ID: 1436386
Sample Name: app.exe
Cookbook: default.jbs
Time: 00:21:26
Date: 05/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

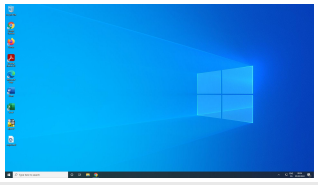
Windows Analysis Report

app.exe

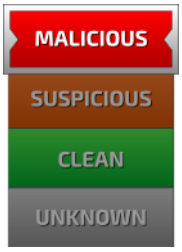
Overview

General Information

Sample name:	app.exe
Analysis ID:	1436386
MD5:	75b9ef9142a78..
SHA1:	0461f1c46644a..
SHA256:	e9bc44cf548a7..
Infos:	



Detection

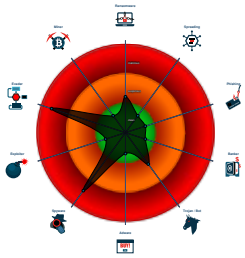


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (creates a PE f…
- Multi AV Scanner detection for drop…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Contains functionality to infect the b…
- Found many strings related to Crypt…
- Machine Learning detection for drop…
- Machine Learning detection for sam…
- PE file contains section with specia…
- PE file has a writeable .text section
- Queries memory information (via WM…
- Queries sensitive physical memory …

Classification



Process Tree

- **System is w10x64native**
- app.exe (PID: 7652 cmdline: "C:\Users\user\Desktop\app.exe" MD5: 75B9EF9142A78671D449C8D22AB6BE14)
  - conhost.exe (PID: 7972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - app.exe (PID: 7132 cmdline: "C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe" MD5: 75B9EF9142A78671D449C8D22AB6BE14)
    - conhost.exe (PID: 7152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - cmd.exe (PID: 1808 cmdline: cmd.exe /c timeout /t 5 & del /f /q C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe && exit MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - conhost.exe (PID: 5108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - timeout.exe (PID: 1172 cmdline: timeout /t 5 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/FireStealer Related Server Response - Source IP: 144.208.127.230 - Destination IP: 192.168.11.20

Timestamp:	05/05/24-00:24:50.450010
SID:	2051909
Source Port:	80
Destination Port:	49789
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance

Detected unpacking (creates a PE file in dynamic memory)

Networking

Snort IDS alert for network traffic

System Summary

PE file contains section with special chars

PE file has a writeable .text section

Data Obfuscation

Detected unpacking (creates a PE file in dynamic memory)

Persistence and Installation Behavior

Contains functionality to infect the boot sector

Boot Survival

Contains functionality to infect the boot sector

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd or bat file

Malware Analysis System Evasion

Queries memory information (via WMI often done to detect virtual machines)

Queries sensitive physical memory information (via WMI, Win32_PhysicalMemory, often done to detect virtual machines)

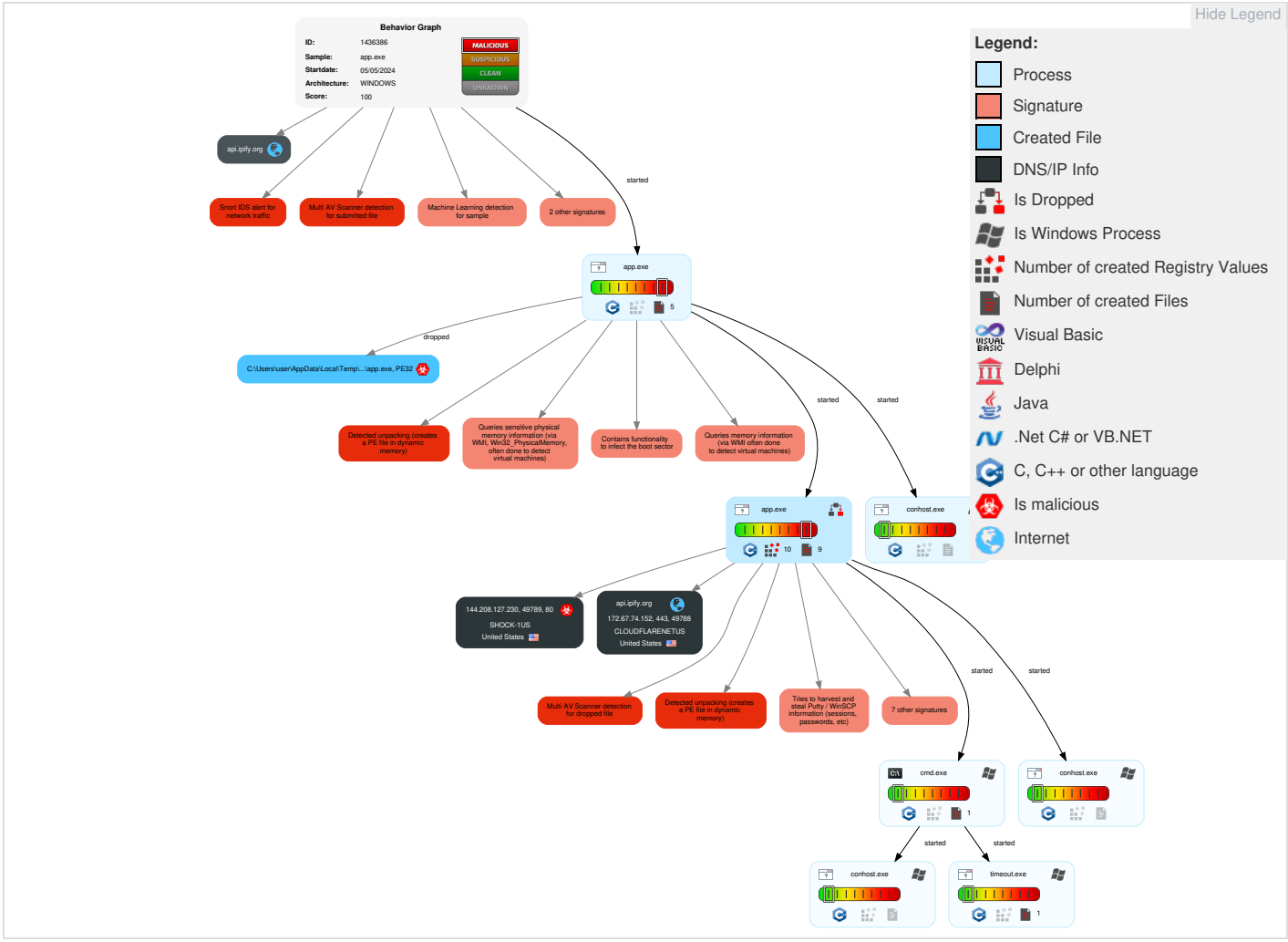
Stealing of Sensitive Information

Found many strings related to Crypto-Wallets (likely being stolen)
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Tries to harvest and steal browser information (history, passwords, etc)
Tries to steal Crypto Currency Wallets

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	3 3 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	1 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Native API	1 Bootkit	1 1 Process Injection	1 Deobfuscate /Decode Files or Information	1 Input Capture	2 File and Directory Discovery	Remote Desktop Protocol	3 Data from Local System	2 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	4 5 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	3 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Software Packing	NTDS	4 6 1 Security Software Discovery	Distributed Component Object Model	Input Capture	1 4 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 3 Virtualization/Sandbox Evasion	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 File Deletion	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 3 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 1 Process Injection	Proc Filesystem	2 System Network Configuration Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	1 Bootkit	/etc/passwd and /etc/shadow	Network Sniffing	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement

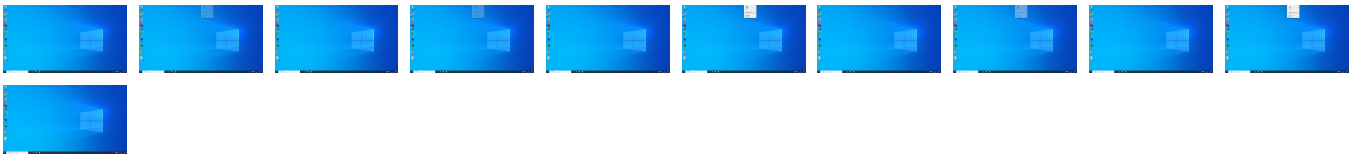
Behavior Graph



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
app.exe	11%	ReversingLabs		
app.exe	100%	Joe Sandbox ML		
app.exe	11%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe	11%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe	11%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://144.208.127.230/J	0%	Avira URL Cloud	safe	
http://144.208.127.230/v	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/w	0%	Avira URL Cloud	safe	
http://144.208.127.230/	0%	Avira URL Cloud	safe	
http://144.208.127.230/z	0%	Avira URL Cloud	safe	
http://144.208.127.230/z	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://144.208.127.230	0%	Avira URL Cloud	safe	
http://144.208.127.230/B	0%	Avira URL Cloud	safe	
http://144.208.127.230/J	0%	Virustotal		Browse
http://144.208.127.230/	0%	Virustotal		Browse
http://144.208.127.230:80/w	0%	Virustotal		Browse
http://144.208.127.230/Y	0%	Avira URL Cloud	safe	
http://144.208.127.230/U	0%	Avira URL Cloud	safe	
http://https://ocsp.quovadisoffshore.com0	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/-35b871f0a661	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/L	0%	Avira URL Cloud	safe	
http://144.208.127.230	0%	Virustotal		Browse
http://144.208.127.230/7	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/	0%	Virustotal		Browse
http://144.208.127.230/Y	0%	Virustotal		Browse
http://https://POSTHTTP/1.1Content-Type:	0%	Avira URL Cloud	safe	
http://144.208.127.230/e&	0%	Avira URL Cloud	safe	
http://https://alldrivers4devices.net	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/o	0%	Avira URL Cloud	safe	
http://144.208.127.230/7	0%	Virustotal		Browse
http://144.208.127.230/~	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/T	0%	Avira URL Cloud	safe	
http://www.quovadis.bm0	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/-35b871f0a661ozi	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/R	0%	Avira URL Cloud	safe	
http://144.208.127.230:80/T	0%	Virustotal		Browse
http://144.208.127.230U	0%	Avira URL Cloud	safe	
http://144.208.127.230/~	0%	Virustotal		Browse
http://https://alldrivers4devices.net	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ipify.org	172.67.74.152	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://144.208.127.230/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.ipify.org/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	app.exe, 00000003.00000003.3188734917.00000000058E3000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3182590144.00000000058E8000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3183161453.00000000058E8000.00000004.00000020.00020000.00000000.sdmp, Web Data.3.dr	false		high
http://https://uk.search.yahoo.com/favicon.icohttps://uk.search.yahoo.com/search	app.exe, 00000003.00000003.3188734917.00000000058E3000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3182590144.00000000058E8000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3183161453.00000000058E8000.00000004.00000020.00020000.00000000.sdmp, Web Data.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://setup.office.com/EnterPin?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	Web Data.3.dr	false		high
http://https://www.autoitscript.com/site/autoit/downloads/https://www.autoitscript.com/site/autoit/download	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://windows-drivers-x04.blogspot.com	app.exe, 00000003.00000003.3245462405.000000058E5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.autoitscript.com	app.exe, 00000003.00000003.3245462405.000000058E5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/?&brand=CHWL&utm_campaign=en&utm_source=en-et-na-us-chrome-bubble&utm_	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dl.packetstormsecurity.net/Crackers/bios/BIOS320.EXE	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://setup.office.com/home/ProvisionLoading?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8-_	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_flash	app.exe, 00000003.00000003.3177221257.000000055AC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://consent.trustarc.com	app.exe, 00000003.00000003.3245462405.000000058E5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230/z	app.exe, 00000003.00000003.3246373817.000000000956000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3177623712.0000000000956000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://144.208.127.230:80/w	app.exe, 00000003.00000003.3139260264.000000005588000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3123698644.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3134624186.0000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3130432829.0000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3132299964.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3125985144.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3128278501.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3139068962.0000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3116136458.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3136784723.0000000005586000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://144.208.127.230/v	app.exe, 00000003.00000002.3296988780.000000005518000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://setup.office.com/SignIn?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8&redirectUri=https%3A%2F%2F	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://secure.eicar.org/eicar.com;9	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com	app.exe, 00000003.00000003.3245462405.000000058E5000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3257419916.00000000055D6000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3261882543.00000000055DC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://sdlc-esd.oracle.com/ESD6/JSCDL/jdk/8u301-b09/d3c52aa6bfa54d3ca74e617f18309292/JavaSetup8u301	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://144.208.127.230/J	app.exe, 00000003.00000003.3112020011.00000000956000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3123955917.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3121520475.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3116384116.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3126108218.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3118889457.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3114263668.0000000000956000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.eicar.org/download-anti-malware-testfile/:	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://packetstormsecurity.com/https://packetstormsecurity.com/files/download/22459/BIOS320.EXEhttp	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://setup.office.com/Home/EligibileActModern?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8Microsoft	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://uk.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	app.exe, 00000003.00000003.3188734917.000000058E3000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3182590144.00000000058E8000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3183161453.00000000058E8000.00000004.00000020.00020000.00000000.sdmp, Web Data.3.dr	false		high
http://https://office.com/setup	app.exe, 00000003.00000003.3182859527.000000055F1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230/B	app.exe, 00000003.00000003.3112020011.00000000956000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3123955917.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3107954475.000000000095600.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3121520475.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3116384116.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3103448637.000000000956000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3126108218.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3118889457.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3114263668.0000000000956000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://setup.office.com/Home/EligibileActModern?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.stubdownloader.services.mozilla.com/builds/firefox-latest-ssl/en-GB/win64/b5110ff5d41570	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://lh5.googleusercontent.com/p/AF1QipOvNh-L3TTVll_wDyQd66TEaShUCp3i0iabc8se=w92-h92-n-k-no	app.exe, 00000003.00000003.3242282826.000000055C6000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3242197510.00000000058C6000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3246273895.00000000058E5000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3245462405.00000000058E5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230	app.exe, 00000003.00000002.3294569055.000000008CF000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/search?q=at	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high

