ID: 755179
Sample Name: Swift Mesaj#U0131#09971.exe
Cookbook: default.jbs
Time: 12:43:49
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

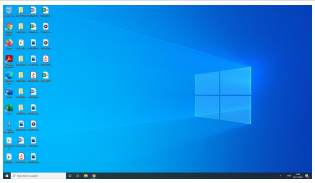
Windows Analysis Report

Swift Mesaj#U0131#09971.exe

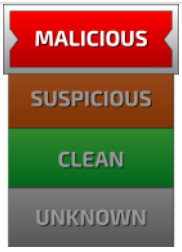
Overview

General Information

Sample Name:	Swift Mesaj#U0131#09971.exe
Analysis ID:	755179
MD5:	310df09294b852..
SHA1:	9b69175fcbcc71…
SHA256:	d27bf1156e1a46..
Infos:	



Detection



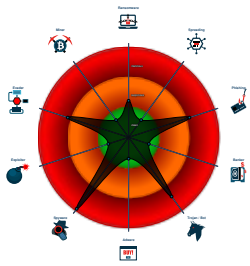
Azorult, GuLoader

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

Signatures

- Yara detected Azorult
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to steal Crypto Currency Walle…
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Self deletion via cmd or bat file
- Tries to harvest and steal ftp login c…
- Tries to harvest and steal Bitcoin W…

Classification



Process Tree

- **System is w10x64native**
- Swift Mesaj#U0131#09971.exe (PID: 7596 cmdline: C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe MD5: 310DF09294B852BAB67E158D95788150)
  - Swift Mesaj#U0131#09971.exe (PID: 3172 cmdline: C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe MD5: 310DF09294B852BAB67E158D95788150)
    - cmd.exe (PID: 6040 cmdline: C:\Windows\system32\cmd.exe" /c C:\Windows\system32\timeout.exe 3 & del "Swift Mesaj#U0131#09971.exe MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - conhost.exe (PID: 4920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - timeout.exe (PID: 8964 cmdline: C:\Windows\system32\timeout.exe 3 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.8040635695.000000001D9B8000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Azorult_1	Yara detected Azorult	Joe Security	
00000001.00000002.7935875493.0000000002AF0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000004.00000000.7688018397.0000000001660000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000002.7934819719.00000000005AB000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	
00000004.00000002.8078319161.000000001D460000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Azorult_1	Yara detected Azorult	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.Swift Mesaj#U0131#09971.exe.1e2ce63c.3.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
4.2.Swift Mesaj#U0131#09971.exe.1e2ce63c.3.raw.unpack	OlympicDestroyer_1	OlympicDestroyer Payload	kevoreilly	• 0x37c6f7:$string1: SELECT origin_url, username_value, password_value FROM logins • 0x37d628:$string1: SELECT origin_url, username_value, password_value FROM logins • 0x1eceb2:$string2: API call with %s database connection pointer • 0x1edae6:$string3: os_win.c:%d: (%lu) %s(%s) - %s
4.2.Swift Mesaj#U0131#09971.exe.1e2c94d2.5.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
4.2.Swift Mesaj#U0131#09971.exe.1e2c94d2.5.raw.unpack	OlympicDestroyer_1	OlympicDestroyer Payload	kevoreilly	• 0x381861:$string1: SELECT origin_url, username_value, password_value FROM logins • 0x382792:$string1: SELECT origin_url, username_value, password_value FROM logins • 0x1f201c:$string2: API call with %s database connection pointer • 0x1f2c50:$string3: os_win.c:%d: (%lu) %s(%s) - %s
4.2.Swift Mesaj#U0131#09971.exe.1e2c38e3.4.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN AZORult v3.3 Server Response M2 - Source IP: 172.67.203.65 - Destination IP: 192.168.11.20

Timestamp:	172.67.203.65192.168.11.2080498362029137 11/28/22-12:46:57.711672
SID:	2029137
Source Port:	80
Destination Port:	49836
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/AZORult V3.3 Client Checkin M15 - Source IP: 192.168.11.20 - Destination IP: 172.67.203.65

Timestamp:	192.168.11.20172.67.203.6549836802029468 11/28/22-12:46:56.779159
SID:	2029468
Source Port:	49836
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd or bat file

Malware Analysis System Evasion

Tries to detect Any.run

Stealing of Sensitive Information

Yara detected Azorult

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

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal Bitcoin Wallet information

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

Tries to steal Instant Messenger accounts or passwords

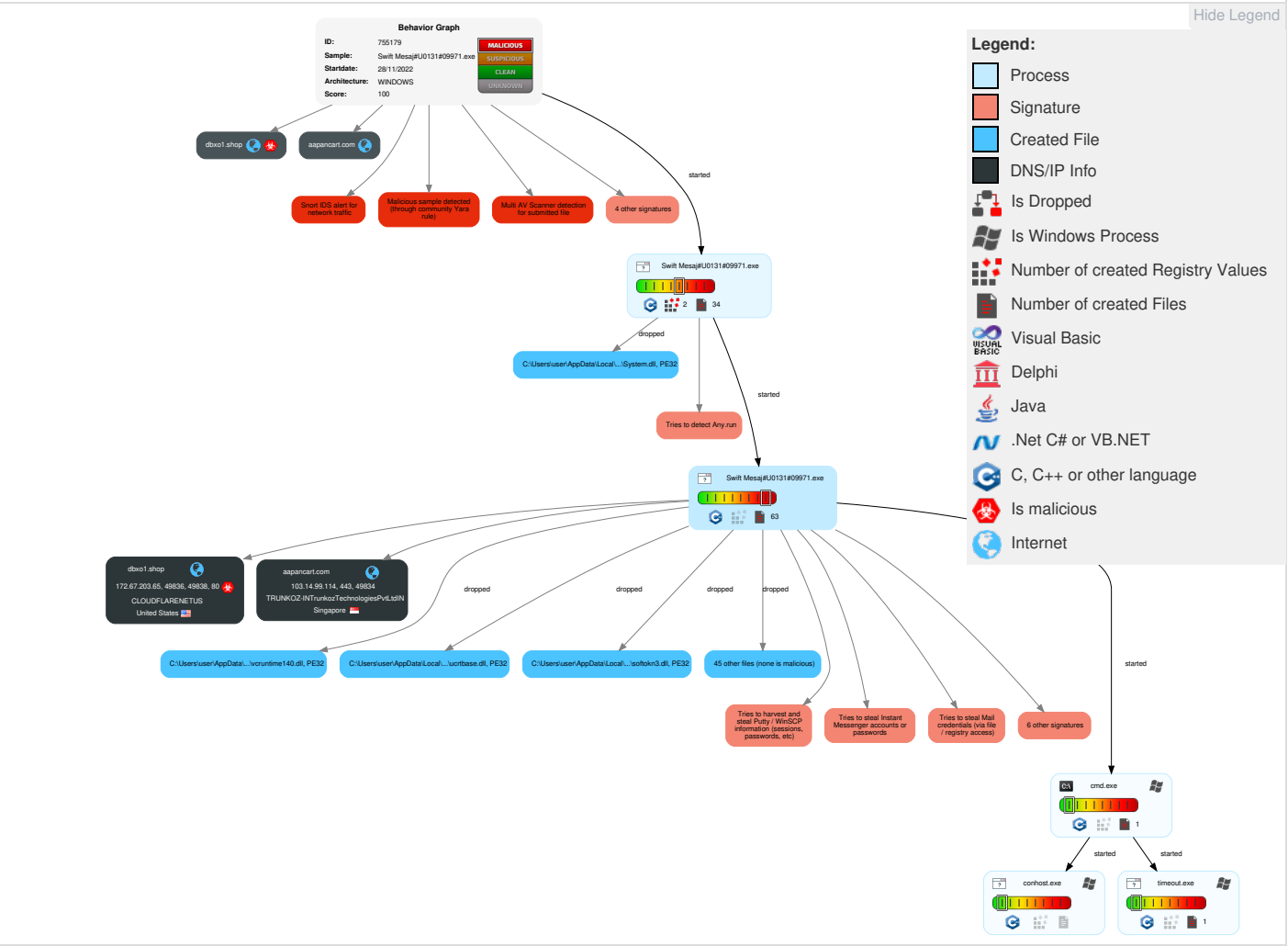
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Obfuscated Files or Information	2 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 Windows Service	1 Access Token Manipulation	1 Timestomp	2 Credentials in Registry	2 6 System Information Discovery	Remote Desktop Protocol	4 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 Registry Run Keys / Startup Folder	1 Windows Service	1 DLL Side-Loading	1 Credentials In Files	1 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 Process Injection	1 File Deletion	NTDS	1 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Registry Run Keys / Startup Folder	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

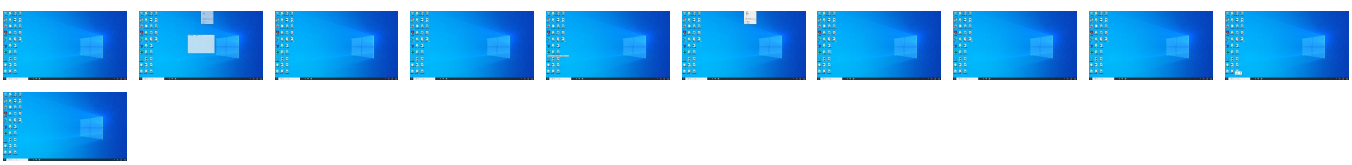
Behavior Graph



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
Swift Mesaj#U0131#09971.exe	10%	Virustotal		Browse
Swift Mesaj#U0131#09971.exe	2%	ReversingLabs	Win32.Downloader.Minix	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-console-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-datetime-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-debug-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-errorhandling-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l2-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-handle-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-interlocked-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-libraryloader-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-localization-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-memory-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-namedpipe-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processenvironment-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-profile-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-rtlsupport-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-string-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-1-0.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-sysinfo-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-timezone-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-util-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-conio-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-convert-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-environment-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-filesystem-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-locale-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-math-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-multibyte-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-private-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-process-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-runtime-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-stdio-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-string-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-time-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-utility-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\mozglue.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\msvcp140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\nss3.dll	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\nssdbm3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\softokn3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\ucrtbase.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\E0F35830\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsjFA0C.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
aapancart.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://dbxo1.shop/db1/index.phpft	0%	Avira URL Cloud	safe	
http://https://aapancart.com/	2%	Virustotal		Browse
http://dbxo1.shop/db1/index.php	0%	Avira URL Cloud	safe	
http://https://aapancart.com/	0%	Avira URL Cloud	safe	
http://dbxo1.shop/db1/index.phpl	0%	Avira URL Cloud	safe	
http://dbxo1.shop/db1/index.phpp	0%	Avira URL Cloud	safe	
http://dbxo1.shop/	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	Avira URL Cloud	safe	
http://www.mozilla.com0	0%	Avira URL Cloud	safe	
http://dbxo1.shop/nr	0%	Avira URL Cloud	safe	
http://dbxo1.shop/db1/index.phpC	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
aapancart.com	103.14.99.114	true	false	• 2%, Virustotal, Browse	unknown
dbxo1.shop	172.67.203.65	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://dbxo1.shop/db1/index.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

