433'152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vxmgtnbz.hkb.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A78792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jj5kt24d.bgw.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A78792	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72BAF4C3	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72BAF4C3	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	6AAA8290	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vvrkyg5q.p2h.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A78792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c5dgxrmw.020.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A78792	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AAA8290	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	6AAA8290	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	6AAA8290	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vxmgtnbz.hkb.ps1	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jj5kt24d.bgw.psm1	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vvrkyg5q.p2h.ps1	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c5dgxrmw.020.psm1	success or wait	1	71A7E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vxmgtnbz.hkb.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A79B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jj5kt24d.bgw.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A79B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vvrkyg5q.p2h.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A79B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c5dgxrmw.020.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A79B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 00 00 00 14 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 14 00 fd 01 08 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	72F776C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	50 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 7f 31 5d 13 fd fd 45 fd 31 a4 86 08 6a 00 00 00 0e 00 28 00	P1]Ej(	success or wait	17	72F776C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	40	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6d 6d 61 6e 64 73 2e 4d 61 6e 61 67 65 6d 65 6e 74	Microsoft.PowerShell.Commands.Management	success or wait	17	72F776C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	262	2	00 00		success or wait	11	72F776C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	28 04 00 03	(	success or wait	1	72F776C2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	1060	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0c fd 00 08 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 0d 0e fd 00 0e 0e fd 00 0f 0c fd 00 00 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 19 02 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 07 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 0a 40 00 fd 0a 40 00 fd 01 40 00 0d 02 40 00 10 0d fd 00 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 21 01 40 10 3c 01 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40	@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@!@<@@@@@@@@@@@	success or wait	1	72F776C2	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BACBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BC738A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BC738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BC738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BC738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Pb378ec07#\bc6fa6cbc82ba7e8e7f31ce87cd85b5f\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	72BBB174	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	71A79B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\1b8c564fd69668e6e62d136259980d9e\System.Data.ni.dll.aux	0	1540	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	2	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P6f792626#\fa050a0a5a69ea7573ca6cbffc254e14\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\d06877b5a0df441a8dc4c7b8d95b5d41\System.Numerics.ni.dll.aux	0	300	success or wait	1	72B50842	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	8	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	3	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	5	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	3	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	2	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	71A79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	2	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	2	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	2	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\d06877b5a0df441a8dc4c7b8d95b5d41\System.Numerics.ni.dll.aux	0	300	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.A9acaf597#\28d73b1a02dd10f20826df677fab36e2\Microsoft.AppV.AppvClientComConsumer.ni.dll.aux	0	712	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	641	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	71A79B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P521220ea#\ee7238e0e97151da928155502d6b496b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Confe64a9051#\48ee4ec9441351bbe4d9095c96b8ea01\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	72B50842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BACBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	success or wait	72	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	104	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	309	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	767	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	417	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	4096	success or wait	16	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	950	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	488	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	986	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	4	71A79B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	994	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	113	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	0	4096	success or wait	4	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	0	114	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	3	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	0	191	end of file	1	71A79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	0	4096	end of file	1	71A79B71	ReadFile

Analysis Process: conhost.exe PID: **7856**, Parent PID: **7812**

General

Target ID:	11
Start time:	14:22:09
Start date:	15/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
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

Analysis Process: schtasks.exe PID: **7908**, Parent PID: **7532**

General

Target ID:	12
Start time:	14:22:09
Start date:	15/06/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\AJzHYZtQlb" /XML "C:\Users\user\AppData\Local\Temp\tmp61B0.tmp"
Imagebase:	0xbb0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	true

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp61B0.tmp	0	2	success or wait	1	BBB43E	ReadFile
C:\Users\user\AppData\Local\Temp\tmp61B0.tmp	0	1584	success or wait	1	BBB4E3	ReadFile

Analysis Process: conhost.exe PID: **7960**, Parent PID: **7908**

General

Target ID:	13
Start time:	14:22:09
Start date:	15/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
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