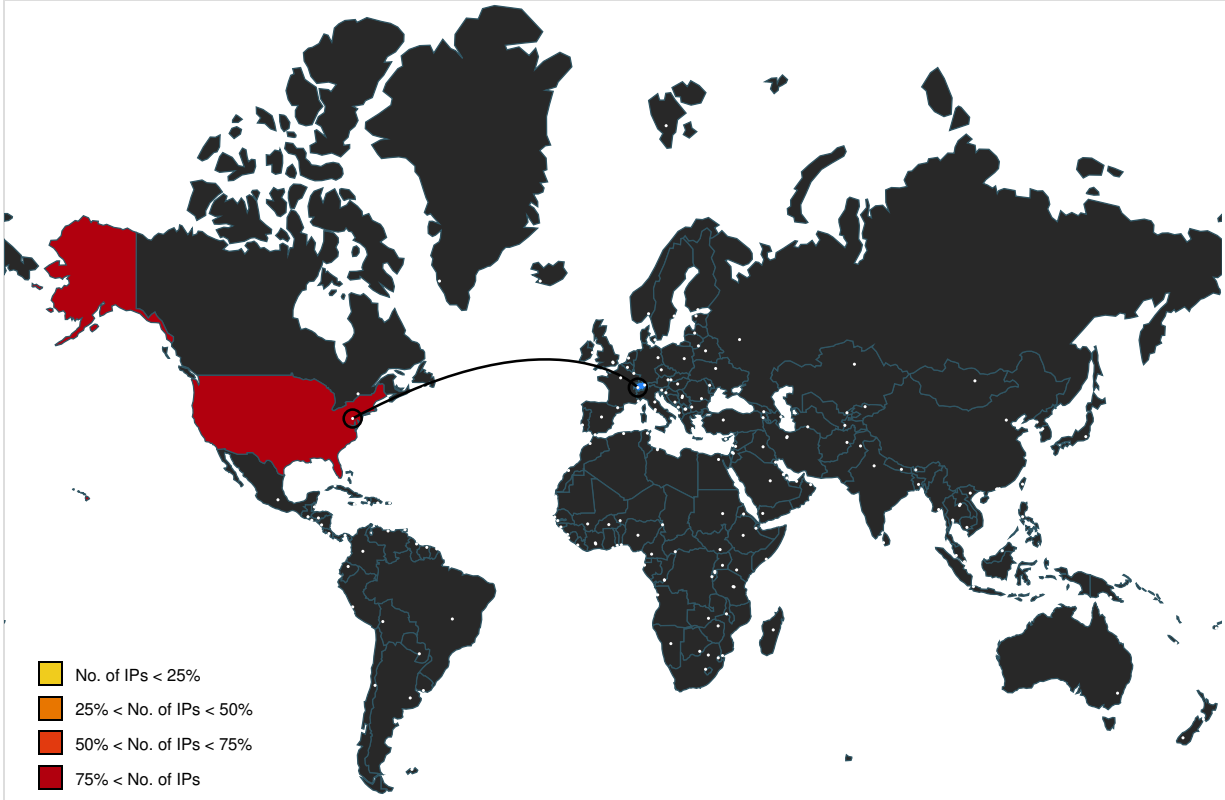
Name	Source	Malicious	Antivirus Detection	Reputation
http://144.208.127.230/Y	app.exe, 00000003.00000002.3296988780.00000000005518000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://javadl.oracle.com/webapps/download/AutoDL?BundleId=245029_d3c52aa6bfa54d3ca74e617f18309292K	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://secure.eicar.org/eicar.com.txtD	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://stubdownloader.services.mozilla.com/?attribution_code=c291cmNlPXd3dy5nb29nbGUuY29tJm1lZGl1bT	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://account.live.com/Abuse?mkt=EN-US&uiflavor=web&client_id=1E000040382627&id=293577&lmif=40&abr	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://lh5.googleusercontent.com/p/AF1QipPFr704HJkdqZ5xefxGs53Btx8SeAbaCnWxa6-y=w92-h92-n-k-no	app.exe, 00000003.00000003.3242282826.000000055C6000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3242197510.00000000058C6000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3246273895.00000000058E5000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3245462405.00000000058E5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230/U	app.exe, 00000003.00000002.3296988780.00000000005518000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ocsp.quovadisoffshore.com0	app.exe, 00000003.00000003.3093301962.0000000551F000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000002.3296988780.0000000005518000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://setup.office.com/?ms.officeurl=setup	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230:80/	app.exe, 00000003.00000003.3114168289.00000000005584000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://recoveringlib.blogspot.com	app.exe, 00000003.00000003.3245462405.000000058E5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230:80/-35b871f0a661	app.exe, 00000003.00000003.3105612570.00000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3107523130.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3101845651.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3111746106.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3103619876.0000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3109755043.0000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3116136458.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3114168289.0000000005584000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	app.exe, 00000003.00000003.3188734917.000000058E3000.00000004.00000020.00020000.00000000.sdmp, Web Data.3.dr	false		high
http://https://aka.office.com/office/url/setupMicrosoft	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://setup.office.com/EnterPin?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8Microsoft	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230:80/L	app.exe, 00000003.00000003.3130432829.00000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3132299964.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3132482295.000000000558B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.eicar.org/eicar.com	app.exe, 00000003.00000003.3182148991.00000000005603000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3178386939.00000000055E3000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3182859527.00000000005603000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://aka.office.com/office/url/setup	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://setup.office.com/SignIn?ru=https%3A%2F%2Fsetup.office.com%2F%3Fms.officeurl%3DsetupSign	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.autoitscript.com/cgi-bin/getfile.pl?autoit3/autoit-v3-setup.exe	app.exe, 00000003.00000003.3182859527.000000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230/7	app.exe, 00000003.00000002.3296988780.000000005518000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/search?q=autoit	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	Web Data.3.dr	false		high
http://https://setup.office.com/?ms.officeurl=setupMicrosoft	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://POSTHTTP/1.1Content-Type:	app.exe, 00000003.00000002.3295913444.000000002530000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://144.208.127.230/e&	app.exe, 00000003.00000002.3296988780.000000005518000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://secure.eicar.org/eicar.com.txt/	app.exe, 00000003.00000003.3182148991.00000000005603000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3178386939.00000000055E3000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3182859527.00000000005603000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/search?q=eicar	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://secure.eicar.org/eicar.com/	app.exe, 00000003.00000003.3182148991.00000000005603000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3178386939.00000000055E3000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3182859527.00000000005603000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://login.windows.net/consumers/oauth2/v2.0/authorize?client_id=77f68844-337b-4044-a0d4-153795cf	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.office.com/setup	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://setup.office.com/SignIn?ru=https%3A%2F%2Fsetup.office.com%2F%3Fms.officeurl%3Dsetup2V	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/favicon.ico	app.exe, 00000003.00000003.3183161453.000000000058E8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://alldrivers4devices.net	app.exe, 00000003.00000003.3245462405.000000000058E5000.00000004.00000020.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://login.microsoftonline.com/consumers/oauth2/v2.0/authorize?client_id=77f68844-337b-4044-a0d4-	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://office.com/setupMicrosoft	app.exe, 00000003.00000003.3182859527.000000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_flashaert	app.exe, 00000003.00000003.3177221257.000000000055AC000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	app.exe, 00000003.00000003.3183161453.00000000058E8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.eicar.org/download-anti-malware-testfile/Download	app.exe, 00000003.00000003.3182148991.00000000005603000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3178386939.00000000055E3000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3182859527.0000000005603000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://setup.office.com/Home/Provision?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8.	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.office.com/setupMicrosoft	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://setup.office.com/Home/Provision?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8Continue/	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230:80/o	app.exe, 00000003.00000003.3130432829.00000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3132299964.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3128278501.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3132482295.000000000558B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://setup.office.com/SignIn?ctid=34c190b7-c610-402a-b0d1-920cecdfcf12&redirectUri=https%3A%2F%2F	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.autoitscript.com/site/autoit/downloads/AutoIt	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230/~	app.exe, 00000003.00000003.3112020011.00000000956000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3123955917.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3121520475.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3116384116.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3126108218.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3118889457.000000000095B000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3114263668.0000000000956000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://144.208.127.230:80/T	app.exe, 00000003.00000003.3105612570.00000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3107523130.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3111746106.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3109755043.0000000005584000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3116136458.0000000005586000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3114168289.0000000005584000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.quovadis.bm0	app.exe, 00000003.00000003.3093301962.00000000551F000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000002.3296988780.0000000005518000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://144.208.127.230:80/-35b871f0a661ozi	app.exe, 00000003.00000003.3177623712.0000000090A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://144.208.127.230:80/R	app.exe, 00000003.00000003.3177623712.0000000090A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.autoitscript.com/files/autoit3/autoit-v3-setup.exeQ	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.eicar.org/https://eicar.org/https://www.eicar.org/download-anti-malware-testfile/https:/	app.exe, 00000003.00000003.3182859527.000000055E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://setup.office.com/Home/Provision?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8Continue	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	app.exe, 00000003.00000003.3183161453.000000058E8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://setup.office.com/home/ProvisionLoading?ctid=7cf86fed-a1e2-4492-bd27-ed1c1d636ca8Microsoft	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://144.208.127.230U	app.exe, 00000003.00000002.3294569055.000000008CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://secure.eicar.org/eicar.com.txt	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3182148991.0000000005603000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3178386939.00000000055E3000.00000004.00000020.00020000.00000000.sdmp, app.exe, 00000003.00000003.3182859527.0000000005603000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.autoitscript.com/site/autoit/downloads/7	app.exe, 00000003.00000003.3182859527.000000055F6000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.208.127.230	unknown	United States		395092	SHOCK-1US	true
172.67.74.152	api.ipify.org	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline

Analysis ID:	1436386
Start date and time:	2024-05-05 00:21:26 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected VM Detection
Number of analysed new started processes analysed:	8
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:	app.exe
Detection:	MAL
Classification:	mal100.spyw.evad.winEXE@10/6@1/2
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 • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- HTTP raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:24:47	API Interceptor	49x Sleep call for process: app.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe

Process:	C:\Users\user\Desktop\app.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1290240
Entropy (8bit):	7.441704402192102
Encrypted:	false
SSDEEP:	24576:CIFxe+AY3rqYsavMOQdbac5IQH97wiI3dzAr09UDZ5YUD8:1xeSNR0vbac5/d8P3diDZ6q
MD5:	75B9EF9142A78671D449C8D22AB6BE14
SHA1:	0461F1C46644ACDE8020BB59B53B1E34B65977CA
SHA-256:	E9BC44CF548A70E7285499209973FAF44B7374DECE1413DFCDC03BF25A6C599C
SHA-512:	14EF889F580C02E319B6D9D899DDBD1BD523C1D8B493EAB8B98DA6D3D276D76EFB9B5694759DF7D68BB9D002A8ACE8FC82D22121A7B4EA236D5F9CEF38CC 09C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 11% • Antivirus: Virustotal, Detection: 11%, Browse
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....P(..>{..>{..>{?.c{..>{v..{..>{...{..>{f."{..>{e."{..>{F.'{..>{..?{..>{F.~{..> {F."{&.>{...{..>{..5{..>{..^{..>{F.#{.>{F.{{..>{F..{..>{Rich..>{.....PE..L.....P.....]..... .....@..... .....$..... .....text...2..... ....rdata...&.....0.....@..@.data..... ...@... .....@....rsrc.....`... .....@..@)m&.....P.....P...`.....@.....

C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\app.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\Cookies

Process:	C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000, file counter 10, database pages 7, 1st free page 5, free pages 2, cookie 0x9, schema 4, UTF-8, version-valid-for 10

Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.5161495002712742
Encrypted:	false
SSDEEP:	96:s3n5HGsht8kAM0hsYfxqYgXZBqIcsrl3tuY2sWsqF:c5mF5wnpx9uYSF
MD5:	16A6EDF5F48F2A7B20B3B8825384B05C
SHA1:	A59542299A41166F515B18AB8CBC3D72517ED207
SHA-256:	3E1A2BB358B396C201A6058EC8A05E25B167255EB3DAEEB1130331A298CC6F93
SHA-512:	7C4C9D69B05EA5B120C0DB6DF7D0C4487387659AF6D17C387503CA360EF8430F676B0964B6BC3C368BA4DC8D0E648B2750C26970D833788982BBF5BC04AC63 D
Malicious:	false
Preview:	SQLite format 3.....@ .....S`..=.....g..... ....

C:\Users\user\AppData\Local\Temp\History

Process:	C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000, file counter 4, database pages 35, cookie 0x1e, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	163840
Entropy (8bit):	0.44975538801868414
Encrypted:	false
SSDEEP:	96:Ou1HAU+bDoYysX0uhnyZtha58VjN9DLjGQLBE3u:Ou1X+bDo3irhnyBi8Vj3XBBE3u
MD5:	89E4498D0328AFC71113CC75EBE7D770
SHA1:	120CF58C897FF1025F8B4F854A21821D948F74BC
SHA-256:	F50B271AFE0D4950FAE539E4A04C3D07849F0CE2250E73B352CDB3D981095B40
SHA-512:	7914EDF9352FBB1ABB6A0B89A4F47F09DE5672DEB6B4BE9EBEA833C8D1ED3EFD5AD16A612DF3DF65C878EB577FD0B697BC44C3E52D9BBFB82A81C1C90362 1989
Malicious:	false
Preview:	SQLite format 3.....@ .....#.....S`..... ....

C:\Users\user\AppData\Local\Temp\Login Data

Process:	C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000, page size 2048, file counter 3, database pages 27, 1st free page 7, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	57344
Entropy (8bit):	0.7310370201569906
Encrypted:	false
SSDEEP:	96:qsvKLyeymO9K3PlGNxotxPUCbn8MouON3n:q86PlGNxss27e
MD5:	A802F475CA2D00B16F45FEA728F2247C
SHA1:	AF57C02DA108CFA0D7323252126CC87D7B608786
SHA-256:	156ADDC0B949718CF518720E5774557B134CCF769A15E0413ABC257C80E58684
SHA-512:	275704B399A1C236C730F4702B57320BD7F034DC234B7A820452F8C650334233BD6830798446664F133BA4C77AA2F91E66E901CE8A11BD8575C2CD08AB9BE98F
Malicious:	false
Preview:	SQLite format 3.....@ .....S`..... ....

C:\Users\user\AppData\Local\Temp\Web Data

Process:	C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000, page size 2048, file counter 7, database pages 59, cookie 0x52, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	122880
Entropy (8bit):	1.1414673161713362
Encrypted:	false
SSDEEP:	192:8t4nKTjebGA7j9p/XH9eQ3KvphCNKRmquPWTPVusE6:8t4n/9p/39J6hwNKRmqu+7VusE

MD5:	24937DB267D854F3EF5453E2E54EA21B
SHA1:	F519A77A669D9F706D5D537A203B7245368D40CE
SHA-256:	369B8B4465FB5FD7F12258C7DEA941F9CCA9A90C78EE195DF5E02028686869ED
SHA-512:	AED398C6781300E732105E541A6FDD762F04E0EC5A5893762BFDCBDD442348FAF9CB2711EFDC4808D4675A8E48F77BEAB3A0D6BC635B778D47B2DADC9B608A3
Malicious:	false
Preview:	SQLite format 3.....@ .....;.....R.....S`.....5.....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.441704402192102
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	app.exe
File size:	1'290'240 bytes
MD5:	75b9ef9142a78671d449c8d22ab6be14
SHA1:	0461f1c46644acde8020bb59b53b1e34b65977ca
SHA256:	e9bc44cf548a70e7285499209973faf44b7374dece1413dfcdc03bf25a6c599c
SHA512:	14ef889f580c02e319b6d9d899ddbd1bd523c1d8b493eab8b98da6d3d276d76efb9b5694759df7d68bb9d002a8ace8fc82d22121a7b4ea236d5f9cef38cc809c
SSDEEP:	24576:CIFxe+AY3rqYsavMOQdbac5IQH97wiI3dzAr09UDZ5YUD8:1xeSNR0vbac5/d8P3diDZ6q
TLSH:	8255CF05F3D2B8B1D15192772DC96161B6ED993048D83F0732D0EE5E1B3B9A6B40FE2A
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....P(..>{..>{..>{?.c{..>{v..{..>{...{..>{f."{..>{e."{..>{F.'{..>{..?{..>{F.~{..>{F."{&.>{...{..>{..5{..>{..^{..>{F.#{..>{F.{{..>

File Icon

Icon Hash:	0f4ecda7ae5d1715

Static PE Info

General

Entrypoint:	0x415dde
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x500F9507 [Wed Jul 25 06:41:11 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	26600adf486f72b556f917a64c8fd23f