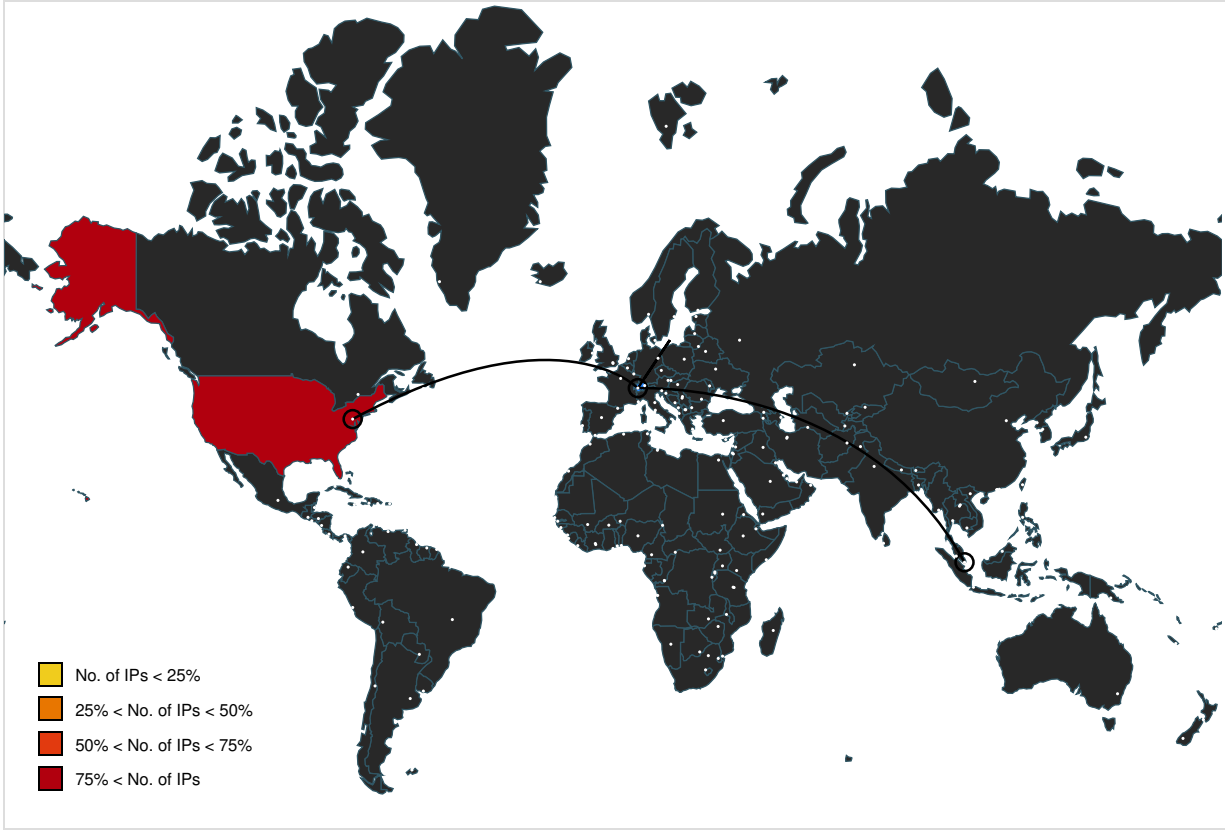
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aapancart.com/	Swift Mesaj#U0131#09971.exe, 00000004.00000002.8060357272.000000000183A000.00000004.00000020.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://dbxo1.shop/db1/index.phpp	Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033506219.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8030675103.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033003378.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8031540665.000000000186C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mozilla.com/en-US/blocklist/	mozglue.dll.4.dr	false		high
http://dbxo1.shop/db1/index.phpft	Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033506219.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8030675103.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033003378.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8031540665.000000000186C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dbxo1.shop/db1/index.phpl	Swift Mesaj#U0131#09971.exe, 00000004.00000002.8078319161.000000001D460000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.thawte.com/ThawteTimestampingCA.crl0	Swift Mesaj#U0131#09971.exe, 00000004.00000003.8021778482.000000001DAEC000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8030240707.000000001DCE8000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7996026153.000000001DD00000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8005301719.000000001D47C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7994139478.000000001DD5C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8006844600.000000001D49C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8020950343.000000001DA9C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8002183781.000000001E710000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8025045932.000000001DB7C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8021957690.000000001DB14000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8027339216.000000001DCC4000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8011167801.000000001D498000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7994673416.000000001DD04000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7992634785.000000001DD00000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7996275434.000000001DD58000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8026822739.000000001DCAC000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8000125730.000000001E840000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8007210967.000000001D474000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8005491336.000000001D464000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000002.8095117598.000000001E2C0000.00000004.00001000.00020000.00000000.sdmp, nss3.dll.4.dr	false		high
http://dbxo1.shop/	Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033506219.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8030675103.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033003378.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8031540665.000000000186C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.thawte.com0	Swift Mesaj#U0131#09971.exe, 00000004.00000003.8021778482.000000001DAEC000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8030240707.000000001DCE8000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7996026153.000000001DD00000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8005301719.000000001D47C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7994139478.000000001DD5C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8006844600.000000001D49C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8020950343.000000001DA9C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8002183781.000000001E710000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8025045932.000000001DB7C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8021957690.000000001DB14000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8027339216.000000001DCC4000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8011167801.000000001D498000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7994673416.000000001DD04000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7992634785.000000001DD00000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7996275434.000000001DD58000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8026822739.000000001DCAC000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8000125730.000000001E840000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8007210967.000000001D474000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8005491336.000000001D464000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000002.8095117598.000000001E2C0000.00000004.00001000.00020000.00000000.sdmp, nss3.dll.4.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mozilla.com0	Swift Mesaj#U0131#09971.exe, 00000004.00000003.8021778482.000000001DAEC000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8030240707.000000001DCE8000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7996026153.000000001DD00000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8005301719.000000001D47C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7994139478.000000001DD5C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8006844600.000000001D49C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8020950343.000000001DA9C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8002183781.000000001E710000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8025045932.000000001DB7C000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8021957690.000000001DB14000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8027339216.000000001DCC4000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8011167801.000000001D498000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7994673416.000000001DD04000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7992634785.000000001DD00000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.7996275434.000000001DD58000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8026822739.000000001DCAC000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8000125730.000000001E840000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8007210967.000000001D474000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8005491336.000000001D464000.00000004.00001000.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000002.8095117598.000000001E2C0000.00000004.00001000.00020000.00000000.sdmp, nss3.dll.4.dr	false	• Avira URL Cloud: safe	unknown
http://dbxo1.shop/nr	Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033506219.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8030675103.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033003378.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8031540665.000000000186C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	Swift Mesaj#U0131#09971.exe	false		high
http://dbxo1.shop/db1/index.phpC	Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033506219.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8030675103.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8033003378.000000000186C000.00000004.00000020.00020000.00000000.sdmp, Swift Mesaj#U0131#09971.exe, 00000004.00000003.8031540665.000000000186C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.14.99.114	aapancart.com	Singapore		58641	TRUNKOZ-INTrunkozTechnologiesPvt LtdIN	false
172.67.203.65	dbxo1.shop	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755179
Start date and time:	2022-11-28 12:43:49 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Swift Mesaj#U0131#09971.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@8/55@2/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24% (good quality ratio 23.5%) • Quality average: 87.8% • Quality standard deviation: 21.8%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, ctldl.windowsupdate.com, wdcp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- 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.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

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\4925762587255721772989999.tmp

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000, page size 2048, file counter 3, database pages 22, 1st free page 7, free pages 2, cookie 0x10, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.7853305971874845

Encrypted:	false
SSDEEP:	48:43b/DVIIgyZKLk8s8LKvUf9K4UKTgyJqhtcebVEq8Ma0D0HOlcjlGxdKmtAONu41:Sb+uKLyeym/grcebn8MouOjlGxdKmt3N
MD5:	00C036C61F625BF9D25362B9BE24ADEB
SHA1:	6738C3D037E4A2E9F41B1398BA88E5771532F593
SHA-256:	0C187B091E99E5BB665C59F8F8E027D5658904B32E4196D2EB402F3B1CAD69EF
SHA-512:	711265BC8C1653BF6E862343BF3149A2AB09F4BA7D38E2D8A437001DB6C0F1936F6362571DD577CD7BDBEEC766DF141CB7E0681512C12E25A99CDB71731232D1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....S`..... ....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-console-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.080160932980843
Encrypted:	false
SSDEEP:	192:3jBMWIghWGZiKedXe123Ouo+Uggs/nGfe4pBjS/uBmWh0txKdmVWQ4GWDZoiyqnP:GWPhWVXYi00GftpBjSemTltcwpS
MD5:	502263C56F931DF8440D7FD2FA7B7C00
SHA1:	523A3D7C3F4491E67FC710575D8E23314DB2C1A2
SHA-256:	94A5DF1227818EDBFD0D5091C6A48F86B4117C38550343F780C604EEE1CD6231
SHA-512:	633EFAB26CDED9C3A5E144B81CBBD3B6ADF265134C37D88CFD5F49BB18C345B2FC3A08BA4BBC917B6F64013E275239026829BA08962E94115E94204A47B8022D1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....".....!.. ....0.....J....@.....+..... .....8=.....T.....text...+..... ..`.rsrc..... .....@..@.....".....:...T...T.....".....d.....".....RSDSMB...5.G.8.'.d.....api-ms-win-core-console-l1-1-0.pdb.....T....rdata..T.... ....rdata$zzzdbg.....+....edata... ..`....rsrc$01....` .....rsrc$02.....".....(...`.....W.....G...o.....D...s.....5...b..... .....api-ms-win-core-console-l1-1-0.dll.AllocConsole.kern

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-datetime-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.093995452106596
Encrypted:	false
SSDEEP:	192:RWIghWG4U9xluZo123Ouo+Uggs/nGfe4pBjSbMDPxVWh0txKdmVWQ4CWrDry6qnZ:RWPhWFv0i00GftpBjBHem6plUG+zIw
MD5:	CB978304B79EF53962408C611DFB20F5
SHA1:	ECA42F7754FB0017E86D50D507674981F80BC0B9
SHA-256:	90FAE0E7C3644A6754833C42B0AC39B6F23859F9A7CF4B6C8624820F59B9DAD3
SHA-512:	369798CD3F37FBAE311B6299DA67D19707D8F770CF46A8D12D5A6C1F25F85FC959AC5B5926BC68112FA9EB62B402E8B495B9E44F44F8949D7D648EA7C572CF8C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...A..... .....!..... ....0.....#....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@....A.....<...T...T.....A.....d.....A.....RSDS...W,X.I..o....4....api-ms-win-core-datetime-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....A.....P.....(...8...H.....t.....api-ms-win-core-datetime-l1-1-0.dll.GetDateFormatA.kernel32.GetDateFormatA.GetDateFormatW.kernel32.GetDateFormatW.GetTimeFormatA.kernel32.GetTimeFormatA

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-debug-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1028816880814265
Encrypted:	false

SSDEEP:	384:cWPhWM4Ri00GftpBj2YILemtclD16PaEC:l10oiBQe/L
MD5:	88FF191FD8648099592ED28EE6C442A5
SHA1:	6A4F818B53606A5602C609EC343974C2103BC9CC
SHA-256:	C310CC91464C9431AB0902A561AF947FA5C973925FF70482D3DE017ED3F73B7D
SHA-512:	942AE86550D4A4886DAC909898621DAB18512C20F3D694A8AD444220AEAD76FA88C481DF39F93C7074DBBC31C3B4DAF97099CFED86C2A0AAA4B63190A4B307FD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....GF....@..... .....8=.....T.....text..... ..`.rsrc..... .....@..@.....9...T...T.....d.....RSDS.j..v..C...B..h....api-ms-win-core-debug-l1-1-0.pdb.....T....rdata..T.... ....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....P.....(...8...H...|.....q.....api-ms-win-core-debug-l1-1-0.dll.DebugBreak .kernel32.DebugBreak.IsDebuggerPresent.kernel32.IsDebuggerPresent.OutputDebugStringA.kernel32.OutputDebugStri

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-errorhandling-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.126358371711227
Encrypted:	false
SSDEEP:	192:NFmxD3PWIghWGJY/luZo123Ouo+Uggs/nGfe4pBjSffcp8Wh0txKdmVWQ4yWRzOr:NFkWPhW60i00GftpBj4emHlD16Pa7v
MD5:	6D778E83F74A4C7FE4C077DC279F6867
SHA1:	F5D9CF848F79A57F690DA9841C209B4837C2E6C3
SHA-256:	A97DCCA76CDB12E985DFF71040815F28508C655AB2B073512E386DD63F4DA325
SHA-512:	02EF01583A265532D3970B7D520728AA9B68F2B7C309EE66BD2B38BAF473EF662C9D7A223ACF2DA722587429DA6E4FBC0496253BA5C41E214BEA240CE824E8A2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...\x..... .....!..... ....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@....\x.....A...T...T.....\x.....d.....\x.....RSDS.1....U45.z.d.....api-ms-win-core-errorhandling-l1-1-0.pdb..... T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....\x.....n.....(...D...`.....4...f.....'...J.....api-ms-win-core-errorhandling-l1-1-0.dll.GetErrorMode.kernel32.GetErrorMode.GetLastError.kernel32.GetLastError.RaiseExcept

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21816
Entropy (8bit):	7.014255619395433
Encrypted:	false
SSDEEP:	384:d6PvVXHWPhWnsnhi00GftpBjaJemyDlD16PamW8:UPvVX85nhoisJeLt8
MD5:	94AE25C7A5497CA0BE6882A00644CA64
SHA1:	F7AC28BBC47E46485025A51EEB6C304B70CEE215
SHA-256:	7EA06B7050F9EA2BCC12AF34374BDF1173646D4E5EBF66AD690B37F4DF5F3D4E
SHA-512:	83E570B79111706742D0684FC16207AE87A78FA7FFEF58B40AA50A6B9A2C2F77FE023AF732EF577FB7CD2666E33FFAF0E427F41CA04075D83E0F6A52A177C2B0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... .....0.....@...../....@.....0.....8=.....T.....text..... ..`.rsrc.....0.....@..@.....8...T...T.....d.....RSDS.0...B..8....G....api-ms-win-core-file-l1-1-0.pdb.....T....rdata..T.....rdata $zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....K...K.....D...p...6...`.....?...l.....A.....6..._.....;...e..... ...l...n.... .....-...d.....*...g.....*...U.....M...