Analysis Process: PO.exe PID: **8068**, Parent PID: **7532**

General

Target ID:	14
Start time:	14:22:10
Start date:	15/06/2024
Path:	C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\RarSFX0\PO.exe"
Imagebase:	0xcb0000
File size:	743'944 bytes
MD5 hash:	86F98523CEB67DF5CC3431A839F63134
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: 0000000E.00000002.2274416687.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000E.00000002.2274416687.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 0000000E.00000002.2274416687.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000E.00000002.2276292357.00000000031D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72BAF4C3	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72BAF4C3	unknown
C:\Users\user\AppData\Local\Temp\tmp9F36.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9F46.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9F47.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9F58.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9F59.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9F5A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2BA8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2BB9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2BD9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2BDA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2BFA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp621E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp623F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp624F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp6270.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp6280.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp6291.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9838.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9858.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9869.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9889.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp989A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp98BA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCDE5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCDF5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCE06.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCE16.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCE27.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCE38.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCE48.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2F6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp306.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp327.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp337.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp348.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp358.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp369.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp3799.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp37AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp37BB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp37CB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp37DC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp37FC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp380D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720A246F	GetTempFileNameW
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A80794	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A80794	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9F36.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9F46.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9F47.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9F58.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9F59.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9F5A.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2BB9.tmp	success or wait	2	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2BA8.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2BD9.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp621E.tmp	success or wait	3	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2BFA.tmp	success or wait	3	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp624F.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp623F.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp6280.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9838.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp6291.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9869.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp989A.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9889.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpCDE5.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp98BA.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpCE06.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpCDF5.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp306.tmp	success or wait	3	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2F6.tmp	success or wait	2	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp327.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp3799.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp369.tmp	success or wait	2	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp37BB.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp37DC.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp37CB.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp380D.tmp	success or wait	1	71A7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp37FC.tmp	success or wait	1	71A7E04E	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BACBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B50842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BC738A	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BC738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\a3127677749631df61e96a8400ddcb87\System.Runtime.Serialization.ni.dll.aux	0	1100	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B50842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72BACBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71A79B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\bb5812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll.aux	0	536	success or wait	1	72B50842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72B50842	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9F36.tmp	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9F46.tmp	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9F47.tmp	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9F58.tmp	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9F59.tmp	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9F5A.tmp	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	144	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	747	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2BB9.tmp	0	40960	success or wait	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	146	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	747	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	146	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	747	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp621E.tmp	0	40960	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	747	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp624F.tmp	0	106496	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	146	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	747	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6280.tmp	0	106496	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	155	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	747	end of file	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	end of file	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9838.tmp	0	106496	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	747	end of file	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9869.tmp	0	106496	success or wait	1	71A79B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp989A.tmp	0	106496	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	144	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	747	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCDE5.tmp	0	106496	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	919	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCE06.tmp	0	51200	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	10	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	919	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCE27.tmp	0	51200	success or wait	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	919	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp306.tmp	0	196608	success or wait	3	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	10	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	919	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	10	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	919	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	919	end of file	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3799.tmp	0	196608	success or wait	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	20	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	919	end of file	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	end of file	2	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp37DC.tmp	0	196608	success or wait	1	71A79B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp380D.tmp	0	98304	success or wait	1	71A79B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\PO_RASMANCS	success or wait	1	70D9FC58	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\PO_RASMANCS	EnableFileTracing	dword	0	success or wait	1	70D9FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\PO_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	70D9FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\PO_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	70D9FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\PO_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	70D9FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\PO_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	70D9FC58	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\PO_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	70D9FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\PO_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	70D9FC58	unknown

Analysis Process: conhost.exe PID: **8080**, Parent PID: **8068**

General

Target ID:	15
Start time:	14:22:10
Start date:	15/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: AJzHYZtQIb.exe PID: **8164**, Parent PID: **1068**

General

Target ID:	16
Start time:	14:22:11
Start date:	15/06/2024
Path:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe
Imagebase:	0xb00000
File size:	743'944 bytes
MD5 hash:	86F98523CEB67DF5CC3431A839F63134
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.2247047739.0000000004AFD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000010.00000002.2247047739.0000000004AFD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000010.00000002.2247047739.0000000004AFD000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 88%, ReversingLabs • Detection: 58%, Virustotal, Browse
Reputation:	low
Has exited:	true

Analysis Process: WmiPrvSE.exe PID: **5020**, Parent PID: **752**

General

Target ID:	17
Start time:	14:22:11
Start date:	15/06/2024

Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff6ef0c0000
File size:	496'640 bytes
MD5 hash:	60FF40CFD7FB8FE41EE4FE9AE5FE1C51
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: schtasks.exe PID: **8028**, Parent PID: **8164**

General	
Target ID:	19
Start time:	14:22:18
Start date:	15/06/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\AJzHYZtQlb" /XML "C:\Users\user\AppData\Local\Temp\tmp8574.tmp"
Imagebase:	0xbb0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: conhost.exe PID: **7960**, Parent PID: **8028**

General	
Target ID:	20
Start time:	14:22:18
Start date:	15/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: AJzHYZtQlb.exe PID: **5404**, Parent PID: **8164**

General	
Target ID:	21
Start time:	14:22:18
Start date:	15/06/2024
Path:	C:\Users\user\AppData\Roaming\AJzHYZtQlb.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Roaming\AJzHYZtQIb.exe"
Imagebase:	0xac0000
File size:	743'944 bytes
MD5 hash:	86F98523CEB67DF5CC3431A839F63134
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000015.00000002.2357626482.0000000002FF0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

Analysis Process: conhost.exe PID: **7848**, Parent PID: **5404**

General

Target ID:	22
Start time:	14:22:18
Start date:	15/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Disassembly

No disassembly