Entrypoint Preview

Instruction
push 00000060h
push 0043A478h
call 00007F8C48B70DE3h
mov edi, 00000094h
mov eax, edi
call 00007F8C48B6F33Fh
mov dword ptr [ebp-18h], esp
mov esi, esp
mov dword ptr [esi], edi
push esi
call dword ptr [0042F2B4h]
mov ecx, dword ptr [esi+10h]
mov dword ptr [0044B190h], ecx
mov eax, dword ptr [esi+04h]
mov dword ptr [0044B19Ch], eax
mov edx, dword ptr [esi+08h]
mov dword ptr [0044B1A0h], edx
mov esi, dword ptr [esi+0Ch]
and esi, 00007FFFh
mov dword ptr [0044B194h], esi
cmp ecx, 02h
je 00007F8C48B6FCDEh
or esi, 00008000h
mov dword ptr [0044B194h], esi
shl eax, 08h
add eax, edx
mov dword ptr [0044B198h], eax
xor esi, esi
push esi
mov edi, dword ptr [0042F20Ch]
call edi
cmp word ptr [eax], 5A4Dh
jne 00007F8C48B6FCF1h
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
cmp dword ptr [ecx], 00004550h
jne 00007F8C48B6FCE4h
movzx eax, word ptr [ecx+18h]
cmp eax, 0000010Bh
je 00007F8C48B6FCF1h
cmp eax, 0000020Bh
je 00007F8C48B6FCD7h
mov dword ptr [ebp-1Ch], esi
jmp 00007F8C48B6FCF9h
cmp dword ptr [ecx+00000084h], 0Eh
jbe 00007F8C48B6FCC4h
xor eax, eax
cmp dword ptr [ecx+000000F8h], esi
jmp 00007F8C48B6FCE0h
cmp dword ptr [ecx+74h], 0Eh
jbe 00007F8C48B6FCB4h
xor eax, eax
cmp dword ptr [ecx+000000E8h], esi
setne al
mov dword ptr [ebp-1Ch], eax

Rich Headers

Programming Language:	• [ASM] VS2002 (.NET) build 9466 • [C] VS2002 (.NET) build 9466 • [C++] VS2003 (.NET) build 3077 • [C++] VS2002 (.NET) build 9466 • [RES] VS2002 (.NET) build 9466 • [LNK] VS2002 (.NET) build 9466

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3f924	0x118	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4d000	0x2f5f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2f000	0x594	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2db32	0x2e000	7868e2f41e5b3ab908ac5a72a66f5953	False	0.6095076851222826	data	6.670624963209676	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x2f000	0x126c6	0x13000	efd458d4cde7206fd4c5482997a30ba9	False	0.4482421875	data	5.736665908168061	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x42000	0xa9f4	0x4000	07b79e131c84ddfb0842641915843ec1	False	0.4459228515625	data	5.072911159589167	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x4d000	0x2f5f0	0x30000	2686df77c23e2ca3144ababd1a5e1501	False	0.2823994954427083	data	4.484521144858898	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
)m&	0x7d000	0xc5000	0xc5000	acab40631ef6f655b384348be6aac2b9	False	0.841724996034264	data	7.775469163423906	IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
JPG	0x4f2b0	0x2b1e6	PC bitmap, Windows 3.x format, 635 x 276 x 8, cbSize 176614, bits offset 1078	Chinese	China	0.27774128891254374
RT_CURSOR	0x7a498	0x134	Targa image data - RGB 64 x 65536 x 1 +32 "\001"	Chinese	China	0.4805194805194805
RT_CURSOR	0x7a5d0	0xb4	Targa image data - Map 32 x 65536 x 1 +16 "\001"	Chinese	China	0.7
RT_CURSOR	0x7a6b0	0x134	AmigaOS bitmap font "(", fc_YSize 4294967264, 5120 elements, 2nd "\377\360?\377\377\370\177\377\377\374\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377", 3rd	Chinese	China	0.36363636363636365
RT_CURSOR	0x7a800	0x134	Targa image data - RLE 64 x 65536 x 1 +32 "\001"	Chinese	China	0.35714285714285715
RT_CURSOR	0x7a950	0x134	data	Chinese	China	0.37337662337662336
RT_CURSOR	0x7aaa0	0x134	data	Chinese	China	0.37662337662337664

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_CURSOR	0x7abf0	0x134	Targa image data 64 x 65536 x 1 +32 "\001"	Chinese	China	0.36688311688311687
RT_CURSOR	0x7ad40	0x134	Targa image data 64 x 65536 x 1 +32 "\001"	Chinese	China	0.37662337662337664
RT_CURSOR	0x7ae90	0x134	Targa image data - Mono - RLE 64 x 65536 x 1 +32 "\001"	Chinese	China	0.36688311688311687
RT_CURSOR	0x7afe0	0x134	Targa image data - RGB - RLE 64 x 65536 x 1 +32 "\001"	Chinese	China	0.38636363636363635
RT_CURSOR	0x7b130	0x134	data	Chinese	China	0.44155844155844154
RT_CURSOR	0x7b280	0x134	data	Chinese	China	0.4155844155844156
RT_CURSOR	0x7b3d0	0x134	AmigaOS bitmap font "(", fc_YSize 4294966847, 3840 elements, 2nd "\377?\374\377\377\300\003\377\377\300\003\377\377\340\007\377\377\360\017\377\377\370\037\377\377\374?\377\377\376\177\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377", 3rd	Chinese	China	0.5422077922077922
RT_CURSOR	0x7b520	0x134	data	Chinese	China	0.2662337662337662
RT_CURSOR	0x7b670	0x134	data	Chinese	China	0.2824675324675325
RT_CURSOR	0x7b7c0	0x134	data	Chinese	China	0.3246753246753247
RT_BITMAP	0x7b9f8	0xb8	Device independent bitmap graphic, 12 x 10 x 4, image size 80	Chinese	China	0.44565217391304346
RT_BITMAP	0x7bab0	0x144	Device independent bitmap graphic, 33 x 11 x 4, image size 220	Chinese	China	0.37962962962962965
RT_ICON	0x4db70	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Chinese	China	0.6042418772563177
RT_ICON	0x4e430	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Chinese	China	0.6042418772563177
RT_DIALOG	0x4ecf0	0x23e	data	Chinese	China	0.5174216027874564
RT_DIALOG	0x4ef30	0x94	data	Chinese	China	0.6959459459459459
RT_DIALOG	0x7b910	0xe2	data	Chinese	China	0.6637168141592921
RT_STRING	0x7bbf8	0x46	data	Chinese	China	0.6857142857142857
RT_STRING	0x7bc40	0x54	data	Chinese	China	0.8571428571428571
RT_STRING	0x7bc98	0x2c	data	Chinese	China	0.5909090909090909
RT_STRING	0x7bcc8	0x74	data	Chinese	China	0.8448275862068966
RT_STRING	0x7bd40	0x1d0	data	Chinese	China	0.8060344827586207
RT_STRING	0x7c088	0x164	data	Chinese	China	0.48314606741573035
RT_STRING	0x7bf50	0x132	data	Chinese	China	0.6405228758169934
RT_STRING	0x7c570	0x50	data	Chinese	China	0.725
RT_STRING	0x7bf10	0x40	data	Chinese	China	0.65625
RT_STRING	0x7c4d8	0x6a	data	Chinese	China	0.7452830188679245
RT_STRING	0x7c1f0	0x1d6	data	Chinese	China	0.6723404255319149
RT_STRING	0x7c3c8	0x110	data	Chinese	China	0.625
RT_STRING	0x7c548	0x24	data	Chinese	China	0.4444444444444444
RT_STRING	0x7c5c0	0x30	data	Chinese	China	0.625
RT_GROUP_CURSOR	0x7a688	0x22	Lotus unknown worksheet or configuration, revision 0x2	Chinese	China	1.0294117647058822
RT_GROUP_CURSOR	0x7ae78	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7a7e8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7ad28	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7abd8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b508	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7aa88	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b118	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7a938	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7afc8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_GROUP_CURSOR	0x7b268	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b3b8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b658	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b7a8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b8f8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_ICON	0x4e418	0x14	data	Chinese	China	1.15
RT_GROUP_ICON	0x4ecd8	0x14	data	Chinese	China	1.25
RT_VERSION	0x4efc8	0x2e8	data	Chinese	China	0.5631720430107527