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-2-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.112057846012794
Encrypted:	false
SSDEEP:	192:IWIghWGJnWdsNtL/123Ouo+Uggs/nGfe4pBjSfcD63QXWh0txKdmVWQ4yW1rwqnh:IWPhWIsnhi00GftpBjnem9lD16PamFP

MD5:	E2F648AE40D234A3892E1455B4DBBE05
SHA1:	D9D750E828B629CFB7B402A3442947545D8D781B
SHA-256:	C8C499B012D0D63B7AFC8B4CA42D6D996B2FCF2E8B5F94CACFBEC9E6F33E8A03
SHA-512:	18D4E7A804813D9376427E12DAA444167129277E5FF30502A0FA29A96884BF902B43A5F0E6841EA1582981971843A4F7F928F8AECAC693904AB20CA40EE4E954
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...._.L.... .....!..... ....0.....@.....L..... .....8=.....T.....text...<..... ....`.rsrc..... .....@..@....._.L.....8...T...T....._.L.....d....._.L.....RSDS.....g"Y.....api-ms-win-core-file-l1-2-0.pdb.....T....rdata..T..... rdata$zzzdbg.....L....edata... ..`....rsrc$01....` .....rsrc$02....._.L....@.....(...8...l.....`.....api-ms-win-core-file-l1-2-0.dll.CreateFile2.kerne l32.CreateFile2.GetTempPathW.kernel32.GetTempPathW.GetVolumeNameForVolumeMountPointW.kernel32.GetVolumeNameForVolumeMou

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l2-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.166618249693435
Encrypted:	false
SSDEEP:	192:BZwWIghWG4U9ydsNtL/123Ouo+Uggs/nGfe4pBjSbUGHvNWh0txKdmVWQ4CWVU9h:UWPhWFBsnhi00GftpBjKvxemPlP55QQ7
MD5:	E479444BDD4AE4577FD32314A68F5D28
SHA1:	77EDF9509A252E886D4DA388BF9C9294D95498EB
SHA-256:	C85DC081B1964B77D289AAC43CC64746E7B141D036F248A731601EB98F827719
SHA-512:	2AFAB302FE0F7476A4254714575D77B584CD2DC5330B9B25B852CD71267CDA365D280F9AA8D544D4687DC388A2614A51C0418864C41AD389E1E847D81C3AB74
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...4..|.... .....!..... ....0.....t.....@..... .....8=.....T.....text...}..... ....`.rsrc..... .....@..@....4..|.....8...T...T.....4..|.....d.....4..|.....RSDS.=.Co.P..Gd./%P....api-ms-win-core-file-l2-1-0.pdb.....T....rdata. .T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....4..|.....D...p.....#...P.....;...g.....<...m.....%...Z..... .api-ms-win-core-file-l2-1-0.dll.CopyFile2.kernel32.CopyFile2.CopyFileExW.kernel32.CopyFileExW.Crea

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-handle-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1117101479630005
Encrypted:	false
SSDEEP:	384:AWPhWXDz6i00GftpBj5FrFaemx+lDbNh/6:hroidkeppp
MD5:	6DB54065B33861967B491DD1C8FD8595
SHA1:	ED0938BBC0E2A863859AAD64606B8FC4C69B810A
SHA-256:	945CC64EE04B1964C1F9FCDC3124DD83973D332F5CFB696CDF128CA5C4CBD0E5
SHA-512:	AA6F0BCB760D449A3A82AED67CA0F7FB747CBB82E627210F377AF74E0B43A45BA660E9E3FE1AD4CBD2B46B1127108EC4A96C5CF9DE1BDEC36E993D0657A61 5B6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....G..... .....!..... ....0.....V.....@..... ....8=.....T.....text..._..... ....`.rsrc..... .....@..@.....G.....:...T...T.....G.....d.....G.....RSDSQ..{...IS].0.> ....api-ms-win-core-handle-l1-1-0.pdb.....T ....rdata..T.....rdata$zzzdbg.....__....edata... ..`....rsrc$01....` .....rsrc$02.....G....Z.....(...<...P.....A...|.....,.....api-ms-win-core-handle-l1-1-0.dll.CloseHandle.kernel32.CloseHandle.CompareObjectHandles.kernel32.CompareObjectHandles.DuplicateHandle.kernel32

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-heap-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.174986589968396
Encrypted:	false
SSDEEP:	192:GElqWIghWGZi5edXe123Ouo+Uggs/nGfe4pBjS/PHyRWh0txKdmVWQ4GWC2w4Dj3:GElqWPhWCXYi00GftpBjP9emYXlDbNs
MD5:	2EA3901D7B50BF6071EC8732371B821C
SHA1:	E7BE926F0F7D842271F7EDC7A4989544F4477DA7

SHA-256:	44F6DF4280C8ECC9C6E609B1A4BFEE041332D337D84679CFE0D6678CE8F2998A
SHA-512:	6BFFAC8E157A913C5660CD2FABD503C09B47D25F9C220DCE8615255C9524E4896EDF76FE2C2CC8BDEF58D9E736F5514A53C8E33D8325476C5F605C2421F15C D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....:.....!.. ....0.....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.....:.....8...T...T.....:.....d.....:.....RSDS.K....OB;....X.....api-ms-win-core-heap-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....:.....X.....2...Q...q.....C...h.....(...E...f.....0..._...z..... .....api-ms-win-core-heap-l1-1-0.dll.GetProcessHeap.k

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-interlocked-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17856
Entropy (8bit):	7.076803035880586
Encrypted:	false
SSDEEP:	192:DtiYsFWWIghWGQtu7B123Ouo+Uggs/nGfe4pBjSPiZadcbWh0txKdmVWQ4mWf2FN:5iYsFWWPhWUTi00GftpBjremUBNlgC
MD5:	D97A1CB141C6806F0101A5ED2673A63D
SHA1:	D31A84C1499A9128A8F0EFEA4230FCFA6C9579BE
SHA-256:	DECCD75FC3FC2BB31338B6FE26DEFFBD7914C6CD6A907E76FD4931B7D141718C
SHA-512:	0E3202041DEF9D2278416B7826C61621DCED6DEE8269507CE5783C193771F6B26D47FEB0700BBE937D8AFF9F7489890B5263D63203B5BA99E0B4099A5699C620
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....$..... .....!..... .....0.....@..... .....9.....T.....text..... ....`.rsrc..... .....@..@.....$.....?...T...T.....$.....d.....$.....RSDS#.....,.S.6.~j....api-ms-win-core-interlocked-l1-1-0.pdb.....T.. ..rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....$.....(...T.....L.....!...U.....1.....p.....@...s..... .....api-ms-win-core-interlocked-l1-1-0.dll.InitializeSListHead.kernel32.InitializeSLis

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-libraryloader-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.131154779640255
Encrypted:	false
SSDEEP:	384:yHvuBL3BmWPhWZTi00GftpBjNKnemenyAlvN9W/L:yWBL3BXYoinKne1yd
MD5:	D0873E21721D04E20B6FFB038ACCF2F1
SHA1:	9E39E505D80D67B347B19A349A1532746C1F7F88
SHA-256:	BB25CCF8694D1FCFCE85A7159DCF6985FDB54728D29B021CB3D14242F65909CE
SHA-512:	4B7F2AD9EAD6489E1EA0704CF5F1B1579BAF1061B193D54CC6201FFDDA890A8C8FACB23091DFD851DD70D7922E0C7E95416F623C48EC25137DDD66E32DF9A 37
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u*I.... .....!..... .....0.....9.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@.....u*I.....A...T...T.....u*I.....d.....u*I.....RSDSU..e.j.(.wD.....api-ms-win-core-libraryloader-l1-1-0.pdb..... T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....u*I.....(...p.....R...}.....*...Y.....8..._.....B...k..... .....F...u.....)...P...w.....api-ms-win-c

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-localization-l1-2-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.089032314841867
Encrypted:	false
SSDEEP:	384:KOMw3zdp3bwjGjue9/0jCRrndbVWPhWIDz6i00GftpBj6cemjlD16Pa+4r:KOMwBprwjGjue9/0jCRrndbCOoireqv
MD5:	EFF11130BFE0D9C90C0026BF2FB219AE
SHA1:	CF4C89A6E46090D3D8FEEB9EB697AEA8A26E4088
SHA-256:	03AD57C24FF2CF895B5F533F0ECBD10266FD8634C6B9053CC9CB33B814AD5D97

SHA-512:	8133FB9F6B92F498413DB3140A80D6624A705F80D9C7AE627DFD48ADEB8C5305A61351BF27BBF02B4D3961F9943E26C55C2A66976251BB61EF1537BC8C212AD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...S.v..... .....!..... ....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T. ...rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....S.v.....v.....;...;...(.....<...f.....5...]..... .....l...l...q..... N...../...j...../...^...../...\.....8...`.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-memory-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.101895292899441
Encrypted:	false
SSDEEP:	384:+bZWPhWUsnhi00GftpBjwBemQlD16Par7:b4nhoi6BedH
MD5:	D500D9E24F33933956DF0E26F087FD91
SHA1:	6C537678AB6CFD6F3EA0DC0F5ABEFD1C4924F0C0
SHA-256:	BB33A9E906A5863043753C44F6F8165AFE4D5EDB7E55EFA4C7E6E1ED90778ECA
SHA-512:	C89023EB98BF29ADEEBFBCB570427B6DF301DE3D27FF7F4F0A098949F987F7C192E23695888A73F1A2019F1AF06F2135F919F6C606A07C8FA9F07C00C64A34B5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....%(.... .....!..... ....0.....@.....!..... .....8=.....T.....text...!..... ....`.rsrc..... .....@..@.....%(.....:...T...T.....%(.....d.....%(.....RSDS.~....%.T.....CO....api-ms-win-core-memory-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....!....edata... ..`....rsrc$01....` .....rsrc$02.....%(.....(...h.....)...P...w.....C...g.....%...P.....B...g..... .....4...[...|.....=.....api-ms-win-core-memory-l1-1-0.dl

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-namedpipe-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.16337963516533
Encrypted:	false
SSDEEP:	192:pgWIghWGZiBeS123Ouo+Uggs/nGfe4pBjS/fE/hWh0txKdmVWQ4GWoxYyqnaj/6B:iWPhWUEi00GftpBj1temnltcwWB
MD5:	6F6796D1278670CCE6E2D85199623E27
SHA1:	8AA2155C3D3D5AA23F56CD0BC507255FC953CCC3
SHA-256:	C4F60F911068AB6D7F578D449BA7B5B9969F08FC683FD0CE8E2705BBF061F507
SHA-512:	6E7B134CA930BB33D2822677F31ECA1CB6C1DFF55211296324D2EA9EBDC7C01338F07D22A10C5C5E1179F14B1B5A4E3B0BAFB1C8D39FCF1107C57F9EAF063A 7B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L... .....!.. ....0.....-....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.... .....=...T...T..... .....d..... .....RSDS...IK..XM.&.....api-ms-win-core-namedpipe-l1-1-0.pdb.....T....rdata..T.. .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02..... .....(...P...x.....:...w.....O...y.....&...W.....=...j.....api-m s-win-core-namedpipe-l1-1-0.dll.ConnectNamedPipe.kernel32.ConnectNamedPipe.CreateNamedP

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processenvironment-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.073730829887072
Encrypted:	false
SSDEEP:	192:wXjWIghWGd4dsNtL/123Ouo+Uggs/nGfe4pBjSXcYddWh0txKdmVWQ4SW04engo5:MjWPhWHsnhi00GftpBjW7emOj5l1z6hP
MD5:	5F73A814936C8E7E4A2DFD68876143C8
SHA1:	D960016C4F553E461AFB5B06B039A15D2E76135E
SHA-256:	96898930FFB338DA45497BE019AE1ADCD63C5851141169D3023E53CE4C7A483E
SHA-512:	77987906A9D248448FA23DB2A634869B47AE3EC81EA383A74634A8C09244C674ECF9AADCDE298E5996CAFBB8522EDE78D08AAA270FD43C66BEDE24115CDBD FED

Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...).r..... .....!..... ....0.....:....@.....G..... .....0=.....T.....text...G..... ....`.rsrc..... .....@..@....).r.....F...T...T.....).r.....d.....).r.....RSDS.6..~x.....'.....api-ms-win-core-processenvironment-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....G....edata... ..`....rsrc$01....` .....rsrc$02.....).r.....(...|.....B.....$...M...{.....P.....6...k..... ...../...(...e.....=...f.....8...q.....!..T..... .....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19392
Entropy (8bit):	7.082421046253008
Encrypted:	false
SSDEEP:	384:afk1JzNcKSIJWPhW2snhi00GftpBjZqcLvemr4PlgC:RcKST+nhoi/BbeGv
MD5:	A2D7D7711F9C0E3E065B2929FF342666
SHA1:	A17B1F36E73B82EF9BFB831058F187535A550EB8
SHA-256:	9DAB884071B1F7D7A167F9BEC94BA2BEE875E3365603FA29B31DE286C6A97A1D
SHA-512:	D436B2192C4392A041E20506B2DFB593FE5797F1FDC2CDEB2D7958832C4C0A9E00D3AEA6AA1737D8A9773817FEADF47EE826A6B05FD75AB0BDAE984895C2C4EF
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....I.....@..... ....9.....T.....text..... . .`.rsrc..... .....@..@.....B...T...T.....d.....RSDS..t.....=j.....api-ms-win-core-processthreads-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....1...1...(.....K...x.....,..`.....C...q.....'...N...y.....".....I...{..... .....B...p.....,...c.....H...x.....9...S...p.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-1.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.1156948849491055
Encrypted:	false
SSDEEP:	384:xzADfIeRWPhWKEi00GftpBjj1emMVlvN0M:xzfeWeoi11ep
MD5:	D0289835D97D103BAD0DD7B9637538A1
SHA1:	8CEEBE1E9ABB0044808122557DE8AAB28AD14575
SHA-256:	91EEB842973495DEB98CEF0377240D2F9C3D370AC4CF513FD215857E9F265A6A
SHA-512:	97C47B2E1BFD45B905F51A282683434ED784BFB334B908BF5A47285F90201A23817FF91E21EA0B9CA5F6EE6B69ACAC252EEC55D895F942A94EDD88C4BFD2DAFD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....9..... .....!..... ....0.....k.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@.....9.....B...T...T.....9.....d.....9.....RSDS&.n....5..I....)....api-ms-win-core-processthreads-l1-1-1.pdb..... ..T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....9.....(...`.....-...I.....)"...W.....N.....P.....F...q..... .....3...r.....api-ms-win-core-processthreads-l1-1-1.dll.FlushInstr

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-profile-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17712
Entropy (8bit):	7.187691342157284
Encrypted:	false
SSDEEP:	192:w9WIghWGdUuDz7M123Ouo+Uggs/nGfe4pBjSXrw58h6Wh0txKdmVWQ4SW7QQtzko:w9WPhWYDz6i00GftpBjXPemD5l1z6hv
MD5:	FEE0926AA1BF00F2BEC9DA5DB7B2DE56
SHA1:	F5A4EB3D8AC8FB68AF716857629A43CD6BE63473
SHA-256:	8EB5270FA99069709C846DB38BE743A1A80A42AA1A88776131F79E1D07CC411C
SHA-512:	0958759A1C4A4126F80AA5CDD9DF0E18504198AEC6828C8CE8EB5F615AD33BF7EF0231B509ED6FD1304EEAB32878C5A649881901ABD26D05FD686F5EBEF2D1C3

Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....&..... .....!..... ....0.....0.....@..... ....0=.....T.....text..... ....`.rsrc..... .....@..@.....&.....;...T...T.....&.....d.....&.....RSDS...O.""#.n....D:....api-ms-win-core-profile-l1-1-0.pdb.....T....rdata ..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....&.....<.....(...0...8...w....._.....api-ms-win-core-profile-l1-1-0.dll.QueryPerform anceCounter.kernel32.QueryPerformanceCounter.QueryPerformanceFrequency.kernel32.QueryPerformanceFrequency.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-rtlsupport-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17720
Entropy (8bit):	7.19694878324007
Encrypted:	false
SSDEEP:	384:61G1WPhWksnhi00GftpBjEVXremWRlP55Jk:kGiYnhoiqVXreDT5Y
MD5:	FDBA0DB0A1652D86CD471EAA509E56EA
SHA1:	3197CB45787D47BAC80223E3E98851E48A122EFA
SHA-256:	2257FEA1E71F7058439B3727ED68EF048BD91DCACD64762EB5C64A9D49DF0B57
SHA-512:	E5056D2BD34DC74FC5F35EA7AA8189AAA86569904B0013A7830314AE0E2763E95483FABDCBA93F6418FB447A4A74AB0F07712ED23F2E1B840E47A099B1E68E1 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....(.....!.. ....0.....}"....@..... .....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....(.....>...T...T.....(.....d.....(.....RSDS?.L.N.o.....=.....api-ms-win-core-rtlsupport-l1-1-0.pdb.....T....rdata.. T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....(....F.....(...4...@...~.....l.....api-ms-win-core-rtlsupport-l1-1-0.dll.RtlC aptureContext.ntdll.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind.

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-string-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.137724132900032
Encrypted:	false
SSDEEP:	384:xyMvRWPhWFs0i00GftpBjwCJdemnflUG+zl4:xyMvWWoibeTnn
MD5:	12CC7D8017023EF04EBDD28EF9558305
SHA1:	F859A66009D1CAAE88BF36B569B63E1FBDAE9493
SHA-256:	7670FDEDE524A485C13B11A7C878015E9B0D441B7D8EB15CA675AD6B9C9A7311
SHA-512:	F62303D98EA7D0DDBE78E4AB4DB31AC283C3A6F56DBE5E3640CBCF8C06353A37776BF914CFE57BBB77FC94CCFA48FAC06E74E27A4333FBDD112554C646838 929
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....R..... .....!..... ....0.....\....@..... .....8=.....T..... .....text..... ....`.rsrc..... .....@..@.....R.....:...T...T.....R.....d.....R.....RSDS..D..a..1.f....7....api-ms-win-core-string-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....R.....x.....(...H...h.....)...O...x.....>...i.....api-ms-win-core-string-l1-1-0.dll.CompareStringEx.kernel32.CompareStringEx.CompareStringOrdinal.kernel32.Compare

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.04640581473745
Encrypted:	false
SSDEEP:	384:5Xdv3V0dfpkXc0vVaHWPhWXEi00GftpBj9em+4lndanJ7o:5Xdv3VqpkXc0vVa8poivex
MD5:	71AF7ED2A72267AAAD8564524903CFF6
SHA1:	8A8437123DE5A22AB843ADC24A01AC06F48DB0D3
SHA-256:	5DD4CCD63E6ED07CA3987AB5634CA4207D69C47C2544DFEFC41935617652820F
SHA-512:	7EC2E0FEBC89263925C0352A2DE8CC13DA37172555C3AF9869F9DBB3D627DD1382D2ED3FDAD90594B3E3B0733F2D3CFDEC45BC713A4B7E85A09C164C3DFA 875

Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....2.... .....!..... .....0.....@.....V..... .....8=.....T.....text...V..... ....`.rsrc..... .....@..@.....2.....9...T...T.....2.....d.....2.....RSDS...z..C...+Q_.....api-ms-win-core-synch-l1-1-0.pdb.....T....rda ta..T.....rdata$zzzdbg.....V....edata... ..`....rsrc$01....` .....rsrc$02.....2.....)...)...(.....p.....1...c.....!...F...m.....$...X.....$...[..... ..@...i.....!...Q.....[.....7.....O.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-2-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.138910839042951
Encrypted:	false
SSDEEP:	384:JtZ3gWPhWFA0i00GftpBj4Z8wemFfYlP55t:j+oiVweb53
MD5:	0D1AA99ED8069BA73CFD74B0FDDC7B3A
SHA1:	BA1F5384072DF8AF5743F81FD02C98773B5ED147
SHA-256:	30D99CE1D732F6C9CF82671E1D9088AA94E720382066B79175E2D16778A3DAD1
SHA-512:	6B1A87B1C223B757E5A39486BE60F7DD2956BB505A235DF406BCF693C7DD440E1F6D65FFEF7FDE491371C682F4A8BB3FD4CE8D8E09A6992BB131ADDF11EF2E F9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...X*uY.... .....!..... .....0.....3.....@.....v..... .....8=.....T.....text...v..... ....`.rsrc..... .....@..@....X*uY.....9...T...T.....X*uY.....d.....X*uY.....RSDS.V..B...`..S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rda ta..T.....rdata$zzzdbg.....v....edata... ..`....rsrc$01....` .....rsrc$02.....X*uY.....(...l.....R.....W.....&...b.....$...W.....6...w..... .....;...|.....H.....A.....api-ms-win-core-synch-

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-sysinfo-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.072555805949365
Encrypted:	false
SSDEEP:	384:2q25WPhWWsnhi00GftpBj1u6qXxem4l1z6hi:25+SnhoiG6IeA8
MD5:	19A40AF040BD7ADD901AA967600259D9
SHA1:	05B6322979B0B67526AE5CD6E820596CBE7393E4
SHA-256:	4B704B36E1672AE02E697EFD1BF46F11B42D776550BA34A90CD189F6C5C61F92
SHA-512:	5CC4D55350A808620A7E8A993A90E7D05B441DA24127A00B15F96AAE902E4538CA4FED5628D7072358E14681543FD750AD49877B75E790D201AB9BAFF6898C8D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....C=.... .....!..... .....0.....@.....E..... .....0=.....T.....text...E..... ....`.rsrc..... .....@..@.....C=.....;...T...T.....C=.....d.....C=.....RSDS....T.>eD.#|.../....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....E....edata... ..`....rsrc$01....` .....rsrc$02.....C=.....(.....:...i.....N.....7...s.....+...M...r...../...'... V.....:...k.....X..... ...?...d.....".....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-timezone-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18224
Entropy (8bit):	7.17450177544266
Encrypted:	false
SSDEEP:	384:SWPhWK3di00GftpBjH35Gvem2Al1z6hIu:77NoiOve7eu
MD5:	BABF80608FD68A09656871EC8597296C
SHA1:	33952578924B0376CA4AE6A10B8D4ED749D10688
SHA-256:	24C9AA0B70E557A49DAC159C825A013A71A190DF5E7A837BFA047A06BBA59ECA
SHA-512:	3FFFFD90800DE708D62978CA7B50FE9CE1E47839CDA11ED9E7723ACEC7AB5829FA901595868E4AB029CDFB12137CF8ECD7B685953330D0900F741C894B88257 B
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....Y.x.... .....!..... ....0.....}3....@..... .....0=.....T.....text..... ....`.rsrc..... .....@..@.....Y.x.....<...T...T.....Y.x.....d.....Y.x.....RSDS.^.b. .t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rd ata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....Y.x.....(...L...p.....5...s.....+...i.....U.....I.....api-ms-win-core-timezone-l1-1-0.dll.FileTimeToSystemTime.kernel32.FileTimeToSystemTime.GetDynamicTimeZ

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-util-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1007227686954275
Encrypted:	false
SSDEEP:	192:pePWIghWG4U9wluZo123Ouo+Uggs/nGfe4pBjSbKT8wuxWh0txKdmVWQ4CWnFnwQ:pYWPhWFS0i00GftpBj7DudemJIP552
MD5:	0F079489ABD2B16751CEB7447512A70D
SHA1:	679DD712ED1C46FBD9BC8615598DA585D94D5D87
SHA-256:	F7D450A0F59151BCEFB98D20FCAE35F76029DF57138002DB5651D1B6A33ADC86
SHA-512:	92D64299EBDE83A4D7BE36F07F65DD868DA2765EB3B39F5128321AFF66ABD66171C7542E06272CB958901D403CCF69ED716259E0556EE983D2973FAA03C55D3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.. ....0.....`k....@.....9..... .....8=.....T.....text...)..... . .`.rsrc..... .....@..@.....f.....8...T...T.....f.....d.....f.....RSDS*...$.L.Rm..l.....api-ms-win-core-util-l1-1-0.pdb.....T....rdata..T.....r data$zzzdbg.....9....edata... ..`....rsrc$01....` .....rsrc$02.....f.....J.....,...@...o.....j...}.....api-ms-win-core-util-l1-1-0.dll.Beep.kernel32.Beep .DecodePointer.kernel32.DecodePointer.DecodeSystemPointer.kernel32.DecodeSystemPointer.EncodePointer.kernel3

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-conio-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.088693688879585
Encrypted:	false
SSDEEP:	384:8WPhWz4Ri00GftpBjDb7bemHlndanJ7DW:Fm0oiV7beV
MD5:	6EA692F862BDEB446E649E4B2893E36F
SHA1:	84FCEAE03D28FF1907048ACEE7EAE7E45BAAF2BD
SHA-256:	9CA21763C528584BDB4EFEBE914FAAF792C9D7360677C87E93BD7BA7BB4367F2
SHA-512:	9661C135F50000E0018B3E5C119515CFE977B2F5F88B0F5715E29DF10517B196C81694D074398C99A572A971EC843B3676D6A831714AB632645ED25959D5E3E7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....@..... ....8=.....T.....text..... .. `.rsrc..... .....@..@v.....8...d...d.....d.....RSDS....<....2..u....api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....T.....(.....>...w...../...W...p.....,...L...l.....,...L...m..... t.....'...^.....P...g.....$...=...

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-convert-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22328
Entropy (8bit):	6.929204936143068
Encrypted:	false
SSDEEP:	384:EuydWPhW7snhi00GftpBjd6t/emJlDbN:3tnhoi6t/eAp
MD5:	72E28C902CD947F9A3425B19AC5A64BD
SHA1:	9B97F7A43D43CB0F1B87FC75FEF7D9EEEA11E6F7
SHA-256:	3CC1377D495260C380E8D225E5EE889CBB2ED22E79862D4278CFA898E58E44D1
SHA-512:	58AB6FEDCE2F8EE0970894273886CB20B10D92979B21CDA97AE0C41D0676CC0CD90691C58B223BCE5F338E0718D1716E6CE59A106901FE9706F85C3ACF7855F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE..... .....!.....0.....@.....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....NE.....:...d...d.....NE.....d.....NE.....RSDS..e.7P.g^j..[....api-ms-win-crt-convert-l1-1-0.pdb.....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....NE.....z...z...8... .....(...C...^...y.....1...N...k..... .....*...E...`...y.....5...R...o.....,...M...n.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-environment-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18736
Entropy (8bit):	7.078409479204304
Encrypted:	false
SSDEEP:	192:bWIghWGd4edXe123Ouo+Uggs/nGfe4pBjSXXmv5Wh0txKdmVWQ4SWEApkqnajPBZ:bWPhWqXYi00GftpBjBemPl1z6h2
MD5:	AC290DAD7CB4CA2D93516580452EDA1C
SHA1:	FA949453557D0049D723F9615E4F390010520EDA
SHA-256:	C0D75D1887C32A1B1006B3CFFC29DF84A0D73C435CDCB404B6964BE176A61382
SHA-512:	B5E2B9F5A9DD8A482169C7FC05F018AD8FE6AE27CB6540E67679272698BFCA24B2CA5A377FA61897F328B3DEAC10237CAFBD73BC965BF9055765923ABA9478 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....jU..... .....!..... ....0.....G.....@.....".....0=.....T.....text...2..... ....`.rsrc..... .....@..@v.....jU.....>...d...d.....jU.....d.....jU.....RSDSu..1.N....R.s,"\....api-ms-win-crt-environment-l1-1-0.pdb.....d....rdata..d.....rdata$zzzdbg....."....edata... ..`....rsrc$01....` .....rsrc$02.....jU.....8.....C...d.....3...O...l..... ..... 5...Z...w.....)...F...a.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-filesystem-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.085387497246545
Encrypted:	false
SSDEEP:	384:sq6nWm5C1WPhWFK0i00GftpBjB1UemKklUG+zIOd/:x6nWm5CiooiKeZnbd/
MD5:	AEC2268601470050E62CB8066DD41A59
SHA1:	363ED259905442C4E3B89901BFD8A43B96BF25E4
SHA-256:	7633774EFFE7C0ADD6752FFE90104D633FC8262C87871D096C2FC07C20018ED2
SHA-512:	0C14D160BFA3AC52C35FF2F2813B85F8212C5F3AFBCFE71A60CCC2B9E61E51736F0BF37CA1F9975B28968790EA62ED5924FAE4654182F67114BD20D8466C4B8 F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....h.... .....!..... ....0.....l.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....h.....=...d...d.....h.....d.....h.....RSDS.....a.'..G...A.....api-ms-win-crt-filesystem-l1-1-0.pdb..... ....d....rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....h.....A...A...8...<...@.....$...=...V...q.....)...M...q...../... O...o.....7...X...v.....6...U...r.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-heap-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.060393359865728
Encrypted:	false
SSDEEP:	192:+Y3vY17aFBR4WIghWG4U9CedXe123Ouo+Uggs/nGfe4pBjSbGGAPWh0txKdmVWQC:+Y3e9WPhWFsXYi00GftpBjfemnlP55s
MD5:	93D3DA06BF894F4FA21007BEE06B5E7D
SHA1:	1E47230A7EBCFAF643087A1929A385E0D554AD15
SHA-256:	F5CF623BA14B017AF4AEC6C15EEE446C647AB6D2A5DEE9D6975ADC69994A113D
SHA-512:	72BD6D46A464DE74A8DAC4C346C52D068116910587B1C7B97978DF888925216958CE77BE1AE049C3DCCF5BF3FFFB21BC41A0AC329622BC9BBC190DF63ABB2 C6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...J.o ....!..... ....0.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@v.....J.o .....7...d...d.....J.o .....d.....J.o .....RSDSq.....pkQX[....api-ms-win-crt-heap-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....J.o ....6.....(.....c.....S.....1...V...y.....<...c..... .....U...z.....:...u.....&...E...p.....,...U...

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-locale-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.13172731865352
Encrypted:	false
SSDEEP:	192:fiWIghWGZirX+4z123Ouo+Uggs/nGfe4pBjS/RFcpOWh0txKdmVWQ4GWs8ylDikh:aWPhWjO4Ri00GftpBjZOemSXlvNQ0
MD5:	A2F2258C32E3BA9ABF9E9E38EF7DA8C9
SHA1:	116846CA871114B7C54148AB2D968F364DA6142F
SHA-256:	565A2EEC5449EEEED68B430F2E9B92507F979174F9C9A71D0C36D58B96051C33
SHA-512:	E98CBC8D958E604EFFA614A3964B3D66B6FC646BDCA9AA679EA5E4EB92EC0497B91485A40742F3471F4FF10DE83122331699EDC56A50F06AE86F21FAD70953F E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...|..O.... .....!..... ....0.....E*....@..... .....e..... .....8=.....T.....text...u..... ....`.rsrc..... .....@..@v.....|..O.....9...d...d.....|..O.....d.....|..O.....RSDS.X...7.....$k....api-ms-win-crt-locale-l1-1-0.pdb... .....d....rdata..d.....rdata$zzzdbg.....e....edata... ..`....rsrc$01....` .....rsrc$02.....|..O.....8.....5...h.....E.....$...N...t..... .$...D...b...!...R..... ...s.....:...k.....9...X.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-math-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28984
Entropy (8bit):	6.6686462438397
Encrypted:	false
SSDEEP:	384:7OTEmbM4Oe5grykfIgTmLyWPhW30i00GftpBjAKemXlDbNI:dEMq5grxfInbRoiNeSp
MD5:	8B0BA750E7B15300482CE6C961A932F0
SHA1:	71A2F5D76D23E48CEF8F258EAAD63E586CFC0E19
SHA-256:	BECE7BAB83A5D0EC5C35F0841CBBF413E01AC878550FBDB34816ED55185DCFED
SHA-512:	FB646CDCDB462A347ED843312418F037F3212B2481F3897A16C22446824149EE96EB4A4B47A903CA27B1F4D7A352605D4930DF73092C380E3D4D77CE4E972C5A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....@.....P.....@.....+.....@.....4..8=.....T.....text...,..... ....`.rsrc.....@.....0.....@..@v.....7...d...d.....d.....RSDSB...=.....,....api-ms-win-crt-math-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....+...edata...@..`....rsrc$01....`@.....rsrc$02.....l.....:..:...(.....(...@...X...q.....4...M...g..... ..= ..i ... ...!..E!..o!...!...!...!..."..F"..s"..."..."..."...#..E#..o#...#...#..

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-multibyte-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26424
Entropy (8bit):	6.712286643697659
Encrypted:	false
SSDEEP:	384:kDy+Kr6aLPmIHJI6/CpG3t2G3t4odXL5WPhWFY0i00GftpBjbnMxem8hzlmTMiLV:kDZKrZPmIHJI64GoiZMxe0V
MD5:	35FC66BD813D0F126883E695664E7B83
SHA1:	2FD63C18CC5DC4DEFC7EA82F421050E668F68548
SHA-256:	66ABF3A1147751C95689F5BC6A259E55281EC3D06D3332DD0BA464EFFA716735
SHA-512:	65F8397DE5C48D3DF8AD79BAF46C1D3A0761F727E918AE63612EA37D96ADF16CC76D70D454A599F37F9BA9B4E2E38EBC845DF4C74FC1E1131720FD0DCB8814 31
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u'..... .....!....$.....@.....P.....@..... .....@.....*..8=.....T.....text....".....$ ....`.rsrc.....@.....&.....@..@v.....u'.....<...d...d.....u'.....d.....u'.....RSDS7.%..5..+...+.....api-ms-win-crt-multibyte-l1-1- 0.pdb.....d....rdata..d.....rdata$zzzdbg..... ...edata...@..`....rsrc$01....`@.....rsrc$02.....u'.....8...X...x...;..`.....1...T...w.....'. ..L...q.....B...e.....7...Z...}.....+...L...m.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-private-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73016
Entropy (8bit):	5.838702055399663
Encrypted:	false
SSDEEP:	1536:VAHEGlVDe5c4bFE2Jy2cvxXWpD9d3334BkZnkPFZo6kt:Vc7De5c4bFE2Jy2cvxXWpD9d3334BkZj
MD5:	9910A1BFDC41C5B39F6AF37F0A22AACD
SHA1:	47FA76778556F34A5E7910C816C78835109E4050
SHA-256:	65DED8D2CE159B2F5569F55B2CAF0E2C90F3694BD88C89DE790A15A49D8386B9
SHA-512:	A9788D0F8B3F61235EF4740724B4A0D8C0D3CF51F851C367CC9779AB07F208864A7F1B4A44255E0DE8E030D84B63B1BDB58F12C8C20455FF6A55EF6207B31A9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....^1.... .....!.....R.....@.....8=.....T.....text..... ....`.rsrc.....@..@v.....^1.....:...d...d.....^1.....d.....^1.....RSDS.J..w/.8..bu..3.....api-ms-win-crt-private-l1-1-0.pdb..... d....rdata..d.....rdata$zzzdbg.....edata.....`....rsrc$01....`.....rsrc$02.....^1....>.....8...h#...5...>...?..7?.._?...?...?...?...@..V@...@...@...@..+A..\A.. .A...A...A...B..LB...B...B...C..HC...C...C...C...C...D..HD...D...D...E..eE...E...F..1F..gF...F...F...G..BG..uG...G..

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-process-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.076072254895036
Encrypted:	false
SSDEEP:	192:aRQqjd7dWIghWG4U9kuDz7M123Ouo+Uggs/nGfe4pBjSbAURWh0txKdmVWQ4CW+6:aKcWPhWFkDz6i00GftpBjYemZlUG+zIU
MD5:	8D02DD4C29BD490E672D271700511371
SHA1:	F3035A756E2E963764912C6B432E74615AE07011
SHA-256:	C03124BA691B187917BA79078C66E12CBF5387A3741203070BA23980AA471E8B
SHA-512:	D44EF51D3AAF42681659FFFFF4DD1A1957EAF4B8AB7BB798704102555DA127B9D7228580DCED4E0FC98C5F4026B1BAB242808E72A76E09726B0AF839E384C3E 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...I.h..... .....!..... .....0.....U....@.....x..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....I.h.....:...d...d.....I.h.....d.....I.h.....RSDSZ\.qM..I....3.....api-ms-win-crt-process-l1-1-0.pdb.....d. ...rdata..d.....rdata$zzzdbg.....x....edata... ..`....rsrc$01....` .....rsrc$02.....I.h.....$...$...8.....X.....&...@...Y...q.....*...E..._...z..... .....!...<...V...q.....9...V...t.....7...R...i...

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-runtime-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22840
Entropy (8bit):	6.942029615075195
Encrypted:	false
SSDEEP:	384:7b7hrKwWPhWFlsnhi00GftpBj+6em90lmTMiLzrF7:7bNrKxZnhoig6eQN7
MD5:	41A348F9BEDC8681FB30FA78E45EDB24
SHA1:	66E76C0574A549F293323DD6F863A8A5B54F3F9B
SHA-256:	C9BBC07A033BAB6A828ECC30648B501121586F6F53346B1CD0649D7B648EA60B
SHA-512:	8C2CB53CCF9719DE87EE65ED2E1947E266EC7E8343246DEF6429C6DF0DC514079F5171ACD1AA637276256C607F1063144494B992D4635B01E09DDEA6F5EEF2(
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....L..... .....!.....0.....@.....i....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....L.....:...d...d.....L.....d.....L.....RSDS6..>[d.=. ....C....api-ms-win-crt-runtime-l1-1-0.pdb.. .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....L.....f.....k...k...8.....4...S...s.....E...g..... ...)...N...n.....&...E...f.....'...D...j.....>.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-stdio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24368
Entropy (8bit):	6.873960147000383
Encrypted:	false
SSDEEP:	384:GZpFVhjWPhWxEi00GftpBjmjjem3Cl1z6h1r:eCfoi0espbr
MD5:	FEFB98394CB9EF4368DA798DEAB00E21
SHA1:	316D86926B558C9F3F6133739C1A8477B9E60740
SHA-256:	B1E702B840AEBE2E9244CD41512D158A43E6E9516CD2015A84EB962FA3FF0DF7
SHA-512:	57476FE9B546E4CAFB1EF4FD1CBD757385BA2D445D1785987AFB46298ACBE4B05266A0C4325868BC4245C2F41E7E2553585BFB5C70910E687F57DAC6A8E911E 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....0.....@.....)....@.....a.....0.....".."..0=.....T.....text...a..... ....`.rsrc.....0.....@..@v.....8...d...d.....d.....RSDS...iS#.hg.....j....api-ms-win-crt-stdio-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....^.....(..... .....<...y.....)...h..... ...].....H.....)...D...^..v..... .....T...u.....9...Z...{.....0...Q...

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23488
Entropy (8bit):	6.840671293766487
Encrypted:	false
SSDEEP:	384:5iFMx0C5yguNvZ5VQgx3SbwA7yMVlkFGlnWPhWGTi00GftpBjslem89lgC:56S5yguNvZ5VQgx3SbwA71lkFv5oialj
MD5:	404604CD100A1E60DFDAF6ECF5BA14C0
SHA1:	58469835AB4B916927B3CABF54AEE4F380FF6748
SHA-256:	73CC56F20268BFB329CCD891822E2E70DD70FE21FC7101DEB3FA30C34A08450C
SHA-512:	DA024CCB50D4A2A5355B7712BA896DF850CEE57AA4ADA33AAD0BAE6960BCD1E5E3CEE9488371AB6E19A2073508FBB3F0B257382713A31BC0947A4BF1F7A20 BE4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....S.... .....!.....0.....@.....B....@.....0....."...9.....T.....text..... ....`.rsrc.....0.....@..@v.....S.....9...d...d.....S.....d.....S.....RSDSI.....$[~f..5....api-ms-win-crt-string-l1-1-0.pdb... .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....S....,.....8.....W...s.....#...B...a.....<... [...z.....;...[...{..... ...A...b.....<...X...r.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-time-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.018061005886957
Encrypted:	false
SSDEEP:	384:8ZSWWVgWPhWFe3di00GftpBjnlfemHlUG+zlTA+0:XRNoibernAA+0
MD5:	849F2C3EBF1FCBA33D16153692D5810F
SHA1:	1F8EDA52D31512EBFDD546BE60990B95C8E28BFB
SHA-256:	69885FD581641B4A680846F93C2DD21E5DD8E3BA37409783BC5B3160A919CB5D
SHA-512:	44DC4200A653363C9A1CB2BDD3DA5F371F7D1FB644D1CE2FF5FE57D939B35130AC8AE27A3F07B82B3428233F07F974628027B0E6B6F70F7B2A8D259BE95222F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....OI..... ......!..... ....0.....@..... ....8=.....T..... .....text..... ....`.rsrc..... .....@..@v.....OI.....7...d...d.....OI.....d.....OI.....RSDS...s..,E.w.9I..D....api-ms-win-crt-time-l1-1-0.pdb..... ..d....rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....OI.....H...H...(...H...h... ...=...\...z.....8...V...s.....&...D...a...~..... .....?...b.....!...F...k.....0...N...k.....

C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-utility-l1-1-0.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.127951145819804
Encrypted:	false
SSDEEP:	192:QqfHQdu3WIghWG4U9lYdsNtL/123Ouo+Uggs/nGfe4pBjSb8Z9Wh0txKdmVWQ4Cg:/fBWPhWF+esnhi00GftpBjLBemHlP55q
MD5:	B52A0CA52C9C207874639B62B6082242
SHA1:	6FB845D6A82102FF74BD35F42A2844D8C450413B
SHA-256:	A1D1D6B0CB0A8421D7C0D1297C4C389C95514493CD0A386B49DC517AC1B9A2B0
SHA-512:	18834D89376D703BD461EDF7738EB723AD8D54CB92ACC9B6F10CBB55D63DB22C2A0F2F3067FE2CC6FEB775DB397030606608FF791A46BF048016A1333028D0A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....!5..... .....!..... ....0.....4....@.....^..... ....8=.....T..... .....text...n..... ....`.rsrc..... .....@..@v.....!5.....:...d...d.....!5.....d.....!5.....RSDS.....k.....api-ms-win-crt-utility-l1-1-0.pdb.....d. ...rdata..d.....rdata$zzzdbg.....^....edata... ..`....rsrc$01....` .....rsrc$02.....!5....d.....8.....(.....#...<...U...l.....+...@...[...r..... .....4...l..._.....3...N...e...|.....

C:\Users\user\AppData\Local\Temp\E0F35830\freebl3.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	332752
Entropy (8bit):	6.8061257098244905
Encrypted:	false
SSDEEP:	6144:C+YBCxpjbRIDmvby5xDXIFVJM8PojGGHrIr1qqDL6XP+jW:Cu4Abg7XV72Gl/qn6z
MD5:	343AA83574577727AABE537DCCFDEAFC
SHA1:	9CE3B9A182429C0DBA9821E2E72D3AB46F5D0A06
SHA-256:	393AE7F06FE6CD19EA6D57A93DD0ACD839EE39BA386CF1CA774C4C59A3BFEBD8
SHA-512:	827425D98BA491CD30929BEE6D658FCF537776CE96288180FE670FA6320C64177A7214FF4884AE3AA68E135070F28CA228AFB7F4012B724014BA7D106B5F0DCE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW.. AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L.....Z....."!.....f.....p.....o..... @.....P...`.....@..p.....P.....T.....8...@.....8.....text...U..... ..`.rdata.....@..@.data. ..IH.....@....rsrc...p....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\E0F35830\mozglue.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	139216
Entropy (8bit):	6.841477908153926
Encrypted:	false
SSDEEP:	3072:8Oqe98Ea4usvd5jm6V0InXx/CHzGYC6NccMmxK3atIYHD2JJJsPyimY4kQkE:Vqe98Evua5Sm0ux/5YC6NccMmtXHD2JR
MD5:	9E682F1EB98A9D41468FC3E50F907635
SHA1:	85E0CECA36F657DDF6547AA0744F0855A27527EE
SHA-256:	830533BB569594EC2F7C07896B90225006B90A9AF108F49D6FB6BEBD02428B2D
SHA-512:	230230722D61AC1089FABF3F2DECFA04F9296498F8E2A2A49B1527797DCA67B5A11AB8656F04087ACADF873FA8976400D57C77C404EBA4AFF89D92B9986F32E D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$......"yQ.f.?Mf.?Mf.?Mo`.Mv.?M.z>Lb.?M...Md.?M.z<Lh.?M.z;Lm.?M.z:Lu.?MDx>Lo.?Mf.>M..?M.{1Lu.?M.{?Lg.?M.{.Mg.?M.{=Lg.?MRichf.?M.....PE..L.....Z....."!.....@.....@.....\...L...,.... ..p.....0.....p...T.....@.....T...@.....text..... ..`.rdata...b.....d.....@..@.data.....@....rsrc...p.... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\E0F35830\msvcp140.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecI
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;....."...;.....;.....;.....;.....;.....;.....;.-...;..... Rich.....PE..L....8'Y....."!.....P..... .....az....@A.....C.....R..;.....x..8?.....4:..f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B.....

C:\Users\user\AppData\Local\Temp\E0F35830\nss3.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1244112
Entropy (8bit):	6.809431682312062
Encrypted:	false
SSDEEP:	24576:XDI7l4/FeoJQuQ3IhXtHfjyqgJ0BnPQAib7/12bg2JSna5xfg0867U4MSpu731hn:uQ3YX5jyqgynPkbd24VwMSpu7Fhn
MD5:	556EA09421A0F74D31C4C0A89A70DC23
SHA1:	F739BA9B548EE64B13EB434A3130406D23F836E3
SHA-256:	F0E6210D4A0D48C7908D8D1C270449C91EB4523E312A61256833BFEAF699ABFB
SHA-512:	2481FC80DFFA8922569552C3C3EBAEF8D0341B80427447A14B291EC39EA62AB9C05A75E85EEF5EA7F857488CAB1463C18586F9B076E2958C5A314E459045EDE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x..c+..c+..c+...+..c++.b*..c+lh.+..c++.`*..c++.f*..c++.g*..c+.b*..c+9.b*..c+..b+..c+9.k*..c+9.g*C.c+9.c*..c+9..+..c+9.a*..c+Rich..c+.....PE..L...a..Z....."!.....T.....@.....@.....d....<..T.....h.....t~..0...T.....@.....text..... ..`.rdata...P.....R.....@..@.data....E...`... ..:.....@....rsrc...h....Z.....@..@.reloc..t~.....^.....@..B.....

C:\Users\user\AppData\Local\Temp\E0F35830\nssdbm3.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639368309935547
Encrypted:	false
SSDEEP:	1536:5vNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwI41ZH:hNGVOiBZbcGmxXMcBqmzoCUZoZebHZMw
MD5:	569A7A65658A46F9412BDFA04F86E2B2
SHA1:	44CC0038E891AE73C43B61A71A46C97F98B1030D
SHA-256:	541A293C450E609810279F121A5E9DFA4E924D52E8B0C6C543512B5026EFE7EC
SHA-512:	C027B9D06C627026774195D3EAB72BD245EBBF5521CB769A4205E989B07CB4687993A47061FF6343E6EC1C059C3EC19664B52ED3A1100E6A78CFFB1C46472AFB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4.. .5.Z.4.Y.5...4...0.A.4...4.X.4....X.4...6.X.4.RichY.4.....PE..L.....Z....."!.....0.....0.....@.....?.....@.....`..p..... .L.....p.....:..T.....(;..@.....0..X.....text..... ..`.rdata..4....0... .....@..@.data.....P.....>.....@....rsrc...p...` .....@.....@..@.reloc.....p.....D.....@..B.....

C:\Users\user\AppData\Local\Temp\E0F35830\softokn3.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144336
Entropy (8bit):	6.5527585854849395
Encrypted:	false
SSDEEP:	3072:zAf6suip+z7FEk/oJz69sFaXeu9CoT2nIZvetBWqIBoE9Mv:Q6PpsF4CoT2EeY2eMv
MD5:	67827DB2380B5848166A411BAE9F0632
SHA1:	F68F1096C5A3F7B90824AA0F7B9DA372228363FF
SHA-256:	9A7F11C212D61856DFC494DE111911B7A6D9D5E9795B0B70BBBC998896F068AE
SHA-512:	910E15FD39B48CD13427526FDB702135A7164E1748A7EACCD6716BCB64B978FE333AC26FA8EBA73ED33BD32F2330D5C343FCD3F0FE2FFD7DF54DB89052DB7 48
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L.....Z.....!.....`.....P.....+Z...@..... .....0..p.....@..`.....T.....(...@.....l.....text..... ..`.rdata...C.....D.....@..@.data..... .....@ ....rsrc...p....0.....@..@.reloc..`....@.....@..B.....

C:\Users\user\AppData\Local\Temp\E0F35830\ucrtbase.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1142072
Entropy (8bit):	6.809041027525523
Encrypted:	false
SSDEEP:	24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvIZPoy4TbK:FBmF2lleaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....o.....p..... .Rich.....PE..L....3.....!....Z.....=.....p.....p.....@A.....`.....0..8=.....$... ...T.....H...@... .....text....Z.....Z..... ..`.data.....p.....^.....@....idata..6.....l.....@..@.rsrc.....@..@.reloc..$..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\E0F35830\vcruntime140.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39nil35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E9 1F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D.....2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@.....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\nsjFA0C.tmp\System.dll

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8Qll972eXqlWBFSt273YOlEz
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37
SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....uY.....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..`....P.....*.....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Bikes\Bombekrater210\Cykelhandlerne.Sme

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	data
Category:	dropped
Size (bytes):	163713
Entropy (8bit):	6.703687358308117
Encrypted:	false
SSDEEP:	3072:j3P7bnP0jsXQmlADxsqOED1twvxrmjVlCTxgdeA1yi:r7bsjsXvlWOqOC1tww7t1J
MD5:	C15A4105508E9FC45F3218E037F75764
SHA1:	36650E7CB589FF9B505173A6FE541A180B63C505
SHA-256:	A1ED770994E83E4E8F7939F9BBF7F1B382E941EBCC31CF93CB995E5A8878AE19
SHA-512:	2933BE999B618DBC27B6EEE94176891A1AA0209B8D87650ED07E9CB32C0D1B527D35344B8A2373A3DA0BEAD331E352C58004262DA23A273FFD7F8F7F5619315
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Castrate\memstat.c

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	C source, ASCII text
Category:	dropped
Size (bytes):	13484
Entropy (8bit):	5.15716859322729
Encrypted:	false
SSDEEP:	192:B3tdgdRmAMgyWkSctse3XX6ZjuguOixHRYqx0NzZW+08e:B3tuPdjJ0TCzZWv
MD5:	BD46EB22C1A1B4EA40373E8F57BFF4E3
SHA1:	CC2943E660BBB1697B7561F2776A7BCE2F36718A
SHA-256:	8361836BCB172722E5F2EE90AF31834B9B08B828A90E80E0BB930C336001B4CE
SHA-512:	5994643BCDFDF59B7EBF8FE36BC30CF0A454966FA95741D80AC81E9C42126A66ACDD782F6D7852A35CAE171FCC0DE1218EC1CD951829F7EC1C72B35EE748774
Malicious:	false

Preview:	/*.** 2018-09-27.**.** The author disclaims copyright to this source code. In place of.** a legal notice, here is a blessing:.**.** May you do good and not evil..** May you find forgiveness for yourself and forgive others..** May you share freely, never taking more than you give..**.********** **********.**.** This file demonstrates an eponymous virtual table that returns information.** from sqlite3_status64() and sqlite3_db_status()..**.** Usage example :.**.** .load ./memstat.** .mode quote.** .header on.** SELECT * FROM memstat;.*/.#if !defined(SQLITE_CORE) || defined(SQLITE_ENABLE_M EMSTATVTAB).#if !defined(SQLITEINT_H).#include "sqlite3ext.h".#endif.SQLITE_EXTENSION_INIT1.#include <assert.h>.#include <string.h>..#ifndef SQLITE_OM IT_VIRTUALTABLE../* memstat_vtab is a subclass of sqlite3_vtab which will.** serve as the underlying representation of a memstat virtual table.*/.typedef struct memstat_vtab memsta

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Coasting102.For

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	data
Category:	dropped
Size (bytes):	125801
Entropy (8bit):	**7.998523783088745**
Encrypted:	**true**
SSDEEP:	3072:RhtQlryNxvwwP0nccqsIyxErSJE/zCClGEog7xfMR9UtLxo:RAyNxvhP0cAJbJE/O+be
MD5:	F79429CFC0A30DD02E6738983443837B
SHA1:	9285EF62440B8BCC95D566ABCD6ADD3A67BA0AA0
SHA-256:	12A9EE2C36002CF30EEF2446FD8B42BF8544A5C41B35DD7C7C7C7A65CC4C6F59
SHA-512:	8F99C12264642E2EA535D099FE003C48E7D4FE40D18CE2CD78B9AA0B172FB647A85F961637386B06FC0E06B024B0E1CA7F50B52A8A2E6C2546CF0AB28B25A7D 7
Malicious:	false
Preview:	......3.<...z'.:w9..YX'I...L9A...{..D.:.8.?}.L..d.<iC..7.....ro...k..98].A.3...2....a...G...O....TH5.....B.....k..y{....Y.....r...pg....L....v.|./..0.D.../..#.*.#....3.-...<Hf.+....h..enR\J.....Y ..s}.L.....!}a.c:..3...]..7..]...y5'.).W..mTb'C8.@.Hv.Z.m..h8.C..5.M(...S.....L.....3....."Y....9C.....IQ.V.6.F..Ih4.)-M..m.M.....ex.YD...ID.dr....f...p.|.....*t..3<.%l.....G.P..x.X 8Q#.S..Z)Z.L.c..=..C..c.f2..:.FG<.V....[..H#...Id....p.[..UW.d@=..:..^.9.....O.*1./..Z.(.vrb&.....UD:s..$.#.[.8...\l...z.Ft"7l\|..nc9,.....;.c&Ul..../..x...wO.{5.3.....'.{..3s..<...w...o. ..+.....D...!.\.*.C../O....D...2.a..A.....;r...z.g.7.1.U...J..v0s../.....U.Y..Pl.....,\|.Z.~..".7._..)..\|..;#O.95.9*..h..mF6.p.\^...'...@'p=H%}ie..c....UD.^JD.9$|..,WPK.j....q.<R..0 .....89HTo.W6...9k.R.[....!.w...Q...;3...[.).2..'..E..n..P....m.....Ue...&....|....k.S..-O..&...0...!..J..o.SI.....6.#.'.efOt.DH)..F\.f0.....?.{..v.`...7./..Jz..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Novelizes\selection-end-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	138
Entropy (8bit):	5.559646592748364
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllO9p2hkq8PQ1/kbcw1w9lDk7kup:6v/lhPys8pQt8PQ2cw1llDXup
MD5:	9863709F8F136F0F38A5D9CF2740143A
SHA1:	0EC6AA74A3FED4719B1B8D2E8468239489D84427
SHA-256:	2C86B3EDF2A397608FE0C12A634F175DE1E3C4E5C4610B8457578B549069A7B0
SHA-512:	B1D8DC9CAFF35264E117201C0DB2112F4C07BAB9235188D32F90B9D00DC2E7AC27ECC1FC9753C5F50949C95D91EEA0C5F318D6D1C8D7587CA0A68AD2CC1C EB5
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....AIDAT8.c`.....X..X.....C...u..(&.%.. ..t.H6...$.....S.F.....a/..&I.....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\libxml2-2.0.typelib

Process:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false

Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;margin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.809605729039489
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:	Swift Mesaj#U0131#09971.exe
File size:	379329
MD5:	310df09294b852bab67e158d95788150
SHA1:	9b69175fcbcc718212d21a77d39969309e9787f8
SHA256:	d27bf1156e1a463ebada17bac3b3a314835cead7e75c4770c95ff21f06e00310
SHA512:	1a04ea3cb29e0ea106ea89d79cf0af5d995f31d3b43fcf80886e488bf86be0bbb928a694653abd996e23ab51d25bbbeba5b2a8042df0aacd4fc18c56f82a4ec5
SSDEEP:	6144:nQ606xDpoDTOfHQerv77fY7U/KTdZ1sj60AyNxvhP0cAJbJE/O+bfTv/1:FpoPOfQqvHfY7UCry6svmb+3H1
TLSH:	168412612364C947E66451B0DC1282F39A769C15E20B3FCFE3913D4CBE32B60E92E795
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...6.uY.....f.....

File Icon

Icon Hash:	c60ccd1616164e46

Static PE Info

General

Entrypoint:	0x403373
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x59759536 [Mon Jul 24 06:35:34 2017 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:	b34f154ec913d2d2c435cbd644e91687

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi

Instruction
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [00434EECh], eax
je 00007F1B7483A023h
push ebx
call 00007F1B7483D2B9h
cmp eax, ebx
je 00007F1B7483A019h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F1B7483D233h
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F1B74839FFCh
push 0000000Ah
call 00007F1B7483D28Ch
push 00000008h
call 00007F1B7483D285h
push 00000006h
mov dword ptr [00434EE4h], eax
call 00007F1B7483D279h
cmp eax, ebx
je 00007F1B7483A021h
push 0000001Eh
call eax
test eax, eax
je 00007F1B7483A019h
or byte ptr [00434EEFh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [00434FB8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0042B208h
call dword ptr [00408188h]
push 0040A2C8h

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8608	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x76000	0x16898	.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	0x8000	0x2b0	.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	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x65ef	0x6600	False	0.6750919117647058	data	6.514810500836391	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x149a	0x1600	False	0.43803267045454547	data	5.007075185851696	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2aff8	0x600	False	0.5162760416666666	data	4.036693470004838	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x35000	0x41000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x76000	0x16898	0x16a00	False	0.7946089433701657	data	7.153289056271752	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x76478	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x767e0	0x9d19	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x80500	0x4102	PNG image data, 256 x 256, 8-bit colormap, non-interlaced	English	United States
RT_ICON	0x84608	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x86bb0	0x16e8	PNG image data, 256 x 256, 4-bit colormap, non-interlaced	English	United States
RT_ICON	0x88298	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x89340	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304	English	United States
RT_ICON	0x8a1e8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024	English	United States
RT_ICON	0x8aa90	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0x8b0f8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256	English	United States
RT_ICON	0x8b660	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x8bac8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x8bdb0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_DIALOG	0x8bed8	0x144	data	English	United States
RT_DIALOG	0x8c020	0x13c	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x8c160	0x100	data	English	United States
RT_DIALOG	0x8c260	0x11c	data	English	United States
RT_DIALOG	0x8c380	0xc4	data	English	United States
RT_DIALOG	0x8c448	0x60	data	English	United States
RT_GROUP_ICON	0x8c4a8	0xae	data	English	United States
RT_MANIFEST	0x8c558	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, SetCurrentDirectoryW, GetFileAttributesW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, ExitProcess, GetShortPathNameW, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, CreateFileW, GetTempFileNameW, WriteFile, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, lstrcmpiW, MoveFileW, GetFullPathNameW, SetFileTime, SearchPathW, CompareFileTime, lstrcmpW, CloseHandle, ExpandEnvironmentStringsW, GlobalFree, GlobalLock, GlobalUnlock, GlobalAlloc, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, lstrlenA, MulDiv, MultiByteToWideChar, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW
USER32.dll	GetSystemMenu, SetClassLongW, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, GetDC, SetTimer, SetWindowTextW, LoadImageW, SetForegroundWindow, ShowWindow, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, EndPaint, CreateDialogParamW, SendMessageTimeoutW, wsprintfW, PostQuitMessage
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, SHFileOperationW
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExW, RegOpenKeyExW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, RegEnumValueW, RegDeleteKeyW, RegDeleteValueW, RegCloseKey, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

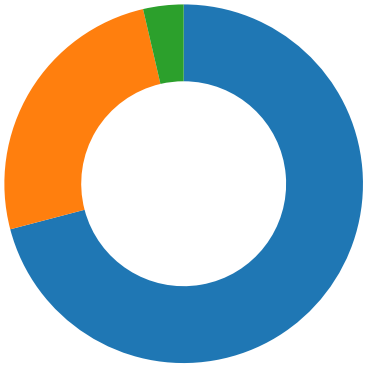
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
172.67.203.65192.168.11.2080498362029137 11/28/22-12:46:57.711672	TCP	2029137	ET TROJAN AZORult v3.3 Server Response M2	80	49836	172.67.203.65	192.168.11.20
192.168.11.20172.67.203.6549836802029468 11/28/22-12:46:56.779159	TCP	2029468	ET TROJAN Win32/AZORult V3.3 Client Checkin M15	49836	80	192.168.11.20	172.67.203.65

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 12:46:55.603820086 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:55.603908062 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:55.604131937 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:55.629722118 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:55.629785061 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:55.932869911 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:55.933147907 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.057482958 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.057508945 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.057931900 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.058120012 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.061511993 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.104389906 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.194681883 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.194745064 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.194956064 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.195015907 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.195036888 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.195287943 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.326483965 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.326664925 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.326752901 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.326767921 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.326795101 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.326910019 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.326910019 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.326971054 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.327001095 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.327014923 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.327063084 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.327265978 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.327265978 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.458192110 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.458354950 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.458357096 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.458451033 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.458484888 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.458631992 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.458683014 CET	49834	443	192.168.11.20	103.14.99.114

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 12:46:56.458790064 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.458949089 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.459009886 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.459053040 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.459086895 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.459142923 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.459295034 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.459330082 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.459357023 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.459449053 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.459460020 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.459639072 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.459676027 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.459702015 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.459927082 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.540010929 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.540296078 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.591116905 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.591326952 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.591387987 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.591638088 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.591880083 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.591974020 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.592205048 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.592233896 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.592281103 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.592349052 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.592525959 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.592652082 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.592652082 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.592720032 CET	443	49834	103.14.99.114	192.168.11.20
Nov 28, 2022 12:46:56.592911959 CET	49834	443	192.168.11.20	103.14.99.114
Nov 28, 2022 12:46:56.766000032 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:56.778613091 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:56.778862953 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:56.779159069 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:56.791711092 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.711672068 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.711761951 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.711833000 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.711895943 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.711905956 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:57.711961031 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.711972952 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:57.712023973 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.712085962 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.712094069 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:57.712151051 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.712151051 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:57.712212086 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:57.712215900 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.712274075 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:57.712280989 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.712403059 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.712400913 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:57.712461948 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:57.712471008 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.712529898 CET	80	49836	172.67.203.65	192.168.11.20
Nov 28, 2022 12:46:57.712603092 CET	49836	80	192.168.11.20	172.67.203.65

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 12:46:57.712661982 CET	49836	80	192.168.11.20	172.67.203.65
Nov 28, 2022 12:46:57.712807894 CET	49836	80	192.168.11.20	172.67.203.65

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 12:46:55.577858925 CET	63342	53	192.168.11.20	1.1.1.1
Nov 28, 2022 12:46:55.594774961 CET	53	63342	1.1.1.1	192.168.11.20
Nov 28, 2022 12:46:56.735022068 CET	53223	53	192.168.11.20	1.1.1.1
Nov 28, 2022 12:46:56.763128996 CET	53	53223	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
Nov 28, 2022 12:46:55.577858925 CET	192.168.11.20	1.1.1.1	0xf676	Standard query (0)	aapancart.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 12:46:56.735022068 CET	192.168.11.20	1.1.1.1	0x273f	Standard query (0)	dbxo1.shop	A (IP address)	IN (0x0001)	false

DNS Answers

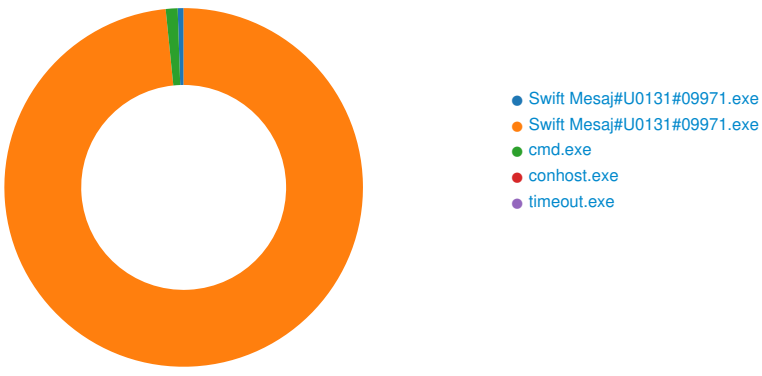
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 28, 2022 12:46:55.594774961 CET	1.1.1.1	192.168.11.20	0xf676	No error (0)	aapancart.com		103.14.99.114	A (IP address)	IN (0x0001)	false
Nov 28, 2022 12:46:56.763128996 CET	1.1.1.1	192.168.11.20	0x273f	No error (0)	dbxo1.shop		172.67.203.65	A (IP address)	IN (0x0001)	false
Nov 28, 2022 12:46:56.763128996 CET	1.1.1.1	192.168.11.20	0x273f	No error (0)	dbxo1.shop		104.21.44.194	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- aapancart.com
- dbxo1.shop

Statistics

Behavior



System Behavior

Analysis Process: Swift Mesaj#U0131#09971.exe PID: **7596**, Parent PID: **4572**

General

Target ID:	1
Start time:	12:46:07
Start date:	28/11/2022
Path:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
Imagebase:	0x400000
File size:	379329 bytes
MD5 hash:	310DF09294B852BAB67E158D95788150
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.7935875493.0000000002AF0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000001.00000002.7934819719.00000000005AB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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: Swift Mesaj#U0131#09971.exe PID: **3172**, Parent PID: **7596**

General

Target ID:	4
Start time:	12:46:33
Start date:	28/11/2022
Path:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe
Imagebase:	0x400000
File size:	379329 bytes
MD5 hash:	310DF09294B852BAB67E158D95788150
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000004.00000003.8040635695.000000001D9B8000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000000.7688018397.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000004.00000002.8078319161.000000001D460000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000004.00000003.8040702551.000000001D9BC000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.8078519186.000000001D570000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000004.00000002.8078519186.000000001D570000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.8095117598.000000001E2C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security

Reputation:	low

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	1683F14	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1683F14	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1683F14	InternetOpenUrlA
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	1683F14	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1683F14	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1683F14	InternetOpenUrlA
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	418A75	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
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	418A75	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4083CC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-console-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-datetime-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-debug-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-errorhandling-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-2-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l2-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-handle-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-heap-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-interlocked-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-libraryloader-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-localization-l1-2-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-memory-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-namedpipe-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processenvironment-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-1.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-profile-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-rtlsupport-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-string-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-2-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-sysinfo-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-timezone-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-util-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-conio-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-convert-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-environment-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-filesystem-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-heap-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-locale-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-math-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-multibyte-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-private-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-process-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-runtime-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-stdio-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-string-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-time-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-utility-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\freebl3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\mozglue.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\msvcp140.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\nss3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\nssdbm3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\softokn3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\ucrtbase.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\E0F35830\vcruntime140.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user\AppData\Local\Temp\492576258725572177298999.tmp	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	409678	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\492576258725572177298999.tmp	success or wait	1	4097FD	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-console-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-datetime-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-debug-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-errorhandling-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-2-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l2-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-handle-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-heap-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-interlocked-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-libraryloader-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-localization-l1-2-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-memory-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-namedpipe-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processenvironment-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-1.dll	success or wait	1	4088ED	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-profile-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-rtlsupport-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-string-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-2-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-sysinfo-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-timezone-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-util-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-conio-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-convert-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-environment-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-filesystem-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-heap-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-locale-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-math-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-multibyte-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-private-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-process-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-runtime-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-stdio-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-string-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-time-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-utility-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\freebl3.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\mozglue.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\msvcp140.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\nss3.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\nssdbm3.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\softokn3.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\ucrtbase.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\E0F35830\vcruntime140.dll	success or wait	1	4088ED	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-console-l1-1-0.dll	0	18744	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 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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd fd 22 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL"!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-datetime-l1-1-0.dll	0	18232	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 41 fd 04 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELA!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-debug-l1-1-0.dll	0	18232	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd fd fd 12 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-errorhandling-l1-1-0.dll	0	18232	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 5c 78 fd fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL\x!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-1-0.dll	0	21816	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 14 42 14 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 12 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL!0	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l1-2-0.dll	0	18232	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 15 5f fd 4c 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL_L!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-file-l2-1-0.dll	0	18232	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 34 fd fd 7c 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL4|!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-handle-l1-1-0.dll	0	18232	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd fd 47 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELG!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-heap-l1-1-0.dll	0	18232	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd fd 3a fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL:!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-interlocked-l1-1-0.dll	0	17856	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 24 06 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL$!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-libraryloader-l1-1-0.dll	0	18744	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 75 2a 6c 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELu*l!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-localization-l1-2-0.dll	0	20792	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 53 fd 76 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELSv!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-memory-l1-1-0.dll	0	18744	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 1c fd 25 28 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL%(!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-namedpipe-l1-1-0.dll	0	18232	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 20 17 fd fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL !	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processenvironment-l1-1-0.dll	0	19248	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 29 fd 72 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL)r!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-0.dll	0	19392	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 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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 19 fd fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 0c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-processthreads-l1-1-1.dll	0	18744	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 11 39 fd fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL9!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-profile-l1-1-0.dll	0	17712	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 26 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL&!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-rtlsupport-l1-1-0.dll	0	17720	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 0a fd fd 28 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL(!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-string-l1-1-0.dll	0	18232	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 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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 1e 52 17 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELR!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-1-0.dll	0	20280	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd fd 10 32 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 0c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL2!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-synch-l1-2-0.dll	0	18744	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 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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 58 2a 75 59 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELX*uY!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-sysinfo-l1-1-0.dll	0	19248	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 02 fd 43 3d 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELC=!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-timezone-l1-1-0.dll	0	18224	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 59 fd 78 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELYx!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-core-util-l1-1-0.dll	0	18232	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 03 66 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELf!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-conio-l1-1-0.dll	0	19256	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 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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 0f fd e8 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-convert-l1-1-0.dll	0	22328	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 4e 45 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 14 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELNE!0	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-environment-l1-1-0.dll	0	18736	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 6a 55 04 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELjU!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-filesystem-l1-1-0.dll	0	20280	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd fd fd 68 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 0c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELh!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-heap-l1-1-0.dll	0	19256	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 4a fd 6f 20 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELJo !	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-locale-l1-1-0.dll	0	18744	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 7c 0f fd 4f 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL|O!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-math-l1-1-0.dll	0	28984	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 17 fd 17 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 2e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL!.@	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-multibyte-l1-1-0.dll	0	26424	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 0a 75 27 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 24 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELu'!$@	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-private-l1-1-0.dll	0	73016	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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd fd 5e 31 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 fd 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 fd 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL^1!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-process-l1-1-0.dll	0	19256	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 6c 1a 68 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELlh!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-runtime-l1-1-0.dll	0	22840	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 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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 08 fd 4c 08 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 16 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELL!0	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-stdio-l1-1-0.dll	0	24368	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 1c 09 fd fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 1c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL!0	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-string-l1-1-0.dll	0	23488	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 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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 01 fd fd 53 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 1c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELS!0	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-time-l1-1-0.dll	0	20792	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 fd 4f 49 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePELOI!	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\api-ms-win-crt-utility-l1-1-0.dll	0	18744	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 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 fd 6d 0b fd fd 0c 65 fd fd 0c 65 fd fd 0c 65 fd fd 6e 65 fd fd 0c 65 fd fd 6e 61 fd fd 0c 65 fd fd 6e fd fd fd 0c 65 fd fd 6e 67 fd fd 0c 65 fd 52 69 63 68 fd 0c 65 fd 50 45 00 00 4c 01 02 00 1e 21 35 fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$meeeneenaeneng eRichePEL!5!	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\freebl3.dll	0	332752	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 2f 05 fd fd 41 56 fd fd 41 56 fd fd 41 56 fd fd fd 56 fd fd 41 56 5d fd 40 57 fd fd 41 56 1a 31 fd 56 fd fd 41 56 5d fd 42 57 fd fd 41 56 5d fd 44 57 fd fd 41 56 5d fd 45 57 fd fd 41 56 fd fd 40 57 fd fd 41 56 4f fd 40 57 fd fd 41 56 fd fd 40 56 91 41 56 4f fd 42 57 fd fd 41 56 4f fd 45 57 fd fd 41 56 4f fd 41 57 fd fd 41 56 4f fd 56 fd fd 41 56 4f fd 43 57 fd fd 41	MZ@ !L!This program cannot be run in DOS mode.$/AVAVAVVAV]@ W AV1VAV]BWAV]DWAV]EWAV@WAVO@WAV @VAVOBWAVOEWAVO AWAVOVAVOCWA	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\mozglue.dll	0	139216	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 00 08 01 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 22 79 51 1e 66 18 3f 4d 66 18 3f 4d 66 18 3f 4d 6f 60 fd 4d 76 18 3f 4d fd 7a 3e 4c 62 18 3f 4d fd fd fd 4d 64 18 3f 4d fd 7a 3c 4c 68 18 3f 4d fd 7a 3b 4c 6d 18 3f 4d fd 7a 3a 4c 75 18 3f 4d 44 78 3e 4c 6f 18 3f 4d 66 18 3e 4d fd 18 3f 4d fd 7b 31 4c 75 18 3f 4d fd 7b 3f 4c 67 18 3f 4d fd 7b fd 4d 67 18 3f 4d fd 7b 3d 4c 67 18 3f 4d 52 69 63 68 66 18 3f 4d 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$"yQf?Mf?Mf?Mo`Mv?Mz>Lb?MMd?Mz<Lh?Mz;Lm?Mz:Lu?MDx>Lo?Mf>M?M{1Lu?M{?Lg?M{Mg?M{=Lg?MRichf?M	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\msvcp140.dll	0	440120	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 3c 41 fd fd 12 fd fd 12 fd fd 12 56 35 3d 12 fd fd 12 fd fd 41 12 fd fd fd 12 3b fd fd 13 fd fd 12 fd fd 12 22 fd fd 12 3b fd fd 13 fd fd 12 3b fd fd 13 fd fd 12 3b fd fd 13 fd fd fd 12 3b fd fd 13 fd fd fd 12 3b fd fd 13 fd fd 12 3b fd 2d 12 fd fd 12 3b fd fd 13 fd fd 12 52 69 63 68 fd fd 12 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ@!L!This program cannot be run in DOS mode.$AV5=A;";;;;;-;RichPEL	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\nss3.dll	0	1244112	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 18 01 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 fd fd 0d 78 fd fd 63 2b fd fd 63 2b fd fd 63 2b fd fd fd 2b fd fd 63 2b 2b fd 62 2a fd fd 63 2b 6c 68 fd 2b fd fd 63 2b 2b fd 60 2a fd fd 63 2b 2b fd 66 2a fd fd 63 2b 2b fd 67 2a fd fd 63 2b 28 62 2a fd fd 63 2b 39 fd 62 2a fd fd 63 2b fd fd 62 2b 04 fd 63 2b 39 fd 6b 2a fd fd 63 2b 39 fd 67 2a 43 fd 63 2b 39 fd 63 2a fd fd 63 2b 39 fd fd 2b fd fd 63 2b 39 fd 61 2a fd fd 63	MZ@!L!This program cannot be run in DOS mode.$xc+c+c++c++b*c+lh+c++`*c++f*c++g*c+b*c+9b*c+ b+c+9k*c+9g*Cc+9c*c+9+c+9a*c	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\nssdbm3.dll	0	92624	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1d fd 5a fd 59 fd 34 fd 59 fd 34 fd 59 fd 34 fd 50 fd fd fd 55 fd 34 fd fd fd 35 fd 5b fd 34 fd fd 79 fd 51 fd 34 fd fd fd 37 fd 58 fd 34 fd fd fd 31 fd 53 fd 34 fd fd fd 30 fd 52 fd 34 fd 7b fd 35 fd 5b fd 34 fd fd fd 35 fd 5a fd 34 fd 59 fd 35 fd fd fd 34 fd fd fd 30 fd 41 fd 34 fd fd fd 34 fd 58 fd 34 fd fd fd e3 58 fd 34 fd fd fd 36 fd 58 fd 34 fd 52 69 63 68 59 fd 34	MZ@!L!This program cannot be run in DOS mode.$ZY4Y4Y4PU45[4y Q47X41S40R4{5[45Z4Y540A44X4X46X4RichY4	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\softokn3.dll	0	144336	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 00 01 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 fd 6c 24 1c fd 0d 4a 4f fd 0d 4a 4f fd 0d 4a 4f fd 75 fd 4f fd 0d 4a 4f 3f 6f 4b 4e fd 0d 4a 4f 3f 6f 49 4e fd 0d 4a 4f 3f 6f 4f 4e fd 0d 4a 4f 3f 6f 4e 4e fd 0d 4a 4f fd 6d 4b 4e fd 0d 4a 4f 2d 6e 4b 4e fd 0d 4a 4f fd 0d 4b 4f 7e 0d 4a 4f 2d 6e 4e 4e fd 0d 4a 4f 2d 6e 4a 4e fd 0d 4a 4f 2d 6e fd 4f fd 0d 4a 4f 2d 6e 48 4e fd 0d 4a 4f 52 69 63 68 fd 0d 4a 4f 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.lJOJOJOuOJO?oKNJO?oINJO?oONJO?oNNJOmKNJO-nKNJOKO~JO-nNNJO-nJNJO-nOJO-nHNJORichJO	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\E0F35830\ucrtbase.dll	0	1142072	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 00 01 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 fd d2 45 fd fd fd 16 fd fd fd 16 fd fd fd 16 fd fd 6f 16 fe fd 16 fd fd fd 16 70 fd fd 16 fd fd 01 16 fd fd fd 16 fd fd fd 17 fd fd 16 fd fd fd 17 fd fd fd 16 fd fd fd 17 fd fd fd 16 fd fd fd 17 fd fd fd 16 fd fd fd 17 fd fd fd 16 fd fd 03 16 fd fd fd 16 fd fd fd 17 fd fd fd 16 52 69 63 68 fd fd fd 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$EopRich	success or wait	1	40730C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E0F35830\vcruntime140.dll	0	83784	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 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 01 fd fd 4e 45 fd fd 1d 45 fd fd 1d 45 fd fd 1d fd 04 22 1d 47 fd fd 1d 4c fd 5e 1d 4e fd fd 1d 45 fd fd 1d 6c fd fd 1d fd fd fd 1c 55 fd fd 1d fd fd fd 1c 56 fd fd 1d fd fd fd 1c 41 fd fd 1d fd fd fd 1c 5f fd fd 1d fd fd fd 1c 44 fd fd 1d fd fd 32 1d 44 fd fd 1d fd fd fd 1c 44 fd fd 1d 52 69 63 68 45 fd fd 1d 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0c 38 27 59 00 00 00	MZ@!L!This program cannot be run in DOS mode.$NEEE"GL^NElUVA_D2DDRichEPEL8'Y	success or wait	1	40730C	WriteFile
C:\Users\user\AppData\Local\Temp\4925762587255721772989999.tmp	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 16 00 00 00 07 00 00 00 02 00 00 00 10 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 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .S`	success or wait	1	409678	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BUFZSQPCOH.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\BWDRWEEARI.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\BWDRWEEARI.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\GNLQNHOLWB.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\UBVUNTSCZJ.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\WHZAGPPPLA.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\GNLQNHOLWB\BWDRWEEARI.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\GNLQNHOLWB\GNLQNHOLWB.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\BWDRWEEARI\BWDRWEEARI.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\BWDRWEEARI\UBVUNTSCZJ.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\BUFZSQPCOH\BUFZSQPCOH.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\BUFZSQPCOH\WHZAGPPPLA.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BUFZSQPCOH.docx	unknown	1026	success or wait	1	407248	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BWDRWEEARI.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BWDRWEEARI.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\GNLQNHOLWB.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\UBVUNTSCZJ.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\WHZAGPPPLA.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\GNLQNHOLWB\BWDRWEEARI.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\GNLQNHOLWB\GNLQNHOLWB.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BWDRWEEARI\BWDRWEEARI.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BWDRWEEARI\UBVUNTSCZJ.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BUFZSQPCOH\BUFZSQPCOH.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BUFZSQPCOH\WHZAGPPPLA.xlsx	unknown	1026	success or wait	1	407248	ReadFile

Analysis Process: cmd.exe PID: **6040**, Parent PID: **3172**

General

Target ID:	5
Start time:	12:47:10
Start date:	28/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe" /c C:\Windows\system32\timeout.exe 3 & del "Swift Mesaj#U0131#09971.exe
Imagebase:	0x210000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe	cannot delete	1	230975	DeleteFileW
C:\Users\user\Desktop\Swift Mesaj#U0131#09971.exe	cannot delete	1	230975	DeleteFileW

Analysis Process: conhost.exe PID: **4920**, Parent PID: **6040**

General

Target ID:	6
Start time:	12:47:10
Start date:	28/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff782ea0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: **8964**, Parent PID: **6040**

General

Target ID:	7
Start time:	12:47:11
Start date:	28/11/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\timeout.exe 3
Imagebase:	0xa20000
File size:	25088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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