Imports

DLL	Import
KERNEL32.dll	LockFile, UnlockFile, SetEndOfFile, DuplicateHandle, FindClose, FindFirstFileA, GetFullPathNameA, GetCPInfo, GetOEMCP, FileTimeToSystemTime, SetErrorMode, FileTimeToLocalFileTime, GetFileAttributesA, GetFileTime, GetTickCount, HeapAlloc, HeapFree, RtlUnwind, GetStartupInfoA, GetCommandLineA, RaiseException, GetSystemTimeAsFileTime, ExitProcess, TerminateProcess, HeapReAlloc, HeapSize, FlushFileBuffers, HeapCreate, VirtualFree, VirtualAlloc, IsBadWritePtr, GetStdHandle, UnhandledExceptionFilter, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, SetUnhandledExceptionFilter, GetStringTypeA, GetStringTypeW, GetCurrentProcessId, LCMapStringA, LCMapStringW, GetTimeZoneInformation, IsBadReadPtr, IsBadCodePtr, VirtualProtect, GetSystemInfo, VirtualQuery, SetStdHandle, SetEnvironmentVariableA, SetFilePointer, GlobalFlags, WritePrivateProfileStringA, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, TlsAlloc, InitializeCriticalSection, TlsGetValue, EnterCriticalSection, GlobalHandle, GlobalReAlloc, LeaveCriticalSection, LocalAlloc, GlobalGetAtomNameA, GlobalFindAtomA, lstrcatA, lstrcmpW, GlobalAddAtomA, GetCurrentThread, GetCurrentThreadId, GlobalDeleteAtom, lstrcmpA, ConvertDefaultLocale, EnumResourceLanguagesA, lstrcpyA, SetLastError, GlobalFree, MulDiv, GlobalAlloc, GlobalLock, GlobalUnlock, GetModuleHandleA, GetProcAddress, FormatMessageA, LocalFree, CopyFileA, GetCurrentDirectoryA, FreeResource, OpenFile, GetCurrentProcess, SetPriorityClass, lstrcpynA, DeviceIoControl, ReadFile, GetFileSize, GetLastError, QueryPerformanceCounter, QueryPerformanceFrequency, GetSystemDirectoryA, CreateFileA, WriteFile, CloseHandle, DeleteFileA, GetModuleFileNameA, LoadLibraryA, FreeLibrary, GetVolumeInformationA, OutputDebugStringA, DebugBreak, InterlockedIncrement, InterlockedDecrement, FindResourceA, LoadResource, LockResource, SizeofResource, lstrlenA, lstrcmpiA, CompareStringW, lstrlenW, CompareStringA, GetVersion, WideCharToMultiByte, MultiByteToWideChar, GetVersionExA, GetThreadLocale, GetLocaleInfoA, GetACP, HeapDestroy, InterlockedExchange
USER32.dll	InvalidateRgn, SetCapture, ReleaseCapture, GetNextDlgGroupItem, MessageBeep, RegisterClipboardFormatA, PostThreadMessageA, GetForegroundWindow, GetTopWindow, UnhookWindowsHookEx, GetMessagePos, MapWindowPoints, SetForegroundWindow, UpdateWindow, GetMenu, GetSysColor, AdjustWindowRectEx, EqualRect, GetClassInfoA, RegisterClassA, UnregisterClassA, GetDlgCtrlID, DefWindowProcA, CallWindowProcA, SetWindowLongA, OffsetRect, IntersectRect, SystemParametersInfoA, GetWindowPlacement, GetWindowRect, CopyRect, PtInRect, GetWindow, SetWindowContextHelpId, MapDialogRect, SetWindowPos, GetDesktopWindow, SetActiveWindow, EndPaint, DestroyWindow, IsWindow, InvalidateRect, GetNextDlgTabItem, EndDialog, SetMenuItemBitmaps, GetFocus, ModifyMenuA, EnableMenuItem, CheckMenuItem, GetMenuCheckMarkDimensions, LoadBitmapA, SetWindowsHookExA, CallNextHookEx, GetMessageA, TranslateMessage, DispatchMessageA, GetActiveWindow, IsWindowVisible, GetKeyState, PeekMessageA, GetCursorPos, ValidateRect, GetParent, GetWindowLongA, GetLastActivePopup, IsWindowEnabled, SetCursor, PostMessageA, PostQuitMessage, wsprintfA, GetMenuState, GetMenuItemID, GetMenuItemCount, CharLowerA, CharUpperA, BeginPaint, GetWindowDC, ReleaseDC, GetDC, ClientToScreen, GetSubMenu, MessageBoxA, CharNextA, wvsprintfA, GetSystemMetrics, LoadIconA, EnableWindow, GetClientRect, IsIconic, GetSystemMenu, SendMessageA, AppendMenuA, CopyAcceleratorTableA, SetRect, IsRectEmpty, DrawIcon, LoadCursorA, GetDlgItem, GetSysColorBrush, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, DestroyMenu, ShowWindow, MoveWindow, SetWindowTextA, IsDialogMessageA, RegisterWindowMessageA, WinHelpA, GetCapture, CreateWindowExA, GetClassLongA, GetClassInfoExA, GetClassNameA, SetPropA, GetPropA, RemovePropA, SendDlgItemMessageA, SetFocus, IsChild, GetWindowTextLengthA, CreateDialogIndirectParamA, GetWindowTextA, GetMessageTime
GDI32.dll	SetMapMode, DeleteObject, GetViewportExtEx, GetWindowExtEx, PtVisible, RectVisible, TextOutA, Escape, SelectObject, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowExtEx, ScaleWindowExtEx, ExtSelectClipRgn, DeleteDC, GetStockObject, GetBkColor, GetTextColor, CreateRectRgnIndirect, GetRgnBox, GetMapMode, RestoreDC, SaveDC, ExtTextOutA, GetObjectA, SetBkColor, SetTextColor, GetClipBox, CreateBitmap, GetDeviceCaps
comdlg32.dll	GetFileTitleA
WINSPOOL.DRV	ClosePrinter, DocumentPropertiesA, OpenPrinterA
ADVAPI32.dll	RegEnumKeyA, RegSetValueExA, RegCreateKeyExA, RegQueryValueA, RegCloseKey, RegDeleteKeyA, RegOpenKeyExA, RegQueryValueExA, RegOpenKeyA
COMCTL32.dll	
SHLWAPI.dll	PathFindExtensionA, PathFindFileNameA, PathStripToRootA, PathIsUNCA
oledlg.dll	
ole32.dll	CreateILockBytesOnHGlobal, StgCreateDocfileOnILockBytes, StgOpenStorageOnILockBytes, CoGetClassObject, CLSIDFromString, CLSIDFromProgID, CoTaskMemAlloc, OleInitialize, OleUninitialize, CoTaskMemFree, CoCreateInstance, CoSetProxyBlanket, CoInitialize, CoUninitialize, CoRevokeClassObject, OleIsCurrentClipboard, OleFlushClipboard, CoFreeUnusedLibraries, CoRegisterMessageFilter

DLL	Import
OLEAUT32.dll	VariantInit, SysAllocStringLen, VariantClear, VariantChangeType, SysStringLen, SysAllocStringByteLen, OleCreateFontIndirect, SystemTimeToVariantTime, SafeArrayDestroy, VariantCopy, SysAllocString, SysFreeString
iphlpapi.dll	GetAdaptersInfo
OLEACC.dll	LresultFromObject, CreateStdAccessibleObject

Possible Origin

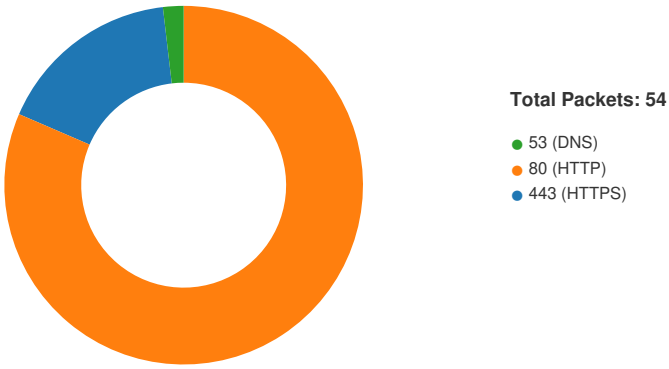
Language of compilation system	Country where language is spoken	Map
Chinese	China	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/05/24-00:24:50.450010	TCP	2051909	ET TROJAN Win32/FireStealer Related Server Response	80	49789	144.208.127.230	192.168.11.20

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2024 00:24:47.904021978 CEST	49788	443	192.168.11.20	172.67.74.152
May 5, 2024 00:24:47.904131889 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:47.904324055 CEST	49788	443	192.168.11.20	172.67.74.152
May 5, 2024 00:24:47.906574965 CEST	49788	443	192.168.11.20	172.67.74.152
May 5, 2024 00:24:47.906646967 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:48.118782997 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:48.119072914 CEST	49788	443	192.168.11.20	172.67.74.152
May 5, 2024 00:24:48.120646954 CEST	49788	443	192.168.11.20	172.67.74.152
May 5, 2024 00:24:48.120656013 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:48.120851994 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:48.152481079 CEST	49788	443	192.168.11.20	172.67.74.152
May 5, 2024 00:24:48.196245909 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:48.459268093 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:48.459501028 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:48.459741116 CEST	49788	443	192.168.11.20	172.67.74.152

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2024 00:24:48.460419893 CEST	49788	443	192.168.11.20	172.67.74.152
May 5, 2024 00:24:48.460481882 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:48.460628033 CEST	49788	443	192.168.11.20	172.67.74.152
May 5, 2024 00:24:48.460686922 CEST	443	49788	172.67.74.152	192.168.11.20
May 5, 2024 00:24:50.109848976 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.215768099 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.216002941 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.216104031 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.216152906 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.320934057 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.320976019 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.450010061 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.450088978 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.450146914 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.450248957 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.450306892 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.450361967 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.450412035 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.450428009 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.450566053 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.502199888 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.615658998 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.615658998 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.720161915 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.720295906 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.746968031 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.784807920 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.784807920 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.889528036 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.913850069 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:50.955168009 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.960611105 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:50.960611105 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.064706087 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.089246988 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.138124943 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.138124943 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.242675066 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.273591042 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.314446926 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.344860077 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.344860077 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.449444056 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.474955082 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.517565966 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.581295013 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.581295013 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.685782909 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.720448017 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.754550934 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.754550934 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.859148026 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.886817932 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:51.939325094 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.993621111 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:51.993621111 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.098404884 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:52.130491972 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:52.173640966 CEST	49789	80	192.168.11.20	144.208.127.230

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2024 00:24:52.209886074 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.209886074 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.314246893 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:52.350059032 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:52.392358065 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.440471888 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.440471888 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.545001030 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:52.572115898 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:52.626641989 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.687793016 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.687793016 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.792337894 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:52.820131063 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:52.861021996 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.944320917 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:52.944320917 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:53.049401999 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:53.075536013 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:53.126554966 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:53.186395884 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:53.186395884 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:53.291074038 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:53.317679882 CEST	80	49789	144.208.127.230	192.168.11.20
May 5, 2024 00:24:53.360930920 CEST	49789	80	192.168.11.20	144.208.127.230
May 5, 2024 00:24:53.392790079 CEST	49789	80	192.168.11.20	144.208.127.230

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2024 00:24:47.800074100 CEST	54765	53	192.168.11.20	1.1.1.1
May 5, 2024 00:24:47.899873972 CEST	53	54765	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 5, 2024 00:24:47.800074100 CEST	192.168.11.20	1.1.1.1	0x3613	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false

DNS Answers

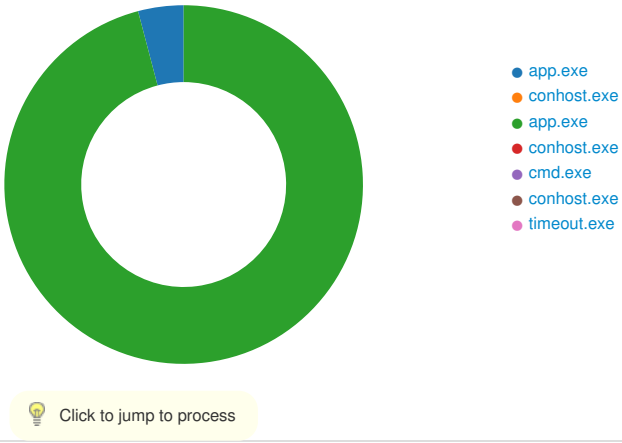
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 5, 2024 00:24:47.899873972 CEST	1.1.1.1	192.168.11.20	0x3613	No error (0)	api.ipify.org		172.67.74.152	A (IP address)	IN (0x0001)	false
May 5, 2024 00:24:47.899873972 CEST	1.1.1.1	192.168.11.20	0x3613	No error (0)	api.ipify.org		104.26.13.205	A (IP address)	IN (0x0001)	false
May 5, 2024 00:24:47.899873972 CEST	1.1.1.1	192.168.11.20	0x3613	No error (0)	api.ipify.org		104.26.12.205	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org
- 144.208.127.230

Statistics

Behavior



System Behavior

Analysis Process: app.exe PID: **7652**, Parent PID: **5364**

General

Target ID:	0
Start time:	00:23:27
Start date:	05/05/2024
Path:	C:\Users\user\Desktop\app.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\app.exe"
Imagebase:	0x400000
File size:	1'290'240 bytes
MD5 hash:	75B9EF9142A78671D449C8D22AB6BE14
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: **7972**, Parent PID: **7652**

General

Target ID:	1
Start time:	00:23:27
Start date:	05/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7cb400000
File size:	875'008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
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: app.exe PID: 7132, Parent PID: 7652

General

Target ID:	3
Start time:	00:24:07
Start date:	05/05/2024
Path:	C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe"
Imagebase:	0x400000
File size:	1'290'240 bytes
MD5 hash:	75B9EF9142A78671D449C8D22AB6BE14
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 11%, ReversingLabs • Detection: 11%, Virustotal, Browse
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Login Data	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	255E417	CopyFileExW
C:\Users\user\AppData\Local\Temp\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	255E417	CopyFileExW
C:\Users\user\AppData\Local\Temp\History	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	255E417	CopyFileExW
C:\Users\user\AppData\Local\Temp\Web Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	255E417	CopyFileExW
C:\Users\user\AppData\Local\Temp\Login Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	255E417	CopyFileExW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	255E417	CopyFileExW
C:\Users\user\AppData\Local\Temp\History	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	255E417	CopyFileExW
C:\Users\user\AppData\Local\Temp\Web Data	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	255E417	CopyFileExW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Login Data	success or wait	2	255180E	DeleteFileW
C:\Users\user\AppData\Local\Temp\Cookies	success or wait	1	255180E	DeleteFileW
C:\Users\user\AppData\Local\Temp\History	success or wait	1	255180E	DeleteFileW
C:\Users\user\AppData\Local\Temp\Web Data	success or wait	1	255180E	DeleteFileW
C:\Users\user\AppData\Local\Temp\Cookies	success or wait	1	255180E	DeleteFileW
C:\Users\user\AppData\Local\Temp\History	success or wait	1	255180E	DeleteFileW
C:\Users\user\AppData\Local\Temp\Web Data	success or wait	1	255180E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	5			object type mismatch	1	25903E5	NtWriteFile
C:\Users\user\AppData\Local\Temp\Login Data	0	45056	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 1b 00 00 00 07 00 00 00 02 00 00 00 13 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 53 60 05 00 00 00 02 07 fd 00 00 00 00 1b 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .S`	success or wait	1	255E417	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cookies	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 0a 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 09 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 2e 53 60 0d 0c 3d 00 04 09 11 00 0f 67 0f fd 09 11 0c 0e 0c 0e 0c 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .S`=g	success or wait	1	255E417	CopyFileExW
C:\Users\user\AppData\Local\Temp\History	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 04 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 53 60 05 00 00 00 01 0f fd 00 00 00 00 1c 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ #.S`	success or wait	2	255E417	CopyFileExW
unknown	unknown	4			object type mismatch	1	25903E5	NtWriteFile
unknown	unknown	10			object type mismatch	4	25903E5	NtWriteFile
unknown	unknown	2			object type mismatch	4	25903E5	NtWriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Web Data	0	92160	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 07 00 00 00 3b 00 00 00 00 00 00 00 00 00 00 00 52 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 53 60 05 00 00 00 06 07 fd 00 00 00 00 35 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ;R.S`5	success or wait	1	255E417	CopyFileExW
unknown	unknown	4			object type mismatch	1	25903E5	NtWriteFile
C:\Users\user\AppData\Local\Temp\Login Data	0	57344	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 1b 00 00 00 07 00 00 00 02 00 00 00 13 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 53 60 05 00 00 00 02 07 fd 00 00 00 00 1b 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .S`	success or wait	1	255E417	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cookies	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 0a 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 09 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 2e 53 60 0d 0c 3d 00 04 09 11 00 0f 67 0f fd 09 11 0c 0e 0c 0e 0c 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .S`=g	success or wait	1	255E417	CopyFileExW
C:\Users\user\AppData\Local\Temp\History	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 04 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 53 60 05 00 00 00 01 0f fd 00 00 00 00 1c 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ #.S`	success or wait	2	255E417	CopyFileExW
unknown	unknown	4			object type mismatch	1	25903E5	NtWriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Web Data	0	122880	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 07 00 00 00 3b 00 00 00 00 00 00 00 00 00 00 00 52 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 53 60 05 00 00 00 06 07 fd 00 00 00 00 35 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ;R.S`5	success or wait	1	255E417	CopyFileExW
unknown	unknown	4			object type mismatch	1	25903E5	NtWriteFile
unknown	unknown	13			object type mismatch	1	25903E5	NtWriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GQSZOBXUFX\GQSZOBXUFX.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\GQSZOBXUFX\GQSZOBXUFX.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\GQSZOBXUFX\MLMJAYLPER.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\GQSZOBXUFX\MLMJAYLPER.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\GQSZOBXUFX\RMDIWSRLPR.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\GQSZOBXUFX\RMDIWSRLPR.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\GQSZOBXUFX.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\GQSZOBXUFX.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER\MLMJAYLPER.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER\MLMJAYLPER.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER\UQMPCTZARJ.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER\UQMPCTZARJ.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER\YCGNAHEPCK.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER\YCGNAHEPCK.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\MLMJAYLPER.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\RMDIWSRLPR.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\RMDIWSRLPR.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\UQMPCTZARJ.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\UQMPCTZARJ.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Desktop\YCGNAHEPCK.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Desktop\YCGNAHEPCK.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\GQSZOBXUFX.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\GQSZOBXUFX.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\MLMJAYLPER.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\MLMJAYLPER.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\RMDIWSRLPR.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\RMDIWSRLPR.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX.docx	0	1026	success or wait	1	2597809	NtReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\GQSZOBXUFX.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER\MLMJAYLPER.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER\MLMJAYLPER.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER\UQMPCTZARJ.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER\UQMPCTZARJ.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER\YCGNAHEPCK.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER\YCGNAHEPCK.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\RMDIWSRLPR.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\RMDIWSRLPR.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\UQMPCTZARJ.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\UQMPCTZARJ.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\YCGNAHEPCK.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\YCGNAHEPCK.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Downloads\eicar.com.txt	0	68	success or wait	1	2597809	NtReadFile
C:\Users\user\Downloads\eicar.com.txt	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Downloads\GQSZOBXUFX.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Downloads\GQSZOBXUFX.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Downloads\MLMJAYLPER.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Downloads\MLMJAYLPER.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Downloads\MLMJAYLPER.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Downloads\MLMJAYLPER.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Downloads\RMDIWSRLPR.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Downloads\RMDIWSRLPR.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Downloads\UQMPCTZARJ.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Downloads\UQMPCTZARJ.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Downloads\YCGNAHEPCK.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Downloads\YCGNAHEPCK.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\GQSZOBXUFX.docx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\GQSZOBXUFX.docx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\MLMJAYLPER.xlsx	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\MLMJAYLPER.xlsx	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\RMDIWSRLPR.pdf	0	1026	success or wait	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX\RMDIWSRLPR.pdf	0	32	end of file	1	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX.docx	0	1026	success or wait	2	2597809	NtReadFile
C:\Users\user\Documents\GQSZOBXUFX.docx	0	32	end of file	2	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER\MLMJAYLPER.docx	0	1026	success or wait	3	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER\MLMJAYLPER.docx	0	32	end of file	3	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER.docx	0	1026	success or wait	4	2597809	NtReadFile
C:\Users\user\Documents\MLMJAYLPER.docx	0	32	end of file	4	2597809	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	185099	success or wait	1	255F648	ReadFile
C:\Users\user\AppData\Local\Temp\Login Data	0	45056	success or wait	1	255F706	ReadFile
C:\Users\user\AppData\Local\Temp\Cookies	0	98304	success or wait	1	2560AAC	ReadFile
C:\Users\user\AppData\Local\Temp\History	0	196608	success or wait	1	2560702	ReadFile
C:\Users\user\AppData\Local\Temp\Web Data	0	92160	success or wait	1	2560767	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	15119	success or wait	1	255F648	ReadFile
C:\Users\user\AppData\Local\Temp\Login Data	0	57344	success or wait	1	255F706	ReadFile
C:\Users\user\AppData\Local\Temp\Cookies	0	28672	success or wait	1	2560AAC	ReadFile
C:\Users\user\AppData\Local\Temp\History	0	163840	success or wait	1	2560702	ReadFile
C:\Users\user\AppData\Local\Temp\Web Data	0	122880	success or wait	1	2560767	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	0	116766	success or wait	1	2597809	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	0	32	end of file	1	2597809	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7152**, Parent PID: **7132**

General

Target ID:	4
Start time:	00:24:07
Start date:	05/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7cb400000
File size:	875'008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
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: cmd.exe PID: **1808**, Parent PID: **7132**

General

Target ID:	5
Start time:	00:25:08
Start date:	05/05/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c timeout /t 5 & del /f /q C:\Users\user\AppData\Local\Temp\7041956494665639546\app.exe && exit
Imagebase:	0x90000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5108**, Parent PID: **1808**

General

Target ID:	6
Start time:	00:25:08

Start date:	05/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7cb400000
File size:	875'008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
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: timeout.exe PID: 1172, Parent PID: 1808

General

Target ID:	7
Start time:	00:25:08
Start date:	05/05/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 5
Imagebase:	0xd40000
File size:	25'088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly