ID: 384212
Sample Name: SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
Cookbook: default.jbs
Time: 18:45:12
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

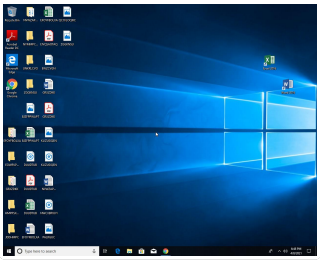
Analysis Report SOLICITUD DE PRESUPUESTO 08-04-2…

Overview

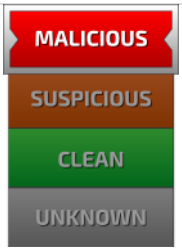
General Information

Sample Name:	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
Analysis ID:	384212
MD5:	ac6576aa4888bb..
SHA1:	e61899b32566e2..
SHA256:	7c90ae17ff566ca..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



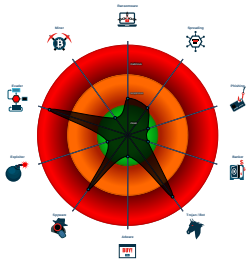
GuLoader Raccoon

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Yara detected GuLoader
- Yara detected Raccoon Stealer
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fil…
- Yara detected VB6 Downloader Gen…

Classification



Startup

- **System is w10x64**
- SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe (PID: 1688 cmdline: 'C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe' MD5: AC6576AA4888BBBB8BD2598E75F8B6D1)
  - SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe (PID: 4516 cmdline: 'C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe' MD5: AC6576AA4888BBBB8BD2598E75F8B6D1)
    - cmd.exe (PID: 6740 cmdline: cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q 'C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 6776 cmdline: timeout /T 10 /NOBREAK MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- **cleanup**

Malware Configuration

Threatname: Raccoon Stealer

```
{
  "Config: ": [
    "00000000 -> Raccoon | 1.7.3",
    "Build compile date: Sat Feb 27 21:25:06 2021",
    "Launched at: 2021.04.09 - 01:46:41 GMT",
    "Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A_user",
    "Running on a desktop",
    "-------------",
    "- Cookies: 1",
    "- Passwords: 0",
    "- Files: 0",
    "System Information:",
    "- System Language: English",
    "- System TimeZone: -8 hrs",
    "- IP: 185.32.222.8",
    "- Location: 47.431301, 8.562700 | Glattbrugg, Zurich, Switzerland (8152)",
    "- ComputerName: 123716",
    "- Username: user",
    "- Windows version: NT 10.0",
    "- Product name: Windows 10 Pro",
    "- System arch: x64",
    "- CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz (4 cores)",
    "- RAM: 8191 MB (8125 MB used)",
    "- Screen resolution: 1280x1024",
    "- Display devices:",
    "0) Microsoft Basic Display Adapter",
    "-------------",
    "Installed Apps:",
    "Adobe Acrobat Reader DC (19.012.20035)",
    "Google Chrome (85.0.4183.121)",
    "Google Update Helper (1.3.35.451)",
    "Java 8 Update 211 (8.0.2110.12)",
    "Java Auto Updater (2.8.211.12)",
    "Update for Skype for Business 2016 (KB4484286) 32-Bit Edition",
    "-------------"
  ]
}
```


Yara Overview

Memory Dumps

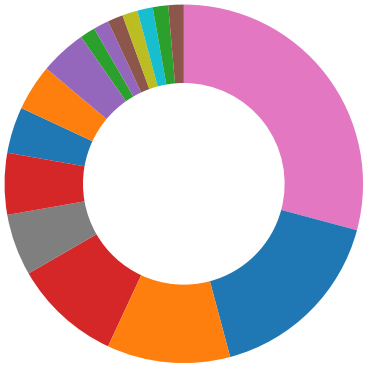
Source	Rule	Description	Author	Strings
00000002.00000002.313364575.000000000056 1000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe PID: 4516	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe PID: 4516	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
Process Memory Space: SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe PID: 4516	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe PID: 1688	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing



- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Yara detected Raccoon Stealer

E-Banking Fraud:

- Yara detected Raccoon Stealer

Data Obfuscation:

- Yara detected GuLoader
- Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

- Contains functionality to detect hardware virtualization (CPUID execution measurement)
- Detected RDTSC dummy instruction sequence (likely for instruction hammering)
- Tries to detect Any.run
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

- Contains functionality to hide a thread from the debugger
- Hides threads from debuggers

Stealing of Sensitive Information:

- Yara detected Raccoon Stealer
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Mail credentials (via file access)

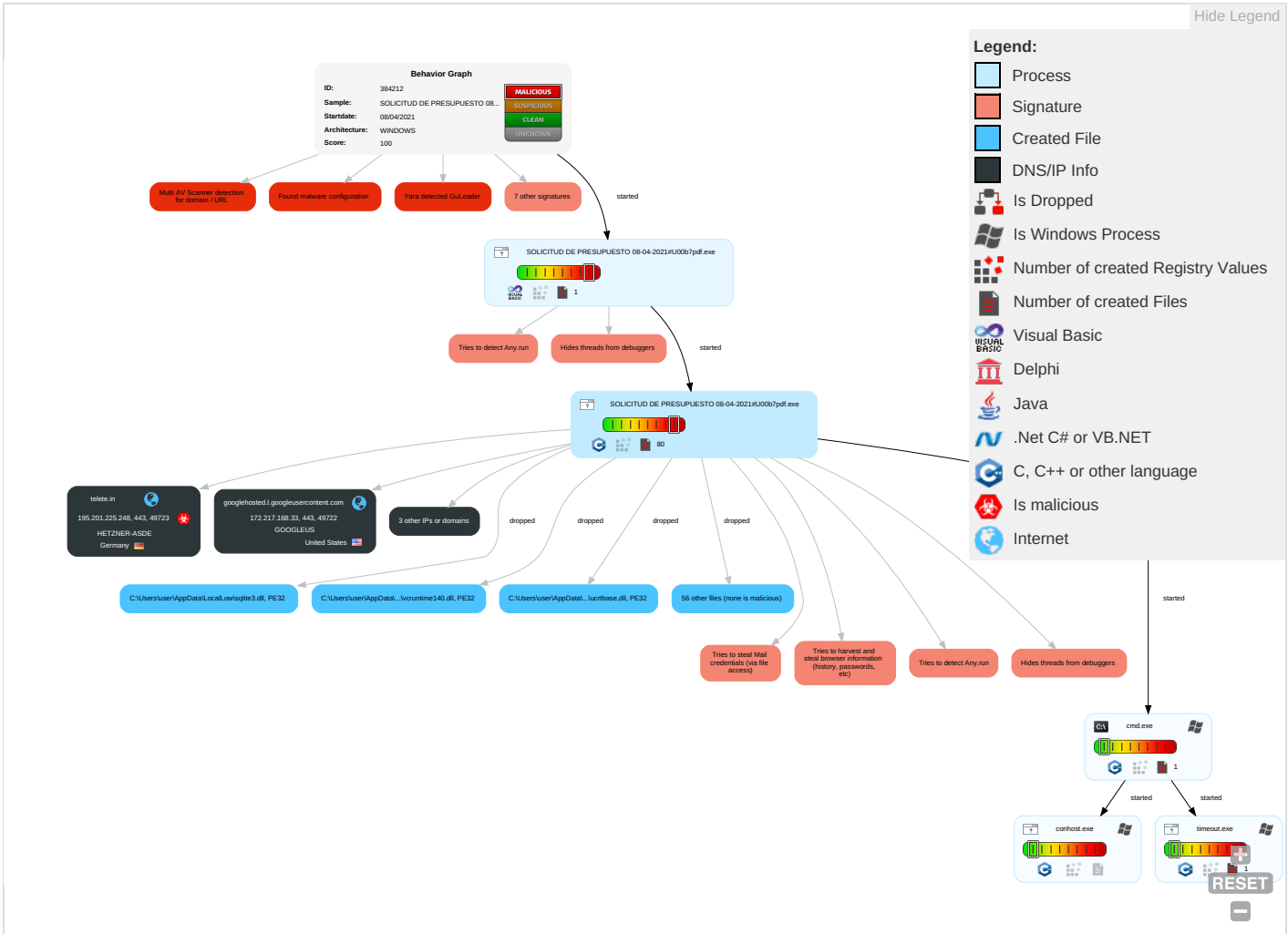
Remote Access Functionality:

- Yara detected Raccoon Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Security Software Discovery 7 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Application Layer Protocol 2	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Virtualization/Sandbox Evasion 2 2	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3 3 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po

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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	0%	Virustotal		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	3%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
shehootastayonwhatshelirned.top	0%	Virustotal		Browse
telete.in	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://https://shehootastayonwhatshelirned.top/	1%	Virustotal		Browse
http://https://shehootastayonwhatshelirned.top/	0%	Avira URL Cloud	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel05	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel05	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel05	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel05	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shehootastayonwhatshelirned.top	5.230.68.40	true	false	• 0%, Virustotal, Browse	unknown
telete.in	195.201.225.248	true	true	• 11%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
doc-0o-7g-docs.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe, 00000002.00000003.302815241.000000001E191000.00000004.00000001.sdmp, RYwTiizs2t.2.dr	false		high
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.mozilla.com/en-US/blocklist/	mozglue.dll.2.dr	false		high
http://https://duckduckgo.com/ac/?q=	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe, 00000002.00000003.302815241.000000001E191000.00000004.00000001.sdmp, RYwTiizs2t.2.dr	false		high
http://crl.chambersign.org/chambersroot.crl0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es/legislacion_c.htm0U	nssckbi.dll.2.dr	false		high
http://www.certicamara.com/dpc/0Z	nssckbi.dll.2.dr	false		high
http://https://repository.luxtrust.lu0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.accv.es0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.thawte.com0	nss3.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.mozilla.com0	nss3.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.chambersign.org1	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe, 00000002.00000003.302815241.000000001E191000.00000004.00000001.sdmp, RYwTiizs2t.2.dr	false		high
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com/cps0	nssckbi.dll.2.dr	false		high
http://www.diginotar.nl/cps/pkioverheid0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	nssckbi.dll.2.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe, 00000002.00000003.302815241.000000001E191000.00000004.00000001.sdmp, RYwTiizs2t.2.dr	false		high
http://crl.securetrust.com/SGCA.crl0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe, 00000002.00000003.302815241.000000001E191000.00000004.00000001.sdmp, RYwTiizs2t.2.dr	false		high
http://https://shehootastayonwhatshelirned.top/	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe, 00000002.00000002.313628670.000000000090E000.00000004.00000020.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.catcert.net/verarrel	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	nss3.dll.2.dr	false		high
http://www.certplus.com/CRL/class2.crl0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	nssckbi.dll.2.dr	false		high
http://www.quovadisglobal.com/cps0	nssckbi.dll.2.dr	false		high
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl0	nssckbi.dll.2.dr	false		high
http://crl.chambersign.org/chambersignroot.crl0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.catcert.net/verarrel05	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es00	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ocsp.quovadisoffshore.com0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pkioverheid.nl/policies/root-policy-G20	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cert.fnmt.es/dpcs/0	nssckbi.dll.2.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe, 00000002.00000003.302815241.000000001E191000.00000004.00000001.sdmp, RYwTiizs2t.2.dr	false		high
http://cps.chambersign.org/cps/chambersignroot.html0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sqlite.org/copyright.html.	sqlite3.dll.2.dr	false		high
http://policy.camerfirma.com0	nssckbi.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe, 00000002.00000003.302815241.000000001E191000.00000004.00000001.sdmp, RYwTiizs2t.2.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.230.68.40	shehootastayonwhatshelirned.top	Germany		12586	ASGHOSTNETDE	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
195.201.225.248	telete.in	Germany		24940	HETZNER-ASDE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384212
Start date:	08.04.2021
Start time:	18:45:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
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.troj.spyw.evad.winEXE@8/67@3/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 82.9% (good quality ratio 69.7%) • Quality average: 63.6% • Quality standard deviation: 36%
HCA Information:	• Successful, ratio: 79% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 204.79.197.200, 13.107.21.200, 104.43.139.144, 168.61.161.212, 13.107.5.88, 13.107.42.23, 95.100.54.203, 172.217.168.14, 20.82.209.183, 23.10.249.26, 23.10.249.43, 8.241.89.254, 8.238.28.126, 8.238.35.254, 8.241.88.254, 8.241.78.126, 20.54.26.129 • Excluded domains from analysis (whitelisted): client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, arc.msn.com.nsatc.net, config.edge.skype.com.trafficmanager.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, l-0014.config.skype.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, drive.google.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, au-bg-shim.trafficmanager.net, www.bing.com, afdo-tas-offload.trafficmanager.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, l-0014.l-msedge.net • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.201.225.248	http://telete.in	Get hash	malicious	Browse	• telete.in/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
telete.in	vgUgvbLjyI.exe	Get hash	malicious	Browse	• 195.201.225.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.W32.AIDetect.malware2.22480.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.16239.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.23167.exe	Get hash	malicious	Browse	• 195.201.225.248
	40JHtWiswn.exe	Get hash	malicious	Browse	• 195.201.225.248
	hGnoFRUIBe.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.7401.exe	Get hash	malicious	Browse	• 195.201.225.248
	SWKp7KyFtP.exe	Get hash	malicious	Browse	• 195.201.225.248
	C6vcYLfTa9.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.21202.exe	Get hash	malicious	Browse	• 195.201.225.248
	EBjyq0UYDN.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.10758.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.25113.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.1450.exe	Get hash	malicious	Browse	• 195.201.225.248
	OektZ8OQ0h.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.Trojan.GenericKD.46018620.1609.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.Trojan.Siggen13.1734.14778.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.Trojan.GenericKD.36625148.3633.exe	Get hash	malicious	Browse	• 195.201.225.248
	L87N50MbDG.exe	Get hash	malicious	Browse	• 195.201.225.248
	o1wxaQ9Fwh.exe	Get hash	malicious	Browse	• 195.201.225.248

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	Fax-Message-4564259.html	Get hash	malicious	Browse	• 46.4.41.213
	XN123gfQJQ.exe	Get hash	malicious	Browse	• 88.99.66.31
	PI-SO-P1010922.exe	Get hash	malicious	Browse	• 176.9.182.156
	SecuriteInfo.com.Trojan.PWS.Siggen2.64388.32153.exe	Get hash	malicious	Browse	• 88.99.66.31
	Three.exe	Get hash	malicious	Browse	• 94.130.198.87
	Four.exe	Get hash	malicious	Browse	• 136.243.150.2
	frox0cheats.exe	Get hash	malicious	Browse	• 168.119.38.182
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 144.76.207.76
	1wOdXavtlE.exe	Get hash	malicious	Browse	• 88.99.66.31
	eQLPRPErea.exe	Get hash	malicious	Browse	• 135.181.58.27
	vbc.exe	Get hash	malicious	Browse	• 195.201.179.80
	vgUgvbLjyI.exe	Get hash	malicious	Browse	• 195.201.225.248
	Rechnung.doc	Get hash	malicious	Browse	• 46.4.51.158
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.W32.AIDetect.malware2.22480.exe	Get hash	malicious	Browse	• 195.201.225.248
	Revised Invoice No CU 7035.exe	Get hash	malicious	Browse	• 78.46.133.81
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 88.99.66.31
	V7UnYc7CCN.exe	Get hash	malicious	Browse	• 88.99.66.31
	uTQdPoKj0h.exe	Get hash	malicious	Browse	• 95.217.123.103
	uTQdPoKj0h.exe	Get hash	malicious	Browse	• 95.217.123.103
ASGHOSTNETDE	purchase order.doc	Get hash	malicious	Browse	• 5.230.28.5
	purchase order.doc	Get hash	malicious	Browse	• 5.230.28.5
	purchase order.doc	Get hash	malicious	Browse	• 5.230.28.5
	svchost.exe	Get hash	malicious	Browse	• 89.144.1.26
	sP6iCH7OJG.exe	Get hash	malicious	Browse	• 85.93.0.136
	NVoSfVRQVy.exe	Get hash	malicious	Browse	• 85.93.1.64

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	purchase order.doc	Get hash	malicious	Browse	• 5.230.28.211
	Construction_Rondeau.doc	Get hash	malicious	Browse	• 193.187.173.215
	Construction_Rondeau.doc	Get hash	malicious	Browse	• 193.187.173.215
	Construction_Rondeau.doc	Get hash	malicious	Browse	• 193.187.173.215
	OriGene_Technologies.doc	Get hash	malicious	Browse	• 193.187.173.215
	SigLaw.doc	Get hash	malicious	Browse	• 193.187.173.215
	Phoenix_Theatres.doc	Get hash	malicious	Browse	• 193.187.173.215
	receipt_FedEX_4028893.doc	Get hash	malicious	Browse	• 193.187.172.42
	receipt_FedEX_4028893.doc	Get hash	malicious	Browse	• 193.187.172.42
	ShipmentInfoUSPS_18557704.doc	Get hash	malicious	Browse	• 193.187.172.42
	ShipmentInfoUSPS_18557704.doc	Get hash	malicious	Browse	• 193.187.172.42
	430#U0437.js	Get hash	malicious	Browse	• 85.93.16.47
	droppe.exe	Get hash	malicious	Browse	• 193.24.209.70
	BK.485799485.jse	Get hash	malicious	Browse	• 193.24.209.70

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	vgUgvbLjyI.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware2.22480.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.16239.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.23167.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	agmz0F8LbA.dll	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	aunobp.dll	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	40JHtWiswn.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	q6W61jpqPB.doc	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	TlUrqQBd4Y.xlsm	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	ofcRreui1e.dll	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	hostsvc.dll	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	sample.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	f6a1vvMXQa.dll	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	hGnoFRUIBe.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	Reports-018315.xlsm	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	Invoice__7477.xlsm	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.7401.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.225.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	44285,5327891204.dll	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.22 5.248
	SWKp7KyFtP.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.22 5.248
	C6vcYLfTa9.exe	Get hash	malicious	Browse	• 5.230.68.40 • 195.201.22 5.248
37f463bf4616ecd445d4a1937da06e19	XN123gfQJQ.exe	Get hash	malicious	Browse	• 172.217.168.33
	documento.xlsb	Get hash	malicious	Browse	• 172.217.168.33
	securedmessage.htm	Get hash	malicious	Browse	• 172.217.168.33
	Smart wireless request.xlsb	Get hash	malicious	Browse	• 172.217.168.33
	SecuriteInfo.com.Trojan.PWS.Siggen2.64388.32153.exe	Get hash	malicious	Browse	• 172.217.168.33
	BB44.vbs	Get hash	malicious	Browse	• 172.217.168.33
	BrgW593cHH.exe	Get hash	malicious	Browse	• 172.217.168.33
	BrgW593cHH.exe	Get hash	malicious	Browse	• 172.217.168.33
	FAKTURA I RACHUNKI.exe	Get hash	malicious	Browse	• 172.217.168.33
	WDnE51mua6.exe	Get hash	malicious	Browse	• 172.217.168.33
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 172.217.168.33
	V7UnYc7CCN.exe	Get hash	malicious	Browse	• 172.217.168.33
	SM25.vbs	Get hash	malicious	Browse	• 172.217.168.33
	FQ45.vbs	Get hash	malicious	Browse	• 172.217.168.33
	Signed pages of agreement copy.html	Get hash	malicious	Browse	• 172.217.168.33
	Payment Report.html	Get hash	malicious	Browse	• 172.217.168.33
	dMeVLLeyLc.exe	Get hash	malicious	Browse	• 172.217.168.33
	avast_secure_browser_setup.exe	Get hash	malicious	Browse	• 172.217.168.33
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 172.217.168.33
	57fvgYpwnN.exe	Get hash	malicious	Browse	• 172.217.168.33

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	vgUgvbLjyI.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware2.22480.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.16239.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.23167.exe	Get hash	malicious	Browse	
	40JHtWiswn.exe	Get hash	malicious	Browse	
	hGnoFRUIBe.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.7401.exe	Get hash	malicious	Browse	
	SWKp7KyFtP.exe	Get hash	malicious	Browse	
	C6vcYLfTa9.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.21202.exe	Get hash	malicious	Browse	
	EBjyq0UYDN.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.10758.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.25113.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.1450.exe	Get hash	malicious	Browse	
	OektZ8OQ0h.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.46018620.1609.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Siggen13.1734.14778.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.36625148.3633.exe	Get hash	malicious	Browse	
	L87N50MbDG.exe	Get hash	malicious	Browse	
	o1wxaQ9Fwh.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\M8gHzW2avYe.zip	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1181
Entropy (8bit):	7.513642713430229
Encrypted:	false
SSDEEP:	24:9sTzXB1YPVlMnyPmE0ABMNN/fnZkzHwlMPeDd4a:9sTT0VlMkbBM3fSri4eDd4a
MD5:	674BB63E297AF95B7813733340B3C5F6
SHA1:	36E5B0766F104981742534ADF2EA531FCC4669FC
SHA-256:	DAF40C4304B64351F2210695B1057A155EF0DE7F04A168BEC3D21B221C4F1514
SHA-512:	E16B89563858D91A909689AB70AD6BFDF2B6116E038DEA99D1F297B5DA15F59933AA2E8B4CA889BCE388A9C8448FC454471CDDAD9A2D8CBB2E7E66BB586B8(41
Malicious:	false
Reputation:	low
Preview:	PK.....R..c.....*...browsers/cookies/Google Chrome_Default.txtUT....Oo`.Oo`.Oo`%.r.0.....Q.....V.!...H.^Jj..0.V..;.[..2F.?...N..y...<.0..;.y..F/..V.8NvZ._..m;f.{H.....].|.[...R.. ...../...J:I.. I/...Cgv..!.LQ...n.....n.SY.B.xSTm2..e_...f)...p..St.C...I..AQe.n..k...PK.....R.G\.....8.....System Info.txtUT....Oo`.Oo`.Oo`uSMO.0.=...a..D-..h....KQ.....i-R;....?~ '4a.@.....x-.....!.....kU...c.J...2...0.;.C.,.QJc..3._.Z..Y...;FhH...@Y..i.`..6..._MS..x6..h.'.x..F.`.E.A..F.h....^..F;.Z.Z+..,Q@!.7.....x..G%]...V.gc..h.....yy.+.`.Qxet.....Z.....(... ..um.j.5$..8....M~:..!...Pv...b>...aQ..w.../.*?\..Y.7iK...%,...f.U..G<..`..6t.....G..<;x..Wq..FI.....=.2;2.M.k....^.+eu...^..u.....].y.C.ck?.....z!...kc.-SH..r.4.fS;Yt.Mn..9..O.1...FyW. T....8$O*..E...a.rk.y.0.N.....:..,]i.EY.`gU....e..I.Pp..b-E!-L'.c#B..3.A.|.0f..gr..(...P..$ ....y`p)...z..$.H..H....#q.P..pCQ.?%..iY(...P:F.....Ni...X.C..8...'q..>.+..B56.k.?PK.....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123344
Entropy (8bit):	6.504957642040826
Encrypted:	false
SSDEEP:	1536:DkO/6RZFrpiS7ewflNGa35iOrjmwWTYP1KxBxZJByEJMBrsuLeLsWxcdaocACs0K:biRZFdBiussQ1MBjq2aocts03/7FE
MD5:	F92586E9CC1F12223B7EEB1A8CD4323C
SHA1:	F5EB4AB2508F27613F4D85D798FA793BB0BD04B0
SHA-256:	A1A2BB03A7CFCEA8944845A8FC12974482F44B44FD20BE73298FFD630F65D8D0
SHA-512:	5C047AB885A8ACCB604E58C1806C82474DC43E1F997B267F90C68A078CB63EE78A93D1496E6DD4F5A72FDF246F40EF19CE5CA0D0296BBCFCFA964E4921E68AF
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: vgUgvbLjyI.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware2.22480.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.16239.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.23167.exe, Detection: malicious, Browse • Filename: 40JHtWiswn.exe, Detection: malicious, Browse • Filename: hGnoFRUIBe.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.7401.exe, Detection: malicious, Browse • Filename: SWKp7KyFtP.exe, Detection: malicious, Browse • Filename: C6vcYLfTa9.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.21202.exe, Detection: malicious, Browse • Filename: EBjyq0UYDN.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.10758.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.25113.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.1450.exe, Detection: malicious, Browse • Filename: OektZ8OQ0h.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.46018620.1609.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Siggen13.1734.14778.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.36625148.3633.exe, Detection: malicious, Browse • Filename: L87N50MbDG.exe, Detection: malicious, Browse • Filename: o1wxaQ9Fwh.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.Z.....x.....x.....x.....=z.....=z.....=z.....x.....x.....z.../{.....}/{...../{.....}/{b...../{.....Rich.....PE..L...C@.\.....''!.....b.....0.....~p....@.....p.....h.....0...T.....@.....0..$.....text...7..... ..`.orpc..... ..... ..`.rdata...y...0...z.....@..@.data.....@....rsrc...h.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26064
Entropy (8bit):	5.981632010321345
Encrypted:	false
SSDEEP:	384:KuAjyb0Xc6JzVuLoW2XDOc3TXg1hjsvDG8A3OPLon07zS:BEygs6RV6oW2Xd38njiDG8Mj
MD5:	A7FABF3DCE008915CEE4FFC338FA1CE6
SHA1:	F411FB41181C79FBA0516D5674D07444E98E7C92
SHA-256:	D368EB240106F87188C4F2AE30DB793A2D250D9344F0E0267D4F6A58E68152AD
SHA-512:	3D2935D02D1A2756AAD7060C47DC7CABBA820CC9977957605CE9BBB44222289CBC451AD331F408317CF01A1A4D3CF8D9CFC666C4E6B4DB9DDD404C7629CEA70
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....U...U...U...U...U..T...U..T...U..T...U..T...U5.T...U...U!..U..T.. .U..T...U...U...U..T...URich...U.....PE..L...<@.\....."!.....8.....0.....0.....7....@.....=.....0>..x...`.....H.....<...09..T..... .....9..@.....0.....text...f..... ..`.orpc..... ....`.rdata.....0.....@..@.data...@....P.....(.....@....rsrc.....`.....* .....@..@.reloc..<.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	70608
Entropy (8bit):	5.389701090881864
Encrypted:	false
SSDEEP:	768:3n8PHF564hn4wva3AVqH5PmE0SjA6QM0avrDG8MR43:38th4wvaQVE5PRl0xs
MD5:	5243F66EF4595D9D8902069EED8777E2
SHA1:	1FB7F82CD5F1376C5378CD88F853727AB1CC439E
SHA-256:	621F38BD19F62C9CE6826D492ECDF710C00BBDCF1FB4E4815883F29F1431DFDA
SHA-512:	A6AB96D73E326C7EEF75560907571AE9CAA70BA9614EB56284B863503AF53C78B991B809C0C8BAE3BCE99142018F59D42DD4BCD41376D0A30D9932BCFCAEE5A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....K...K...K.g.K...K4}.J...K4}.J...K4}.J...K4}.J...K...J...K...J...K ...K...K&|.J...K&|.J...K&|uK...K&|.J...KRich...K.....PE..L...J@.\....."!.....$.....0.....0.....@.....0z.....z.....v..... .....u..T. .....Hv..@.....0.....orpc...t..... ..`.text..... ..... ..`.rdata...Q...0...R.....@..@.data.....j.....@....rsrc. ...v.....x...t.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X.....PE..L....=.\....."!.....@.....0.....@.....0:.....:..d...`..p.....0.....p.....5..T..... .....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r...0.....@..@.data.....P.....&.....@....rsrc... p....`.....(.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...;...X...;&..X...;...X..Rich.X.....PE..L....=.\....."!.....@.....0.....@.....0:.....:..d....`..p.....0.....p.....5..T.....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc...p....`.....(.....@..@.reloc.....p.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:IWPhWlsnhi00GftpBjnem9lD16PamFP
MD5:	E2F648AE40D234A3892E1455B4DBBE05
SHA1:	D9D750E828B629CFB7B402A3442947545D8D781B
SHA-256:	C8C499B012D0D63B7AFC8B4CA42D6D996B2FCF2E8B5F94CACFBEC9E6F33E8A03
SHA-512:	18D4E7A804813D9376427E12DAA444167129277E5FF30502A0FA29A96884BF902B43A5F0E6841EA1582981971843A4F7F928F8AECAC693904AB20CA40EE4E954
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...._.L.....!..... .....0.....@.....L..... .....8=.....T.....text...<..... ....`.rsrc..... .....@..@...._.L.....8...T...T....._.L.....d....._.L.....RSDS.....g"Y.....api-ms-win-core-file-l1-2-0.pdb.....T....rdata..T..... rdata$zzzdbg.....L....edata... ..`....rsrc$01....` .....rsrc$02....._.L....@.....(...8...l.....`.....api-ms-win-core-file-l1-2-0.dll.CreateFile2.kernel32.CreateFile2.GetTempPathW.kernel32.GetTempPathW.GetVolumeNameForVolumeMountPointW.kernel32.GetVolumeNameForVolumeMou

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...4..|.....!.. ....0.....t.....@..... .....8=.....T.....text...}..... . .`.rsrc..... .....@..@....4..|.....8...T...T.....4..|.....d.....4..|.....RSDS.=.Co.P..Gd./%P....api-ms-win-core-file-l2-1-0.pdb.....T....rdata..T..... rdata$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\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	AA6F0BCB760D449A3A82AED67CA0F7FB747CBB82E627210F377AF74E0B43A45BA660E9E3FE1AD4CBD2B46B1127108EC4A96C5CF9DE1BDEC36E993D0657A615B6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....G..... .....!..... ....0.....V.....@..... ....8=.....T.....text...._..... ....`.rsrc..... .....@..@.....G.....:...T...T.....G.....d.....G.....RSDSQ..{...IS].0.> ....api-ms-win-core-handle-l1-1-0.pdb.....T....rdata. .T.....rdata$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\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....:.....!.. ....0.....@..... ....8=.....T.....text..... . .`.rsrc..... .....@..@.....:.....8...T...T.....:.....d.....:.....RSDS.K....OB;....X.....api-ms-win-core-heap-l1-1-0.pdb.....T....rdata..T..... .rdata$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\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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: Metadefender, Detection: 0%, Browse • 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.....@..... ....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\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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 7
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u*l.....!.. ....0.....9.....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....u*l.....A...T...T.....u*l.....d.....u*l.....RSDSU..e.j.(.wD.....api-ms-win-core-libraryloader-l1-1-0.pdb.....T....rdata ..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....u*l.....(...p.....R...}.....*...Y.....8..._.....B...k.....F... u.....)...P...w.....api-ms-win-c

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-localization-l1-2-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...S.v..... .....I..... ....0.....@..... ....8=.....T..... .....text..... ....`.rsrc..... .....@..@....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T. ...rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....S.v.....v.....;...;...(.....<...f.....5...]..... .....!...I...q..... N.....)...j.....)...^.....)...\.....8...`.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-memory-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....%(.... .....I..... ....0.....@..... .....I..... ....8=.....T..... .....text...I..... ....`.rsrc..... .....@..@.....%(.....:...T...T.....%(.....d.....%(.....RSDS.~....%.T.....CO....api-ms-win-core-memory-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....I....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\LocalLow\gC9tT2iQ3s\api-ms-win-core-namedpipe-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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 B
Malicious:	false
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-ms-win-core-namedpipe-l1-1-0.dll.ConnectNamedPipe.kernel32.ConnectNamedPipe.CreateNamedP

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	
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 ED
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...).r.....!.. ....0.....`....@.....G..... .....0=.....T.....text...G..... . .`.rsrc..... .....@..@....).r.....F...T...T.....).r.....d.....).r.....RSDS.6..~x.....'.....api-ms-win-core-processenvironment-l1-1-0.pdb.....T... .rdata..T.....rdata$zzzdbg.....G....edata... ..`....rsrc$01....` .....rsrc$02.....).r.....(...|.....B.....$...M...{.....P.....6...k...../...(...e..... ..=...f.....8...q.....!...T..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	D436B2192C4392A041E20506B2DFB593FE5797F1FDC2CDEB2D7958832C4C0A9E00D3AEA6AA1737D8A9773817FEADF47EE826A6B05FD75AB0BDAE984895C2C4 EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....l.....@..... .....9.....T.....text..... . .`.rsrc..... .....@..@.....B...T...T.....d.....RSDS..t.....=j.....api-ms-win-core-processthreads-l1-1-0.pdb.....T....rda ta..T.....rdata$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\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-1.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	97C47B2E1BFD45B905F51A282683434ED784BFB334B908BF5A47285F90201A23817FF91E21EA0B9CA5F6EE6B69ACAC252EEC55D895F942A94EDD88C4BFD2DA D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....9.....!.. ....0.....k.....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.....9.....B...T...T.....9.....d.....9.....RSDS&.n....5..l....)....api-ms-win-core-processthreads-l1-1-1.pdb.....T....rda ta..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....9.....(..`.....-...l.....".W.....N.....P.....F...q.....3. ..r.....api-ms-win-core-processthreads-l1-1-1.dll.FlushInstr

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	
MD5:	FEE0926AA1BF00F2BEC9DA5DB7B2DE56
SHA1:	F5A4EB3D8AC8FB68AF716857629A43CD6BE63473
SHA-256:	8EB5270FA99069709C846DB38BE743A1A80A42AA1A88776131F79E1D07CC411C
SHA-512:	0958759A1C4A4126F80AA5CDD9DF0E18504198AEC6828C8CE8EB5F615AD33BF7EF0231B509ED6FD1304EEAB32878C5A649881901ABD26D05FD686F5EBEF2D13
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....&.....!.....0.....0.....@.....0=.....T.....text..... ..`.rsrc..... .....@..@.....&.....;...T...T.....&.....d.....&.....RSDS...O.""#.n....D:....api-ms-win-core-profile-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....&.....<.....(...0...8...w.....`_.....api-ms-win-core-profile-l1-1-0.dll.QueryPerformanceCounter.kernel32.QueryPerformanceCounter.QueryPerformanceFrequency.kernel32.QueryPerformanceFrequency.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-rtlsupport-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
Malicious:	false
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.RtlCaptureContext.ntdll.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind.

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	F62303D98EA7D0DDBE78E4AB4DB31AC283C3A6F56DBE5E3640CBCF8C06353A37776BF914CFE57BBB77FC94CCFA48FAC06E74E27A4333FBDD112554C64683829
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....R.....l.....0.....\....@.....8=.....T.....text..... ..`.rsrc..... .....@..@.....R.....:...T...T.....R.....d.....R.....RSDS..D..a..1.f....7....api-ms-win-core-string-l1-1-0.pdb.....T....rdata..T.....rdata$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\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	7EC2E0FEBC89263925C0352A2DE8CC13DA37172555C3AF9869F9DBB3D627DD1382D2ED3FDAD90594B3E3B0733F2D3CFDEC45BC713A4B7E85A09C164C3DFA375
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....2.....!.. ....0.....@.....V..... .....8=.....T..... .....text...V..... . .`.rsrc..... .....@..@.....2.....9...T...T.....2.....d.....2.....RSDS...z..C...+Q_.....api-ms-win-core-synch-l1-1-0.pdb.....T....rdata..T..... ...rdata$zzzdbg.....V....edata... ..`....rsrc$01....` .....rsrc$02.....2.....)...)...(.....p.....1...c.....!...F...m.....$...X.....$...[.....@...i... .....!...Q.....[.....7.....O.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	6B1A87B1C223B757E5A39486BE60F7DD2956BB505A235DF406BCF693C7DD440E1F6D65FFEF7FDE491371C682F4A8BB3FD4CE8D8E09A6992BB131ADDF11EF2BF9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...X*uY.... .....!..... .....0.....3.....@.....v..... .....8=.....T.....text...v..... ....`.rsrc..... .....@..@....X*uY.....9...T...T.....X*uY.....d.....X*uY.....RSDS.V..B...`..S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rdata..T.....rdata$zzzdbg.....v....edata... ..`....rsrc$01....` .....rsrc$02.....X*uY.....(...I.....R.....W.....&...b.....$...W.....6...w..... .....:...|.....H.....A.....api-ms-win-core-synch-

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-sysinfo-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....C=.... .....!..... .....0.....@.....E..... .....0=.....T.....text...E..... ....`.rsrc..... .....@..@.....C=.....;...T...T.....C=.....d.....C=.....RSDS....T.>eD.#\|.../....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....E....edata... ..`....rsrc$01....` .....rsrc$02.....C=.....(.....:...i.....N.....7...s.....+...M...r...../...'... V.....:...k.....X..... ...?...d.....".....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-timezone-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....Y.x.... .....!..... .....0.....}3...@..... .....0=.....T.....text..... ....`.rsrc..... .....@..@.....Y.x.....<...T...T.....Y.x.....d.....Y.x.....RSDS.^.b. .t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rdata..T.....rdata$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\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	
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:pYWPhWFS0i00GftpBj7DudemJlP552
MD5:	0F079489ABD2B16751CEB7447512A70D
SHA1:	679DD712ED1C46FBD9BC8615598DA585D94D5D87
SHA-256:	F7D450A0F59151BCEFB98D20FCAE35F76029DF57138002DB5651D1B6A33ADC86
SHA-512:	92D64299EBDE83A4D7BE36F07F65DD868DA2765EB3B39F5128321AFF66ABD66171C7542E06272CB958901D403CCF69ED716259E0556EE983D2973FAA03C55D3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.. ....0.....`k....@..... .....9..... .....8=.....T.....text...)..... . .`.rsrc..... .....@..@.....f.....8...T...T.....f.....d.....f.....RSDS*...$.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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... ....0.....@..... .....8=.....T.....text..... .. `.rsrc..... .....@..@v.....8...d...d.....d.....RSDS....<....2..u....api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....T.....(.....>...w...../...W...p.....,...L...l.....,...L...m..... t.....'...^.....P...g.....$...=...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-convert-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE..... .....!.....0.....@.....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....NE.....:...d...d.....NE.....d.....NE.....RSDS..e.7P.g^j..[....api-ms-win-crt-convert-l1-1-0.pdb.... .....d....rdata..d.....rdata$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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	
SHA-512:	B5E2B9F5A9DD8A482169C7FC05F018AD8FE6AE27CB6540E67679272698BFCA24B2CA5A377FA61897F328B3DEAC10237CAFBD73BC965BF9055765923ABA9478F8
Malicious:	false
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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-filesystem-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
Malicious:	false
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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	72BD6D46A464DE74A8DAC4C346C52D068116910587B1C7B97978DF888925216958CE77BE1AE049C3DCCF5BF3FFFB21BC41A0AC329622BC9BBC190DF63ABB25C6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...J.o ....l..... ....0.....@..... ....8=.....T..... .....text..... ....`.rsrc..... .....@..@v.....J.o .....7...d...d.....J.o .....d.....J.o .....RSDSq.....pkQX[....api-ms-win-crt-heap-l1-1-0.pdb.....d.... rdata..d.....rdata$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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-locale-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	E98CBC8D958E604EFFA614A3964B3D66B6FC646BDCA9AA679EA5E4EB92EC0497B91485A40742F3471F4FF10DE83122331699EDC56A50F06AE86F21FAD70953FE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...|..O.... .....l..... ....0.....E*....@..... .....e..... .....8=.....T..... .....text...u..... ....`.rsrc..... .....@..@v.....|..O.....9...d...d.....|..O.....d.....|..O.....RSDS.X...7.....$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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28984
Entropy (8bit):	6.6686462438397
Encrypted:	false
SSDEEP:	384:7OTEmbM4Oe5grykfIgTmLyWPhW30i00GftpBjAKemXlDbNl:dEMq5grxfInbRoiNeSp
MD5:	8B0BA750E7B15300482CE6C961A932F0
SHA1:	71A2F5D76D23E48CEF8F258EAAD63E586CFC0E19
SHA-256:	BECE7BAB83A5D0EC5C35F0841CBBF413E01AC878550FBDB34816ED55185DCFED
SHA-512:	FB646CDCDB462A347ED843312418F037F3212B2481F3897A16C22446824149EE96EB4A4B47A903CA27B1F4D7A352605D4930DF73092C380E3D4D77CE4E972C5A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....@.....P.....@.....+.....@.....4..8=.....T.....text...,..... ....`.rsrc.....@.....0.....@..@v.....7...d...d.....d.....RSDSB...=.....,....api-ms-win-crt-math-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....+...edata...@..`....rsrc$01....`@.....rsrc$02.....l.....:..:...(.....(...@...X...q.....4...M...g..... ..= ..i ... ...!..E!..o!...!...!...!..."..F"..s"..."..."..."...#..E#..o#...#...#..

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-multibyte-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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 1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u'.....!.. ...$.....@.....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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-private-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	A9788D0F8B3F61235EF4740724B4A0D8C0D3CF51F851C367CC9779AB07F208864A7F1B4A44255E0DE8E030D84B63B1BDB58F12C8C20455FF6A55EF6207B31A91
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....^1.... .....!.....R.....@.....8=.....T.....text..... ....`.rsrc.....@..@v.....^1.....:...d...d.....^1.....d.....^1.....RSDS.J..w/.8..bu..3.....api-ms-win-crt-private-l1-1-0.pdb..... d....rdata..d.....rdata$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...E...F..1F..gF...F...F...G..BG..uG...G..

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	
SHA1:	F3035A756E2E963764912C6B432E74615AE07011
SHA-256:	C03124BA691B187917BA79078C66E12CBF5387A3741203070BA23980AA471E8B
SHA-512:	D44EF51D3AAF42681659FFFFF4DD1A1957EAF4B8AB7BB798704102555DA127B9D7228580DCED4E0FC98C5F4026B1BAB242808E72A76E09726B0AF839E384C3B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...l.h.....!.. ....0.....U....@.....x..... .....8=.....T.....text..... . .`.rsrc..... .....@..@v.....l.h.....:...d...d.....l.h.....d.....l.h.....RSDSZ\.qM..I....3.....api-ms-win-crt-process-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....x....edata.. ..`....rsrc$01....` .....rsrc$02.....l.h.....$...$...8.....X.....&...@...Y...q.....*...E..._...z.....!...<. ..V...q.....9...V...t.....7...R...i...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	8C2CB53CCF9719DE87EE65ED2E1947E266EC7E8343246DEF6429C6DF0DC514079F5171ACD1AA637276256C607F1063144494B992D4635B01E09DDEA6F5EEF20
Malicious:	false
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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-stdio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
Malicious:	false
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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23488
Entropy (8bit):	6.840671293766487
Encrypted:	false
SSDEEP:	384:5iFMx0C5yguNvZ5VQgx3SbwA7yMVIkFGlnWPhWGTi00GftpBjslem89lgC:56S5yguNvZ5VQgx3SbwA71IkFv5oialj
MD5:	404604CD100A1E60DFDAF6ECF5BA14C0
SHA1:	58469835AB4B916927B3CABF54AEE4F380FF6748
SHA-256:	73CC56F20268BFB329CCD891822E2E70DD70FE21FC7101DEB3FA30C34A08450C
SHA-512:	DA024CCB50D4A2A5355B7712BA896DF850CEE57AA4ADA33AAD0BAE6960BCD1E5E3CEE9488371AB6E19A2073508FBB3F0B257382713A31BC0947A4BF1F7A20E E4
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....S.....!.. .....0.....@.....B.....@.....0.....''...9.....T.....text..... ..`.rsrc.....0.....@..@v.....S.....9...d...d.....S.....d.....S.....RSDSl.....$[~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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-time-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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+zITA+0:XRNoibernAA+0
MD5:	849F2C3EBF1FCBA33D16153692D5810F
SHA1:	1F8EDA52D31512EBFDD546BE60990B95C8E28BFB
SHA-256:	69885FD581641B4A680846F93C2DD21E5DD8E3BA37409783BC5B3160A919CB5D
SHA-512:	44DC4200A653363C9A1CB2BDD3DA5F371F7D1FB644D1CE2FF5FE57D939B35130AC8AE27A3F07B82B3428233F07F974628027B0E6B6F70F7B2A8D259BE95222F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....OI..... .....!..... ....0.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@v.....OI.....7...d...d.....OI.....d.....OI.....RSDS...s..,E.w.9I..D....api-ms-win-crt-time-l1-1-0.pdb.....d....rda ta..d.....rdata$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\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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
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\LocalLow\gC9tT2iQ3s\breakpadinjector.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	117712
Entropy (8bit):	6.598338256653691
Encrypted:	false
SSDEEP:	3072:9b9ffsTV5n8cSQQtys6FXCVnx+IMD6eN07e:P25V/QQs6WTMex7e
MD5:	A436472B0A7B2EB2C4F53FDF512D0CF8
SHA1:	963FE8AE9EC8819EF2A674DBF7C6A92DBB6B46A9
SHA-256:	87ED943D2F06D9CA8824789405B412E770FE84454950EC7E96105F756D858E52
SHA-512:	89918673ADDC0501746F24EC9A609AC4D416A4316B27BF225974E898891699B630BB18DB32432DA2F058DC11D9AF7BAF95D067B29FB39052EE7C6F622718271B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..y7.{*7.{*7.{*..x+>.{*..~+I.{*...+%.{*.x+$.{*..+'.{*.~+..{*..z+4.{*7.z*A. {*..~+>.{*..{+6.{*...*6.{*..y+6.{*Rich7.{*.....PE..L....@.\.....''!.....t.....0.....S....@.....P...P.....(.....`...T..... .....@.....0..D.....text..... .`.rdata...l...0...n... .....@..@.data.....@....rsrc.....@..@.reloc... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.808908775107082
Encrypted:	false
SSDEEP:	6144:6cYBCU/bEPU6Rc5xUqc+z75nv4F0GHrIraqqDL6XPSed:67WRCB7zl4F0l4qn6R
MD5:	60ACD24430204AD2DC7F148B8CFE9BDC
SHA1:	989F377B9117D7CB21CBE92A4117F88F9C7693D9
SHA-256:	9876C53134DBBEC4DCCA67581F53638EBA3FEA3A15491AA3CF2526B71032DA97
SHA-512:	626C36E9567F57FA8EC9C36D96CBADEDE9C6F6734A7305ECFB9F798952BBACDFA33A1B6C4999BA5B78897DC2EC6F91870F7EC25B2CEACBAEE4BE942FE881DB01
Malicious:	false
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....@.\....."!.....f.....p.....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...d..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	132048
Entropy (8bit):	6.627391684128337
Encrypted:	false
SSDEEP:	3072:qgXCFTvwqiiynFa6zqeqQZ06DdEH4sq9gHNaIkIQhEwe:qdvwqMFbOePIP/zkIQ2h
MD5:	5A49EBF1DA3D5971B62A4FD295A71ECF
SHA1:	40917474EF7914126D62BA7CDBF6CF54D227AA20
SHA-256:	2B128B3702F8509F35CAD0D657C9A00F0487B93D70336DF229F8588FBA6BA926
SHA-512:	A6123BA3BCF9DE6AA8CE09F2F84D6D3C79B0586F9E2FD0C8A6C3246A91098099B64EDC2F5D7E7007D24048F10AE9FC30CCF7779171F3FD03919807EE6AF768(
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...?S..?S..?S..S..?S|.>R..?S;..S..?S|.<R..?S|.:R..?S|.;R..?S..>R..?S..>S..?Sn.;R.?Sn.?R..?Sn..S..?Sn.=R..?SRich..?S.....PE..L....@.\....."!.....f..... .....0.....@..... x..... .....p...T.....@.....\.....text...:..... ..`.rdata...@.....B.....@..@.data...l.....@....rsrc...x.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldif60.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20432
Entropy (8bit):	6.337521751154348
Encrypted:	false
SSDEEP:	384:YxfML3ALxK0AZEuzOJKRsIFYvDG8A3OPLonw4S:0fMmxFyO4RpGDG8MjS
MD5:	4FE544DFC7CDAA026DA6EDA09CAD66C4
SHA1:	85D21E5F5F72A4808F02F4EA14AA65154E52CE99
SHA-256:	3AABBE0AA86CE8A91E5C49B7DE577AF73B9889D7F03AF919F17F3F315A879B0F
SHA-512:	5C78C5482E589AF7D609318A6705824FD504136AEAAC63F373E913DA85FA03AF868669534496217B05D74364A165D7E08899437FCC0E3017F02D94858BA814BB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9..j..j..j...j..j^..k..j^..k..j^..k..j^..k..j...k..j..j..jL..k..jL..k..jL.bj..jL..k..jRich..j.....PE..L...<.\....."!.....Y.....0.....p.....r.....@.....5.....6.....P..x.....2.....`..x....0..T.....(1..@.....0.....text..... ..`.rdata.....0.....@..@.data.....@.....&.....@....rsrc...x....P.....,.....@..@.reloc..x....`.....0.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55760
Entropy (8bit):	6.738700405402967
Encrypted:	false
SSDEEP:	1536:LxsBS3Q6j+37mWT7DT/GszGrn7iBCmjFCOu:LxTBcmWT7X/Gszen7icmjFtu
MD5:	56E982D4C380C9CD24852564A8C02C3E
SHA1:	F9031327208176059CD03F53C8C5934C1050897F
SHA-256:	7F93B70257D966EA1C1A6038892B19E8360AADD8E8AE58E75EBB0697B9EA8786

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	
SHA-512:	92ADC4C905A800F8AB5C972B166099382F930435694D5F9A45D1FDE3FEF94FAC57FD8FAFF56FFCFCFDBC61A43E6395561B882966BE0C814ECC7E672C67E6765A
Malicious:	false
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....l..l..l.....l..~....l..9...l..~....l..~....l..~....l.....l..l....l..l..l..l..l..l..l..l..l..l..l..l..l..l..l..l..l..l..Rich.l.....PE..L...z@.\.....".....2.....t....@.....x.....T.....@.....text..... ..`.rdata..>.....@..@.data.....@....rodata.8.....@..@.rsrc...x.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\libEGL.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22480
Entropy (8bit):	6.528357540966124
Encrypted:	false
SSDEEP:	384:INZ9mLVDAffJJKAtn0mLAb8X3FbvDG8A3OPLonzvGb:4mx+fXvn4YFrDG8MKb
MD5:	96B879B611B2BBEE85DF18884039C2B8
SHA1:	00794796ACAC3899C1FB9ABBF123FEF3CC641624
SHA-256:	7B9FC6BE34F43D39471C2ADD872D5B4350853DB11CC66A323EF9E0C231542FB9
SHA-512:	DF8F1AA0384A5682AE47F212F3153D26EAFBBF12A8C996428C3366BEBE16850D0BDA453EC5F4806E6A62C36D312D37B8BBAFF549968909415670C9C61A6EC49
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../...N{.N{.N{.6..N{.F,z.N{.F,x.N{.F,~.N{.F,..N{..z.N{.T-z.N{.Nz..N{.T-~.N{.T-{.N{.T-..N{.T-y.N{.Rich.N{.....PE..L...aA.\.....".....(..... .....p.....~.....@.....%.....d....P..x.....:.....`.....!..T. .....".."..@..... .....text... ..... ..`.rdata..... .....@..@.data.....@.....2.....@....rsrc...x....P.....4..... @..@.reloc.....`.....8.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;..;..;.....2.....G.....).....*....."....."....4.....>..;...n.....:.....:.....:.....:...Rich;.....PE..L....=.\....."!.....`.....>.....@.....l.....<....@..P.....(.....P..d...0...T.....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P..... .....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32_InUse.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;..;..;.....2.....G.....).....*....."....."....4.....>..;...n.....:.....:.....:.....:...Rich;.....PE..L....=.\....."!.....`.....>.....@.....l.....<....@..P.....(.....P..d...0...T.....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P..... .....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.784614237836286
Encrypted:	false
SSDEEP:	3072:Z6s2DIGLXlNJJcPoN0j/kVqhp1qt/TXTv7q1D2JJJvPhrSeXZ5dR:MszGLXlNrE/kVqhp12/TXTjSD2JJJvPt
MD5:	EAE9273F8CDCF9321C6C37C244773139
SHA1:	8378E2A2F3635574C106EEA8419B5EB00B8489B0
SHA-256:	A0C6630D4012AE0311FF40F4F06911BCF1A23F7A4762CE219B8DFFA012D188CC
SHA-512:	06E43E484A89CEA9BA9B9519828D38E7C64B040F44CDAEB321CBDA574E7551B11FEA139CE3538F387A0A39A3D8C4CBA7F4CF03E4A3C98DB85F8121C2212A907
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;.....;.W...;...8..;...?..;...:..;...>..;...:...;...:w.;...?..;...>..;...;..;...;...9..;.Rich.;.....PE..L...{>.\......"!.....z.....@.....j.....@A.....@...t.....;. ..x.....0..l.....T.....T.... ...h...@.....l.....text...x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... ....@..@.reloc..l....0.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
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\LocalLow\gC9tT2iQ3s\nss3.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1245136
Entropy (8bit):	6.766715162066988
Encrypted:	false
SSDEEP:	24576:ido5Js2a56/+VwJebKj5KYFsRjzx5ZxKV6D1Z4Go/LCiytoxq2Zwn5hCM4MSRdY8:Q2aY4w6aozx5ZWMM7yew8MSRK1y
MD5:	02CC7B8EE30056D5912DE54F1BDFC219
SHA1:	A6923DA95705FB81E368AE48F93D28522EF552FB
SHA-256:	1989526553FD1E1E49B0FEA8036822CA062D3D39C4CAB4A37846173D0F1753D5
SHA-512:	0D5DFCF4FB19B27246FA799E339D67CD1B494427783F379267FB2D10D615FFB734711BAB2C515062C078F990A44A36F2D15859B1DACD4143DCC35B5C0CEE0EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c.4.'.Z.'.Z.'.Z.....3.Z...[.%.Z.B..#.Z...Y.*.Z..._.-.Z...^.,.Z...[./.Z..[.$.Z.'.[. ..Z..^.-.Z..Z.&.Z...&.Z..X.&.Z.Rich'.Z.....PE..L....@.\....."!.....@.....Q.....@.....x=..T.....p.....|.. ....T.....h...@.....text..... ..`.rdata...Q.....R.....@..@.data...tG...`..."...>.....@....rsrc...p.....`..... .....@..@.reloc...|.....~...d.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	336336
Entropy (8bit):	7.0315399874711995
Encrypted:	false
SSDEEP:	6144:8bndzEL04gF85K9autIMyEhZ/V3psPyHa9tBe1:8bndzEL04pnutIMyAp2z9tBe1
MD5:	BDAF9852F588C86B055C846B53D4C144

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	
SHA1:	03B739430CF9EADE21C977B5B416C4DD94528C3B
SHA-256:	2481DA1C459A2429A933D19AD6AE514BD2AE59818246DDB67B0EF44146CED3D8
SHA-512:	19D9A952A3DF5703542FA52A5A780C2E04D6A132059F30715954EAC40CD1C3F3B119A29736D4A911BE85086AFE08A54A7482FA409DFD882BAC39037F9EECD7E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pi.Pi.Pi.(..Pi.F2h.Pi.F2j.Pi.F2l.Pi.F2m.Pi.0h.Pi.T3h.Pi.P h.Pi.T3m.Pi.T3i.Pi.T3..Pi.T3k.Pi.Rich.Pi.....PE..L....@.\....."!.....`.....q.....@.....@.....P.....d.....x.....t)..p...T..... .....@.....text..... ..`.rdata..>.....@..@.data....N.....L.....@....rsrc...x.....@..@.reloc ..t).....*.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639527605275762
Encrypted:	false
SSDEEP:	1536:YvNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwI41Pc:+NGVOiBZbcGmxXMcBqmzoCUZoZebHPAT
MD5:	94919DEA9C745FBB01653F3FDAE59C23
SHA1:	99181610D8C9255947D7B2134CDB4825BD5A25FF
SHA-256:	BE3987A6CD970FF570A916774EB3D4E1EDCE675E70EDAC1BAF5E2104685610B0
SHA-512:	1A3BB3ECADD76678A65B7CB4EBE3460D0502B4CA96B1399F9E56854141C8463A0CFCFFEDF1DEFFB7470DDFBAC3B608DC10514ECA196D19B70803FBB02188E 5E
Malicious:	false
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....@.\....."!.....0.....0.....*q....@..... ?.....(@.....`..x. .....L.....p.....:..T.....(;..@.....0..X.....text..... ..`.rdata..D....0... .....@..@.data.....P.....>.....@....rsr c...x....`.....@.....@..@.reloc.....p.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	2828315
Entropy (8bit):	**7.998625956067725**
Encrypted:	**true**
SSDEEP:	49152:tiGLaX5/cgbRETlc0EqgSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJSVP1fnefekGt5CP
MD5:	1117CD347D09C43C1F2079439056ADA3
SHA1:	93C2CE5FC4924314318554E131CFBCD119F01AB6
SHA-256:	4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97
SHA-512:	FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF
Malicious:	false
Preview:	PK.....znN<..{r....i.....nssdbm3.dll...|...8...N..Y..6.$J.....$1...D .a.....jL.V..C...N.;....}./.....$...Z,T.R.qc...Ec.=.....;..{..s....p.`..A.?M.....W!.....a..?N...~e.A..W.o..... [.}...,...;.+\....Jw.|...k.....<yR.^.E.o.nxs.c...=V.....,..F....cu.....w.O..[..u.{..<.w....7P...{..K~..E..w...c...z^..[Z....6.G.V.2..+.n4.....1M.....w{f..nJL..{. d.....M..+.. ...../.)..$X!.....L..K.`. M...w.I..LA8r.IX...r...87..}.....<.].r.....TWm.....b6/._....a..W.IB...3.n.._...j....o.Mz.._Q.....8....K.*.....gr..L..*H...v....6[*...4I...{.1g..<..>M..$G.&Y.....-.....O..9\...,t..W.m.X ..Y.3.*...S<#}.".>.0RBg,...lh.s..o.....r.p8...)..3..K.v....ds.n3.+]....+....krMu._.Y\..../8T.....&.BC.".u..;..e.k u$.....~`.{.!.M...\W.Y.37+nQ.Z.*...3\G..5d....Z.hVL..Z.|k.5...XF.Y..lVVW. .C..|.....b..\.Z...m. ..0...P.F8{].U.p..RW,n...MM.....s..._@..>Q.. ...N.>.T?WM....)9B.....mVW.....b.6{..|!.....O....M....>.>.$\.%..L.zF.l...3

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24016
Entropy (8bit):	6.532540890393685
Encrypted:	false
SSDEEP:	384:TQJMOeAdiNcNUO3qgpw6MnTmJk0llEEHAnDl3vDG8A3OPLondJJs2z:KMaNqb6MTmVllEK2p/DG8MlsQ
MD5:	6099C438F37E949C4C541E61E88098B7
SHA1:	0AD03A6F626385554A885BD742DFE5B59BC944F5
SHA-256:	46B005817868F91CF60BAA052EE96436FC6194CE9A61E93260DF5037CDFA37A5
SHA-512:	97916C72BF75C11754523E2BC14318A1EA310189807AC8059C5F3DC1049321E5A3F82CDDD62944EA6688F046EE02FF10B7DDF8876556D1690729E5029EA414A9
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:`wq[.$q[.$q[.$x#.$s[.$.9.%s[.$.9.%p[.$.9.%{[.$.9.%z[.$S;.%s[ .$.8.%t[.$q[.$=[.$.8.%t[.$.8.%p[.$.8.$p[.$.8.%p[.$Richq[.$.....PE..L....@.\......"!..... ... .....%.....0.....p...../....@.....5.....p7..x....P..x... .....@.....`..$...`1..T.....1..@.....0..,.....text...2..... ..... ..`.rdata.....0.....$.....@..@.data...4....@.....4.....@....rsrc. ..x....P.....8.....@..@.reloc..$....`.....<.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\qipcap.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16336
Entropy (8bit):	6.437762295038996
Encrypted:	false
SSDEEP:	192:aPgr1ZCb2vGJ7b20qKvFej7x0KDWpH3vUA397Ae+PjPonZwC7Qm:aYpZPGJP209F4vDG8A3OPLonZwC7X
MD5:	F3A355D0B1AB3CC8EFFCC90C8A7B7538
SHA1:	1191F64692A89A04D060279C25E4779C05D8C375
SHA-256:	7A589024CF0EEB59F020F91BE4FE7EE0C90694C92918A467D5277574AC25A5A2
SHA-512:	6A9DB921156828BCE7063E5CDC5EC5886A13BD550BA8ED88C99FA6E7869ECFBA0D0B7953A4932EB8381243CD95E87C98B91C90D4EB2B0ACD7EE87BE114A91 A9E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s6.7W..7W..7W..>/..5W...5..5W...5..6W...5..>W...5..<W...7..4W. .7W..*W...4..6W...4`.6W...4..6W..Rich7W.....PE..L....B.\....."!..... .....`.....r....@.....$..P....@..x....."....P.. .... ..T..... ..@..... ..h.....text...P..... ..`.rdata..... .....@..@.data.....0.....@....rsrc...x....@..... .@..@.reloc.. ....P..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.54005414297208
Encrypted:	false
SSDEEP:	3072:8Af6suip+I7FEk/oJz69sFaXeu9CoT2nIVFetBW3D2xkEMk:B6POsF4CoT2OeYMzMk
MD5:	4E8DF049F3459FA94AB6AD387F3561AC
SHA1:	06ED392BC29AD9D5FC05EE254C2625FD65925114
SHA-256:	25A4DAE37120426AB060EBB39B7030B3E7C1093CC34B0877F223B6843B651871
SHA-512:	3DD4A86F83465989B2B30C240A7307EDD1B92D5C1D5C57D47EFF287DC9DAA7BACE157017908D82E00BE90F08FF5BADB68019FFC9D881440229DCEA5038F61C 6
Malicious:	false
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....@.\.....!.....b.....P.....|....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ucrtbase.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.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:FBmF2lIeaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
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.....I.....@..@.rsrc.....@..@.reloc..$..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
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\LocalLow\machineinfo.txt	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.263112003222452
Encrypted:	false
SSDEEP:	24:DlAeeIH/v3edyfFdt5IdrBqhKQa7kCGik/R8RA2Tvqzh:BAeX33b32BgFCGik/R0A+0h
MD5:	6E6628317291ACCCC95166E30C8A3C9F
SHA1:	A8DFBEF917DF4B0A1608CF34DBD769A7986FD383
SHA-256:	E0F9CD82E2DCA47FBC065E12151FAB80EC9B9349C79C6ACF16F46D40B9CE9EE0
SHA-512:	7133D91D77C64C5052DA86A6DC145076EF615CD1409283F6B45B6D0D8CA8376F2E41540996D678EA8C642B2736913F8964B827D868E0FDFD888F284DE28FB405
Malicious:	false
Preview:	Raccoon | 1.7.3...Build compile date: Sat Feb 27 21:25:06 2021...Launched at: 2021.04.09 - 01:46:41 GMT...Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A_user...Running on a desktop.....----------..... - Cookies: 1... - Passwords: 0... - Files: 0.....System Information:... - System Language: English... - System TimeZone: -8 hrs... - IP: 185.32.222.8... - Location: 47.431301, 8.562700 | Glattbrugg, Zurich, Switzerland (8152)... - ComputerName: 123716... - Username: user... - Windows version: NT 10.0... - Product name: Windows 10 Pro... - System arch: x64... - CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz (4 cores)... - RAM: 8191 MB (8125 MB used)... - Screen resolution: 1280x1024... - Display devices:....0) Microsoft Basic Display Adapter.....----------.....Installed Apps: ....Adobe Acrobat Reader DC (19.012.20035)....Google Chrome (85.0.4183.121)....Google Update Helper (1.3.35.451)....Java 8 Update 211 (8.0.2110.12)....Java Auto Updater (2.8.211.12)....Update

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F

C:\Users\user\AppData\LocalLow\sqlite3.dll	
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... .....".....@.0@.idata..H.....@.0..CRT.....@.0..tls.... .....@.0..rsrc..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

\Device\Null	
Process:	C:\Windows\SysWOW64\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.300553674183507
Encrypted:	false
SSDEEP:	3:hYFEHgARcWmFsFJQZtctFst3g4t32vov:hYFE1mFSQZi3MXt3X
MD5:	F74899957624A2837F2F86E8E62E92D4
SHA1:	1FCDAC5DEC5B0B1E00CF0247DA2A5F18566F1431
SHA-256:	507992A303C447D1D40D36E2E5163A237077B94F23A7089AC90A2F08682AE9BC
SHA-512:	E3FD14728633614B6552A75C15079AC8B04C0E8B3F49535B522C73312B1C812E30A934099AB18B507A0B4878068987D5545E90FA3747F7E7B10360EE324DB435
Malicious:	false
Preview:	..Waiting for 10 seconds, press CTRL+C to quit ..... 9.. 8.. 7.. 6.. 5.. 4.. 3.. 2.. 1.. 0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.757686000496675
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
File size:	126976
MD5:	ac6576aa4888bbbb8bd2598e75f8b6d1
SHA1:	e61899b32566e203023dc8947c5d9d27b527af97
SHA256:	7c90ae17ff566ca8b5fef5903dab4f0a0c4382354ffe1ba9e4285bcec735fa9f
SHA512:	fc68a91877eb5b43fe679f383d110b4ea03bd0d406dcae7792ae6d377f3f81f354611289e801aedf1f08be6fcd1a627cad5c09a70082494a1c7d734017a9af66
SSDEEP:	1536:QBGouBz01JfYbF7LNgT0F//////////////////////0qbQGRCU+brlihGo:WGZBzwRYZ7RgT0VbQ7UAlihG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L...:NU.....`.....@.....

File Icon

Icon Hash:	0ccea09899191898

Static PE Info

General

Entrypoint:	0x4016bc

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x554E3ACA [Sat May 9 16:50:18 2015 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:	b99d75676bd131a32dd8593967e4443d

Entrypoint Preview

Instruction
push 00410924h
call 00007F98ECDA6743h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
lea ebx, dword ptr [edi+4EC0FA13h]
mov eax, dword ptr [AFD3844Fh]
imul ebp, edi, 2Fh
jp 00007F98ECDA6756h
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
push esp
outsd
jo 00007F98ECDA6772h
and byte ptr [eax], ah
dec esi
jne 00007F98ECDA67C6h
je 00007F98ECDA67B3h
insb
add byte ptr [eax], ah
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
sub byte ptr [esi+48h], ah
or dword ptr [ecx], eax
clc
push FFFFFFFDh
inc edi
cdq
push esp
loop 00007F98ECDA6754h
clc
sbb cl, byte ptr [edi-63h]
fsub qword ptr [EBC50C6Bh]
mov al, byte ptr [ebp-63h]
mov di, ds

Instruction
sbb byte ptr [edi], FFFFFFA8h
jnbe 00007F98ECDA678Ah
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
cmp al, F1h
add byte ptr [eax], al
fiadd dword ptr [eax+eax+00h]
add byte ptr [edi], al
add byte ptr [ebp+4Eh], dl
inc esp
inc ebp
push edx
inc edi
dec ecx
add byte ptr [67000901h], cl
jne 00007F98ECDA67BEh
insd
outsb
je 00007F98ECDA67B7h
outsb
add byte ptr [ecx], bl
add dword ptr [eax], eax
inc edx
add byte ptr [edx], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x18754	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a000	0x4856	.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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x160	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x17cd8	0x18000	False	0.397664388021	data	6.30737519474	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x19000	0xaf4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1a000	0x4856	0x5000	False	0.414208984375	data	4.36128194962	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1c2ae	0x25a8	data		
RT_ICON	0x1b206	0x10a8	data		
RT_ICON	0x1a87e	0x988	data		
RT_ICON	0x1a416	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1a3d8	0x3e	data		
RT_VERSION	0x1a180	0x258	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryVar, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, __vbaStrToAnsi, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, __vbaAryCopy, _allmul, __vbaLateIdSt, _CItan, __vbaFPInt, __vbaVarForNext, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

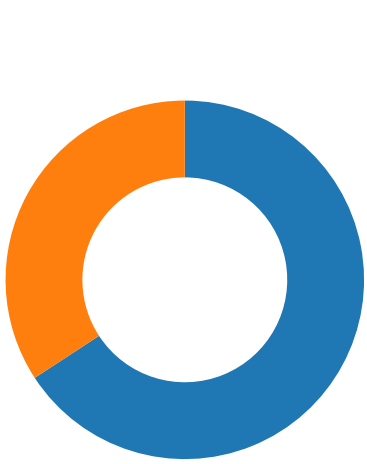
Description	Data
Translation	0x0409 0x04b0
InternalName	Udlgni4
FileVersion	3.00
CompanyName	Salty
Comments	Salty
ProductName	Salty
ProductVersion	3.00
FileDescription	Salty
OriginalFilename	Udlgni4.exe

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 18:46:28.193463087 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.205327034 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.205482960 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.206219912 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.217866898 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.230096102 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.230123043 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.230145931 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.230168104 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.230170012 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.230211020 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.230257988 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.246223927 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.258065939 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.258172035 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.259757042 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.276715994 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.519294024 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.519344091 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.519380093 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.519418001 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.519424915 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.519459009 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.519464970 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.519484997 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.519519091 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.520004034 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.520051003 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.520083904 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.520114899 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.520860910 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.520895958 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.520939112 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.520986080 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.521681070 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.521744013 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.521752119 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.521797895 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.522468090 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.522505999 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.522532940 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.522581100 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.528192043 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.528271914 CEST	49722	443	192.168.2.5	172.217.168.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 18:46:28.531560898 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.531658888 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.531673908 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.531738043 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.531826019 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.531892061 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.532008886 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.532110929 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.532778978 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.532820940 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.532861948 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.532891035 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.533700943 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.533759117 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.533786058 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.533884048 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.534356117 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.534416914 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.534432888 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.534482002 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.535212994 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.535257101 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.535303116 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.535331011 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.536065102 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.536114931 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.536158085 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.536184072 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.536936998 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.536983967 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.537013054 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.537038088 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.537832975 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.537899017 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.537916899 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.537955046 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.538584948 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.538619995 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.538675070 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.538702011 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.539300919 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.539344072 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.539376974 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.539405107 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.540208101 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.540251017 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.540298939 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.540323019 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.540853977 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.540941954 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.542335987 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.542442083 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.542452097 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.542511940 CEST	49722	443	192.168.2.5	172.217.168.33
Apr 8, 2021 18:46:28.542576075 CEST	443	49722	172.217.168.33	192.168.2.5
Apr 8, 2021 18:46:28.542643070 CEST	49722	443	192.168.2.5	172.217.168.33

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 18:45:54.321296930 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 18:45:54.956237078 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:45:54.993563890 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 18:45:55.284269094 CEST	52441	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 18:45:55.297019005 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 18:45:56.122231007 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:45:56.134759903 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 18:45:59.838401079 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:45:59.851428032 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:08.408804893 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:08.421251059 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:09.302000999 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:09.316871881 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:10.763600111 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:10.778618097 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:12.885046005 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:12.899403095 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:14.362267971 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:14.375509024 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:23.569161892 CEST	59736	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:23.582048893 CEST	53	59736	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:23.606267929 CEST	51058	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:23.607131004 CEST	52636	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:23.618297100 CEST	53	51058	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:23.619775057 CEST	53	52636	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:23.761043072 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:23.782010078 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:26.445846081 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:26.472815037 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:27.263010025 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:27.275788069 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:28.152524948 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:28.191073895 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:28.639209032 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:28.652918100 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:28.903700113 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:28.916362047 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:32.063061953 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:32.081640959 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:33.933720112 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:34.134996891 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 18:46:50.092916012 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:46:50.105616093 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 18:47:02.721182108 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:47:02.734487057 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 8, 2021 18:47:07.305150986 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:47:07.323040009 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 8, 2021 18:47:24.627325058 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:47:24.663213015 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 8, 2021 18:47:37.523016930 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:47:37.537092924 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 8, 2021 18:47:39.612608910 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:47:39.625710964 CEST	53	54450	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 18:46:28.152524948 CEST	192.168.2.5	8.8.8.8	0x1614	Standard query (0)	doc-0o-7g-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 8, 2021 18:46:28.639209032 CEST	192.168.2.5	8.8.8.8	0x87ac	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Apr 8, 2021 18:46:33.933720112 CEST	192.168.2.5	8.8.8.8	0x7745	Standard query (0)	shehootastayonwhatshelirned.top	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 18:46:28.191073895 CEST	8.8.8.8	192.168.2.5	0x1614	No error (0)	doc-0o-7g-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 18:46:28.191073895 CEST	8.8.8.8	192.168.2.5	0x1614	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)
Apr 8, 2021 18:46:28.652918100 CEST	8.8.8.8	192.168.2.5	0x87ac	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Apr 8, 2021 18:46:34.134996891 CEST	8.8.8.8	192.168.2.5	0x7745	No error (0)	shehootastayonwhatshelirned.top		5.230.68.40	A (IP address)	IN (0x0001)
Apr 8, 2021 18:46:34.134996891 CEST	8.8.8.8	192.168.2.5	0x7745	No error (0)	shehootastayonwhatshelirned.top		45.139.187.144	A (IP address)	IN (0x0001)

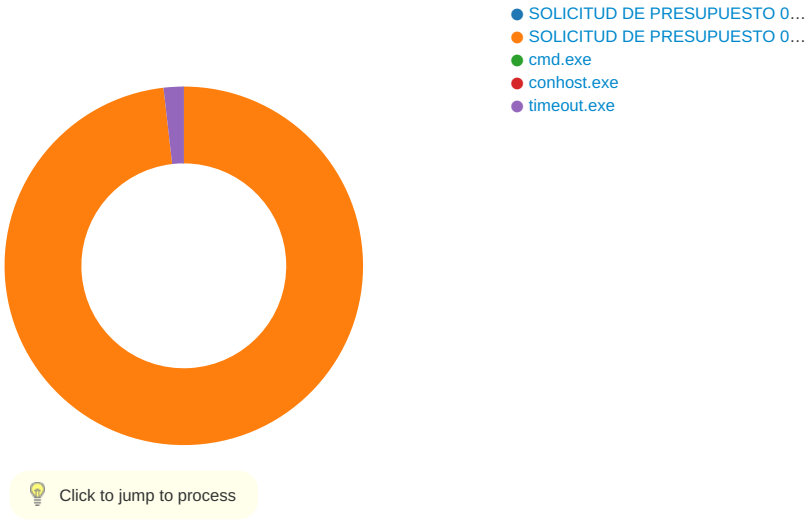
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 18:46:28.230168104 CEST	172.217.168.33	443	192.168.2.5	49722	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:32:57 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:32:56 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 8, 2021 18:46:28.704714060 CEST	195.201.225.248	443	192.168.2.5	49723	CN=telecut.in CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Feb 17 11:17:19 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue May 18 12:17:19 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 8, 2021 18:46:34.178030968 CEST	5.230.68.40	443	192.168.2.5	49727	CN=shehootastayonwhatshelirned.top CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Apr 07 20:31:57 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jul 06 20:31:57 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe PID: 1688 Parent PID: 5604

General

Start time:	18:46:02
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe'
Imagebase:	0x400000
File size:	126976 bytes
MD5 hash:	AC6576AA4888BBBB8BD2598E75F8B6D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe PID: 4516 Parent PID: 1688

General

Start time:	18:46:13
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe'
Imagebase:	0x400000
File size:	126976 bytes
MD5 hash:	AC6576AA4888BBBB8BD2598E75F8B6D1

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000002.00000002.313364575.0000000000561000.00000040.00000001.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	562B6F	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	562B6F	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	562B6F	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	562B6F	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	562B6F	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	562B6F	InternetOpenUrlA
C:\Users\user\AppData\LocalLow\sqlite3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	431374	CreateFileA
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	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	43BA3B	CopyFileW
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43BA3B	CopyFileW
C:\Users\user\AppData\LocalLow\RYwTiizs2t	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43BA3B	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\rQF69AzBla	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43BA3B	CopyFileW
C:\Users\user\AppData\LocalLow\iK0eK1lK3k	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40BF56	CreateDirectoryTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40BF56	CreateDirectoryTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	431374	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\qipcap.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ucrtbase.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\breakpadinjector.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldif60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\libEGL.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32_InUse.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-namedpipe-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-rtlsupport-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-string-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-sysinfo-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-timezone-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-convert-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-filesystem-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-heap-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-locale-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-multibyte-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-private-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-stdio-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-time-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-localization-l1-2-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-memory-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\machineinfo.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	461B1A	CreateFileW
C:\Users\user\AppData\LocalLow\M8gHzW2avYe.zip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	430A36	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\RYwTiizs2t	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\rQF69AzBla	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\machineinfo.txt	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\M8gHzW2avYe.zip	success or wait	1	430EDE	DeleteFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-localization-l1-2-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-memory-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-namedpipe-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-1.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-rtlsupport-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-string-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-sysinfo-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-timezone-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-convert-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-filesystem-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-heap-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-locale-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-multibyte-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-private-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-stdio-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-time-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\breakpadinjector.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldif60.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\libEGL.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	cannot delete	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32_InUse.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nss3.dll	cannot delete	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\qipcap.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ucrtbase.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\sqlite3.dll	success or wait	1	40BF04	DeleteFileTransactedA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\sqlite3.dll	unknown	2969	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 17 19 74 5c 00 10 0c 00 12 10 00 00 e0 00 06 21 0b 01 02 19 00 5a 09 00 00 04 0b 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 70 09 00 00 00 e0 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 b0 0c 00 00 06 00 00 1c 87 0e 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 c0 0a 00 9d 20 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....t\.......... .!.....Z...................p.. ...a..........................	success or wait	113	4315F6	WriteFile
C:\Users\user\AppData\LocalLow\sqlite3.dll	unknown	0			success or wait	1	4315F6	WriteFile
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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......@ ....C.....................	success or wait	1	43BA3B	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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......@ ....$............................ ....C....................	success or wait	1	43BA3B	CopyFileW
C:\Users\user\AppData\LocalLow\RYwTiizs2t	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$............................ ....C....................	success or wait	1	43BA3B	CopyFileW

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\LocalLow\rQF69AzBla</td><td>0</td><td>20480</td><td>53 51 4c 69 74 65 20
66 6f 72 6d 61 74 20
33 00 10 00 01 01 00
40 20 20 00 00 00 03
00 00 00 05 00 00 00
00 00 00 00 00 00 00
00 02 00 00 00 04 00
00 00 00 00 00 00 00
00 00 00 01 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 03 00 2e
43 c1 0d 0f f8 00 04
0d 20 00 0f 67 0f cf 0d
20 0f 38 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00</td><td>SQLite format 3......@ ......
....
....
........C....... ..g... .8....
....
....
....
....
...............</td><td>success or wait</td><td>1</td><td>43BA3B</td><td>CopyFileW</td></tr>
<tr><td>C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip</td><td>unknown</td><td>3815</td><td>50 4b 03 04 14 00 00
00 08 00 9a 7a 6e 4e
3c 09 f8 7b 72 d2 00
00 d0 69 01 00 0b 00
00 00 6e 73 73 64 62
6d 33 2e 64 6c 6c ec
fd 7f 7c 14 d5 d5 38
00 cf ee 4e 92 0d 59
d8 05 36 18 24 4a 90
a0 d1 a0 06 16 24 31
80 d9 84 dd 44 20 b0
61 c9 2e 11 13 b4 6a
4c b7 56 f9 b1 43 b0
12 08 4e 02 3b 19 b7
f5 e9 a3 7d ec 2f ab f5
f1 e9 0f db a7 b6 b5
80 d5 ea 86 d8 24 f8
13 81 5a 2c 54 a3 52
bd 71 63 8d 92 86 45
63 e6 3d e7 dc 99 dd
0d da ef f7 fb be 7f bf
f0 c9 ec cc dc 3b f7 9e
7b ee b9 e7 9e 73 ee
b9 e7 d6 de 70 bf 60
11 04 41 84 3f 4d 13
84 83 02 ff 57 21 fc df
ff e5 99 04 61 ca ec 3f
4e 11 9e ca 7e 65 ce
41 d3 ea 57 e6 ac 6f
f9 fa b6 82 cd 5b ef ba
7d eb cd df 2c b8 e5
e6 3b ef bc 2b 5c f0 b5
db 0a b6 4a 77 16 7c
fd ce 82 15 6b fd 05 df
bc eb d6 db ae 9a 3c
79 52</td><td>PK.........znN<..{r....i......
nssdbm3.dll...|...8...N..Y..6.
$J......$1....D .a.....jL.V..C
...N.;.....}./.............$.
..Z,T.R.qc...Ec.=............
....;..{....s.....p.`..A.?M...
..W!......a..?N...~e.A..W..o..
...[..}...,...;..+\.....Jw.|..
..k.........<yR</td><td>success or wait</td><td>347</td><td>4315F6</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip</td><td>unknown</td><td>0</td><td></td><td></td><td>success or wait</td><td>1</td><td>4315F6</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 b8 5a f0 59 d9 34 a3 59 d9 34 a3 59 d9 34 a3 50 a1 a7 a3 55 d9 34 a3 80 bb 35 a2 5b d9 34 a3 c7 79 f3 a3 51 d9 34 a3 80 bb 37 a2 58 d9 34 a3 80 bb 31 a2 53 d9 34 a3 80 bb 30 a2 52 d9 34 a3 7b b9 35 a2 5b d9 34 a3 92 ba 35 a2 5a d9 34 a3 59 d9 35 a3 ca d9 34 a3 92 ba 30 a2 41 d9 34 a3 92 ba 34 a2 58 d9 34 a3 92 ba cb a3 58 d9 34 a3 92 ba 36 a2 58 d9 34 a3 52 69 63 68 59 d9 34	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	success or wait	6	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 35 3a 60 77 71 5b 0e 24 71 5b 0e 24 71 5b 0e 24 78 23 9d 24 73 5b 0e 24 a8 39 0f 25 73 5b 0e 24 a8 39 0d 25 70 5b 0e 24 a8 39 0b 25 7b 5b 0e 24 a8 39 0a 25 7a 5b 0e 24 53 3b 0f 25 73 5b 0e 24 ba 38 0f 25 74 5b 0e 24 71 5b 0f 24 3d 5b 0e 24 ba 38 0a 25 74 5b 0e 24 ba 38 0e 25 70 5b 0e 24 ba 38 f1 24 70 5b 0e 24 ba 38 0c 25 70 5b 0e 24 52 69 63 68 71 5b 0e 24 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......5:`wq[.$q[.$q[.$x#.$s [.$.9.%s[.$.9.%p[.$.9.% {[.$.9.% z[.$S;.%s[.$.8.%t[.$q[.$= [.$.8 .%t[.$.8.%p[.$.8.$p[.$.8.% p[.$Richq[.$.......	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\qipcap.dll	unknown	16336	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 73 36 f1 9f 37 57 9f cc 37 57 9f cc 37 57 9f cc 3e 2f 0c cc 35 57 9f cc ee 35 9e cd 35 57 9f cc ee 35 9c cd 36 57 9f cc ee 35 9a cd 3e 57 9f cc ee 35 9b cd 3c 57 9f cc 15 37 9e cd 34 57 9f cc 37 57 9e cc 2a 57 9f cc fc 34 9a cd 36 57 9f cc fc 34 60 cc 36 57 9f cc fc 34 9d cd 36 57 9f cc 52 69 63 68 37 57 9f cc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......s6..7W..7W..7W..>/.. 5W ...5..5W...5..6W...5..>W...5. . <W...7..4W..7W..*W...4..6 W...4 `.6W...4..6W..Rich7W........ ..........PE..L..	success or wait	1	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 a2 6c 24 1c e6 0d 4a 4f e6 0d 4a 4f e6 0d 4a 4f ef 75 d9 4f ea 0d 4a 4f 3f 6f 4b 4e e4 0d 4a 4f 3f 6f 49 4e e4 0d 4a 4f 3f 6f 4f 4e ec 0d 4a 4f 3f 6f 4e 4e ed 0d 4a 4f c4 6d 4b 4e e4 0d 4a 4f 2d 6e 4b 4e e5 0d 4a 4f e6 0d 4b 4f 7e 0d 4a 4f 2d 6e 4e 4e f2 0d 4a 4f 2d 6e 4a 4e e7 0d 4a 4f 2d 6e b5 4f e7 0d 4a 4f 2d 6e 48 4e e7 0d 4a 4f 52 69 63 68 e6 0d 4a 4f 00 00 00 00 00 00 00	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-n NN..JO-nJN..JO-n.O..JO- nHN..JORich..JO.......	success or wait	9	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ucrtbase.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 b8 df 92 45 fc be fc 16 fc be fc 16 fc be fc 16 f5 c6 6f 16 cf be fc 16 fc be fd 16 70 be fc 16 8f dc 01 16 fd be fc 16 8f dc f8 17 e8 be fc 16 8f dc fc 17 fd be fc 16 8f dc ff 17 92 be fc 16 8f dc f9 17 a4 be fc 16 8f dc f2 17 9a bc fc 16 8f dc 03 16 fd be fc 16 8f dc fe 17 fd be fc 16 52 69 63 68 fc be fc 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........E..............o... ......p....................... ....Rich............	success or wait	70	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 f9 a3 4e 45 98 cd 1d 45 98 cd 1d 45 98 cd 1d f1 04 22 1d 47 98 cd 1d 4c e0 5e 1d 4e 98 cd 1d 45 98 cc 1d 6c 98 cd 1d 9c fa c9 1c 55 98 cd 1d 9c fa ce 1c 56 98 cd 1d 9c fa c8 1c 41 98 cd 1d 9c fa c5 1c 5f 98 cd 1d 9c fa cd 1c 44 98 cd 1d 9c fa 32 1d 44 98 cd 1d 9c fa cf 1c 44 98 cd 1d 52 69 63 68 45 98 cd 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.... $..........NE...E...E.....".G. ..L.^.N...E...I.......U....... V.......A......._.......D..... 2.D.......D...RichE........... PE..L....8'Y...	success or wait	6	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 a0 79 f3 5a e4 18 9d 09 e4 18 9d 09 e4 18 9d 09 c6 78 9e 08 ed 18 9d 09 c6 78 98 08 9b 18 9d 09 c6 78 99 08 f6 18 9d 09 3d 7a 9e 08 f6 18 9d 09 3d 7a 98 08 ff 18 9d 09 3d 7a 99 08 eb 18 9d 09 c6 78 9b 08 e3 18 9d 09 c6 78 9c 08 eb 18 9d 09 e4 18 9c 09 7a 18 9d 09 2f 7b 99 08 e0 18 9d 09 2f 7b 98 08 ef 18 9d 09 2f 7b 9d 08 e5 18 9d 09 2f 7b 62 09 e5 18 9d 09 2f 7b 9f 08 e5 18 9d	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........y.Z.............x.... ...x.......x......=z......=z.. ....=z.......x.......x........ ..z.../{....../{....../{...... /{b...../{.....	success or wait	8	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 53 e5 ee 06 17 84 80 55 17 84 80 55 17 84 80 55 1e fc 13 55 15 84 80 55 ce e6 81 54 15 84 80 55 ce e6 83 54 16 84 80 55 ce e6 85 54 1e 84 80 55 ce e6 84 54 1c 84 80 55 35 e4 81 54 10 84 80 55 17 84 81 55 21 84 80 55 dc e7 84 54 13 84 80 55 dc e7 80 54 16 84 80 55 dc e7 7f 55 16 84 80 55 dc e7 82 54 16 84 80 55 52 69 63 68 17 84 80 55 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.... $.......S......U...U...U...U.. .U...T...U...T...U...T...U...T ...U5..T...U...U!..U...T...U.. .T...U...U...U...T...URich... U........PE..L..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \gC9tT2iQ3s\breakpadinjector.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 73 83 15 79 37 e2 7b 2a 37 e2 7b 2a 37 e2 7b 2a 15 82 78 2b 3e e2 7b 2a 15 82 7e 2b 49 e2 7b 2a 15 82 7f 2b 25 e2 7b 2a ee 80 78 2b 24 e2 7b 2a ee 80 7f 2b 27 e2 7b 2a ee 80 7e 2b 14 e2 7b 2a 15 82 7a 2b 34 e2 7b 2a 37 e2 7a 2a 41 e2 7b 2a fc 81 7e 2b 3e e2 7b 2a fc 81 7b 2b 36 e2 7b 2a fc 81 84 2a 36 e2 7b 2a fc 81 79 2b 36 e2 7b 2a 52 69 63 68 37 e2 7b 2a 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......s..y7.{*7.{*7. {*..x+>.{*..~+I.{*...+%. {*..x+$.{*...+'.{*..~+.. {*..z+4.{*7.z*A.{*..~+>.{*.. {+6.{*...*6.{*..y+6.{*Rich7. {*.......	success or wait	8	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 c0 f0 2f 05 84 91 41 56 84 91 41 56 84 91 41 56 8d e9 d2 56 88 91 41 56 5d f3 40 57 86 91 41 56 1a 31 86 56 85 91 41 56 5d f3 42 57 80 91 41 56 5d f3 44 57 8f 91 41 56 5d f3 45 57 8f 91 41 56 a6 f1 40 57 80 91 41 56 4f f2 40 57 87 91 41 56 84 91 40 56 d6 91 41 56 4f f2 42 57 86 91 41 56 4f f2 45 57 c0 91 41 56 4f f2 41 57 85 91 41 56 4f f2 be 56 85 91 41 56 4f f2 43 57 85 91 41	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..A VO.AW..AV O..V..AVO.CW..A	success or wait	21	41DB61	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll</td><td>unknown</td><td>16384</td><td>4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 a9 7e e4 18 ed 1f 8a 4b ed 1f 8a 4b ed 1f 8a 4b e4 67 19 4b ef 1f 8a 4b 34 7d 8b 4a ef 1f 8a 4b 34 7d 89 4a ec 1f 8a 4b 34 7d 8f 4a e4 1f 8a 4b 34 7d 8e 4a e6 1f 8a 4b cf 7f 8c 4a ec 1f 8a 4b cf 7f 8b 4a e4 1f 8a 4b ed 1f 8b 4b ad 1f 8a 4b 26 7c 8e 4a ca 1f 8a 4b 26 7c 8a 4a ec 1f 8a 4b 26 7c 75 4b ec 1f 8a 4b 26 7c 88 4a ec 1f 8a 4b 52 69 63 68 ed 1f 8a 4b 00 00 00 00 00 00 00</td><td>MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........~.....K...K...K.g.K.. .K4}.J...K4}.J...K4}.J...K4}. J...K...J...K...J...K...K&| .J...K&|.J...K&|uK...K&|.J... KRich...K.......</td><td>success or wait</td><td>5</td><td>41DB61</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll</td><td>unknown</td><td>16384</td><td>4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e1 d4 51 00 a5 b5 3f 53 a5 b5 3f 53 a5 b5 3f 53 ac cd ac 53 b5 b5 3f 53 7c d7 3e 52 a7 b5 3f 53 3b 15 f8 53 a7 b5 3f 53 7c d7 3c 52 a7 b5 3f 53 7c d7 3a 52 af b5 3f 53 7c d7 3b 52 ae b5 3f 53 87 d5 3e 52 a6 b5 3f 53 a5 b5 3e 53 f6 b5 3f 53 6e d6 3b 52 e5 b5 3f 53 6e d6 3f 52 a4 b5 3f 53 6e d6 c0 53 a4 b5 3f 53 6e d6 3d 52 a4 b5 3f 53 52 69 63 68 a5 b5 3f 53 00 00 00 00 00 00</td><td>MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.........Q...?S..? S..?S...S..?S|.>R..?S;..S..? S|.<R..?S|.:R..?S|.;R..? S..>R..?S..>S..?Sn.;R..? Sn.?R..?Sn..S..?Sn.=R..? SRich..?S.......</td><td>success or wait</td><td>9</td><td>41DB61</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldif60.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 c3 85 f3 39 87 e4 9d 6a 87 e4 9d 6a 87 e4 9d 6a 8e 9c 0e 6a 8f e4 9d 6a 5e 86 9c 6b 84 e4 9d 6a 5e 86 9e 6b 86 e4 9d 6a 5e 86 98 6b 8d e4 9d 6a 5e 86 99 6b 8c e4 9d 6a a5 84 9c 6b 85 e4 9d 6a 87 e4 9c 6a a3 e4 9d 6a 4c 87 99 6b 86 e4 9d 6a 4c 87 9d 6b 86 e4 9d 6a 4c 87 62 6a 86 e4 9d 6a 4c 87 9f 6b 86 e4 9d 6a 52 69 63 68 87 e4 9d 6a 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.... $.....9...j...j...j...j.. .j^..k...j^..k...j^..k...j^..k ...j...k...j...j...jL..k...jL. .k...jL.bj...jL..k...jRich...j	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e3 0d 7f ed a7 6c 11 be a7 6c 11 be a7 6c 11 be ae 14 82 be b3 6c 11 be 7e 0e 10 bf a5 6c 11 be 39 cc d6 be a5 6c 11 be 7e 0e 12 bf a0 6c 11 be 7e 0e 14 bf b7 6c 11 be 7e 0e 15 bf ac 6c 11 be 85 0c 10 bf a3 6c 11 be 6c 0f 10 bf a4 6c 11 be a7 6c 10 be ce 6c 11 be a7 6c 11 be a5 6c 11 be 6c 0f 15 bf a0 6c 11 be 6c 0f 14 bf a5 6c 11 be 6c 0f 11 bf a6 6c 11 be 6c 0f ee be a6 6c 11	MZ.....@..... ..... (.....!..L.!This program cannot be run in DOS mode....$.....l...l...l.....l ..~....l..9....l..~....l..~... .l..~....l.....l..l....l...l ...l...l...l..l....l..l....l..l....l..l....l.	success or wait	4	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\libEGL.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 2f 15 8e 9f 4e 7b dd 9f 4e 7b dd 9f 4e 7b dd 96 36 e8 dd 9d 4e 7b dd 46 2c 7a dc 9d 4e 7b dd 46 2c 78 dc 9e 4e 7b dd 46 2c 7e dc 95 4e 7b dd 46 2c 7f dc 94 4e 7b dd bd 2e 7a dc 9d 4e 7b dd 54 2d 7a dc 9c 4e 7b dd 9f 4e 7a dd fb 4e 7b dd 54 2d 7e dc 9e 4e 7b dd 54 2d 7b dc 9e 4e 7b dd 54 2d 84 dd 9e 4e 7b dd 54 2d 79 dc 9e 4e 7b dd 52 69 63 68 9f 4e 7b dd 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $......../...N{..N{..N{..6...N {.F,z..N{.F,x..N{.F,~..N{.F,.. .N{...z..N{.T- z..N{..Nz..N{.T-~..N{.T- {..N{.T-...N{.T-y..N{. Rich.N{........	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 85 39 b7 bf c1 58 d9 ec c1 58 d9 ec c1 58 d9 ec c8 20 4a ec c3 58 d9 ec 18 3a d8 ed c3 58 d9 ec 18 3a da ed c0 58 d9 ec 18 3a dc ed c8 58 d9 ec 18 3a dd ed ca 58 d9 ec e3 38 d8 ed c4 58 d9 ec c1 58 d8 ec f0 58 d9 ec 0a 3b dd ed c2 58 d9 ec 0a 3b d9 ed c0 58 d9 ec 0a 3b 26 ec c0 58 d9 ec 0a 3b db ed c0 58 d9 ec 52 69 63 68 c1 58 d9 ec 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.... $........9...X...X...X... J..X ...:...X...:...X...:...X...:.. .X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 85 39 b7 bf c1 58 d9 ec c1 58 d9 ec c1 58 d9 ec c8 20 4a ec c3 58 d9 ec 18 3a d8 ed c3 58 d9 ec 18 3a da ed c0 58 d9 ec 18 3a dc ed c8 58 d9 ec 18 3a dd ed ca 58 d9 ec e3 38 d8 ed c4 58 d9 ec c1 58 d8 ec f0 58 d9 ec 0a 3b dd ed c2 58 d9 ec 0a 3b d9 ed c0 58 d9 ec 0a 3b 26 ec c0 58 d9 ec 0a 3b db ed c0 58 d9 ec 52 69 63 68 c1 58 d9 ec 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.... $........9...X...X...X... J..X ...:...X...:...X...:...X...:.. .X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 8d c2 55 b1 c9 a3 3b e2 c9 a3 3b e2 c9 a3 3b e2 c0 db a8 e2 d9 a3 3b e2 57 03 fc e2 cb a3 3b e2 10 c1 38 e3 c7 a3 3b e2 10 c1 3f e3 c2 a3 3b e2 10 c1 3a e3 cd a3 3b e2 10 c1 3e e3 db a3 3b e2 eb c3 3a e3 c0 a3 3b e2 c9 a3 3a e2 77 a3 3b e2 02 c0 3f e3 c8 a3 3b e2 02 c0 3e e3 dd a3 3b e2 02 c0 3b e3 c8 a3 3b e2 02 c0 c4 e2 c8 a3 3b e2 02 c0 39 e3 c8 a3 3b e2 52 69 63 68 c9 a3 3b	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........U...;...;...;....... ;.W.....;...8...;...?...;...:. ..;...>...;...:...;...:.w.;... ?...;...>...;...;...;.......;. ..9...;.Rich..;	success or wait	9	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 7f e3 6d 52 3b 82 03 01 3b 82 03 01 3b 82 03 01 19 e2 00 00 32 82 03 01 19 e2 06 00 47 82 03 01 19 e2 07 00 29 82 03 01 e2 e0 00 00 2a 82 03 01 e2 e0 06 00 22 82 03 01 e2 e0 07 00 34 82 03 01 19 e2 02 00 3e 82 03 01 3b 82 02 01 6e 82 03 01 f0 e1 06 00 3a 82 03 01 f0 e1 03 00 3a 82 03 01 f0 e1 fc 01 3a 82 03 01 f0 e1 01 00 3a 82 03 01 52 69 63 68 3b 82 03 01 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....mR;...;...;.....2. .....G.....).....*..... ".....4.....>...;...n..... ..:.....:.....:.....:... Rich;.....	success or wait	6	41DB61	WriteFile
C:\Users\user\AppData\LocalLow \gC9tT2iQ3s\mozMapi32_InUse.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 7f e3 6d 52 3b 82 03 01 3b 82 03 01 3b 82 03 01 19 e2 00 00 32 82 03 01 19 e2 06 00 47 82 03 01 19 e2 07 00 29 82 03 01 e2 e0 00 00 2a 82 03 01 e2 e0 06 00 22 82 03 01 e2 e0 07 00 34 82 03 01 19 e2 02 00 3e 82 03 01 3b 82 02 01 6e 82 03 01 f0 e1 06 00 3a 82 03 01 f0 e1 03 00 3a 82 03 01 f0 e1 fc 01 3a 82 03 01 f0 e1 01 00 3a 82 03 01 52 69 63 68 3b 82 03 01 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....mR;...;...;.....2. .....G.....).....*..... ".....4.....>...;...n..... ..:.....:.....:.....:... Rich;.....	success or wait	6	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 a6 c8 bc 41 e2 a9 d2 12 e2 a9 d2 12 e2 a9 d2 12 56 35 3d 12 e0 a9 d2 12 eb d1 41 12 fa a9 d2 12 3b cb d3 13 e1 a9 d2 12 e2 a9 d3 12 22 a9 d2 12 3b cb d1 13 eb a9 d2 12 3b cb d6 13 ee a9 d2 12 3b cb d7 13 f4 a9 d2 12 3b cb da 13 95 a9 d2 12 3b cb d2 13 e3 a9 d2 12 3b cb 2d 12 e3 a9 d2 12 3b cb d0 13 e3 a9 d2 12 52 69 63 68 e2 a9 d2 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.... $..........A............V5=... ....A.....;..........."...;... ....;.......;.......;.......;.......;.- .....;.......Rich............PE..L..	success or wait	27	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nss3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 63 83 34 8c 27 e2 5a df 27 e2 5a df 27 e2 5a df 2e 9a c9 df 33 e2 5a df fe 80 5b de 25 e2 5a df b9 42 9d df 23 e2 5a df fe 80 59 de 2a e2 5a df fe 80 5f de 2d e2 5a df fe 80 5e de 2c e2 5a df 05 82 5b de 2f e2 5a df ec 81 5b de 24 e2 5a df 27 e2 5b df d1 e2 5a df ec 81 5e de 2d e3 5a df ec 81 5a de 26 e2 5a df ec 81 a5 df 26 e2 5a df ec 81 58 de 26 e2 5a df 52 69 63 68 27 e2 5a	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......c.4.'.Z.'.Z.'.Z.....3.Z... [.%.Z..B..#.Z...Y.*.Z..._.- .Z...^.,.Z...[./.Z...[.$.Z.'. [...Z...^.-.Z...Z.&.Z.....&.Z. ..X.&.Z.Rich'.Z	success or wait	76	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 31 07 8e 9f 50 69 dd 9f 50 69 dd 9f 50 69 dd 96 28 fa dd 9d 50 69 dd 46 32 68 dc 9d 50 69 dd 46 32 6a dc 9e 50 69 dd 46 32 6c dc 95 50 69 dd 46 32 6d dc 94 50 69 dd bd 30 68 dc 9d 50 69 dd 54 33 68 dc 9c 50 69 dd 9f 50 68 dd a6 50 69 dd 54 33 6d dc be 50 69 dd 54 33 69 dc 9e 50 69 dd 54 33 96 dd 9e 50 69 dd 54 33 6b dc 9e 50 69 dd 52 69 63 68 9f 50 69 dd 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1...Pi..Pi..Pi..(...P i.F2h..Pi.F2j..Pi.F2l..Pi.F2 m. .Pi..0h..Pi.T3h..Pi..Ph..Pi.T 3 m..Pi.T3i..Pi.T3...Pi.T3k..Pi .Rich.Pi........	success or wait	21	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-namedpipe-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 20 17 89 e9 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L... ....!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 29 e5 72 97 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...).r............!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 f3 19 95 b4 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L..................!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-1.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 11 39 ee d7 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....9............!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 e2 bc 26 dc 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....&...........!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-rtlsupport-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 0a c2 c2 28 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 02 00 00 00 04 00 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L......(...........!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-string-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 f9 1e 52 17 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....R............!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 88 d1 10 32 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L......2...........!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 58 2a 75 59 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...X*uY...........!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-sysinfo-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 02 88 43 3d 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....C=...........!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-timezone-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 8c 59 cc 78 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....Y.x...........!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 d9 03 66 ab 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....f............!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 0f c9 df a8 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L..................!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-convert-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 b3 4e 45 c2 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....NE............!.. ....0......	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 c6 6a 55 04 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....jU............!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-filesystem-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 95 96 ad 68 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L......h...........!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-heap-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 4a fc 6f 20 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...J.o ....!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-locale-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 7c 0f de 4f 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...|..O...........!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 a2 17 f8 17 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L..................!.. ....@......	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-multibyte-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 0a 75 27 9f 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....u'............!.. ...$...................@......	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-private-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 9d c7 5e 31 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 da 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 f0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....^1...........!..	success or wait	5	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 6c 1a 68 b4 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...l.h............!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 08 df 4c 08 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 16 00 00 00 04 00 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....L............!.. ....0......	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-stdio-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 1c 09 d5 e0 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L..................!.. ....0......	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 01 bc a7 53 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L......S...........!.. ....0......	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-time-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 e0 b2 4f 49 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....OI...........!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 1e 21 35 ff 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....!5............!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 15 5f 81 4c 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...._.L...........!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 34 ef df 7c 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...4..|...........!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 c9 e0 a3 47 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L......G...........!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 b5 df 3a bf 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....:............!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 ab 24 06 9c 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....$.............!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 d6 75 2a 6c 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....u*l...........!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-localization-l1-2-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 53 bd 76 f4 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...S.v............!..	success or wait	2	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-memory-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 1c f7 25 28 00 00 00 00 00 00 00 00 e0 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.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....%(...........!..	success or wait	2	41DB61	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	793	52 61 63 63 6f 6f 6e 20 7c 20 31 2e 37 2e 33 0d 0d 0a 42 75 69 6c 64 20 63 6f 6d 70 69 6c 65 20 64 61 74 65 3a 20 53 61 74 20 46 65 62 20 32 37 20 32 31 3a 32 35 3a 30 36 20 32 30 32 31 0d 0d 0a 4c 61 75 6e 63 68 65 64 20 61 74 3a 20 32 30 32 31 2e 30 34 2e 30 39 20 2d 20 30 31 3a 34 36 3a 34 31 20 47 4d 54 0d 0d 0a 42 6f 74 5f 49 44 3a 20 44 30 36 45 44 36 33 35 2d 36 38 46 36 2d 34 45 39 41 2d 39 35 35 43 2d 34 38 39 39 46 35 46 35 37 42 39 41 5f 61 6c 66 6f 6e 73 0d 0d 0a 52 75 6e 6e 69 6e 67 20 6f 6e 20 61 20 64 65 73 6b 74 6f 70 0d 0d 0a 0d 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0d 0d 0a 0d 0d 0a 20 20 2d 20 43 6f 6f 6b 69 65 73 3a 20 31 0d 0d 0a 20 20 2d 20 50 61 73 73 77 6f 72 64 73 3a 20 30 0d 0d 0a 20 20 2d 20 46 69 6c 65 73 3a 20 30 0d 0d	Raccoon | 1.7.3...Build compile date: Sat Feb 27 21:25:06 2021...Launched at: 2021.04.09 - 01:46:41 GMT...Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A _user...Running on a desktop.....----------..... - Cookies: 1... - Passwords: 0... - Files: 0..	success or wait	1	45576B	WriteFile
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	287	49 6e 73 74 61 6c 6c 65 64 20 41 70 70 73 3a 20 0d 0d 0a 09 41 64 6f 62 65 20 41 63 72 6f 62 61 74 20 52 65 61 64 65 72 20 44 43 20 28 31 39 2e 30 31 32 2e 32 30 30 33 35 29 0d 0d 0a 09 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 20 28 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 29 0d 0d 0a 09 47 6f 6f 67 6c 65 20 55 70 64 61 74 65 20 48 65 6c 70 65 72 20 28 31 2e 33 2e 33 35 2e 34 35 31 29 0d 0d 0a 09 4a 61 76 61 20 38 20 55 70 64 61 74 65 20 32 31 31 20 28 38 2e 30 2e 32 31 31 30 2e 31 32 29 0d 0d 0a 09 4a 61 76 61 20 41 75 74 6f 20 55 70 64 61 74 65 72 20 28 32 2e 38 2e 32 31 31 2e 31 32 29 0d 0d 0a 09 55 70 64 61 74 65 20 66 6f 72 20 53 6b 79 70 65 20 66 6f 72 20 42 75 73 69 6e 65 73 73 20 32 30 31 36 20 28 4b 42 34 34 38 34 32 38 36 29 20 33 32 2d 42 69 74 20	Installed Apps: ....Adobe Acrobat Reader DC (19.012.20035)....Google Chrome (85.0.4183.121)....Google Update Helper (1.3.35.451)....Java 8 Update 211 (8.0.2110.12)....Java Auto Updater (2.8.211.12)....Update for Skype for Business 2016 (KB4484286) 32-Bit	success or wait	1	45576B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\M8gHzW2avYe.zip	unknown	1181	50 4b 03 04 14 00 02 00 08 00 cc 95 88 52 91 c3 63 18 c5 00 00 00 d8 00 00 00 2a 00 11 00 62 72 6f 77 73 65 72 73 2f 63 6f 6f 6b 69 65 73 2f 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 5f 44 65 66 61 75 6c 74 2e 74 78 74 55 54 0d 00 07 8e 4f 6f 60 8e 4f 6f 60 8e 4f 6f 60 25 c5 bd 72 82 30 00 00 e0 99 de f5 51 b0 92 12 12 86 0e 56 fe 21 d5 e4 c0 48 97 5e 4a 6a ee 1a 30 a0 56 c2 db 3b f4 5b be 95 32 46 f5 3f ab ce 0c 4e cd 9a d8 79 f9 cf 0b 3c 04 30 06 00 3b 1f 79 e4 80 b5 ff 46 2f bf ba 56 b0 38 4e 76 5a a4 5f 0f d7 6d 3b 66 92 7b 48 91 f0 cf 9e de cf a0 ec 5d cd ae 7c e6 5b 81 96 cd 52 15 c7 03 01 1c b9 b7 2f 16 ea c4 4a 3a 49 08 a7 20 49 2f 9f 19 12 43 67 76 92 c1 21 b7 4c 51 e2 7f ef 6e cd 18 bb fb 9c e8 6e ee 53 59 fa 42 e3 78 53 54 6d 32 dc 1b 65 5f a9 c1	PK.....R..c.....*... browsers/cookies/Google Chrome _Default.txtUT....Oo`.Oo`. Oo`% ..r.0.....Q.....V.!...H.^Jj. .0.V..;.[..2F.?...N...y...<.0. .;.y....F/..V.8NvZ._..m;f.{H.. .....]..|.[...R...../...J:I.. I/...Cgv..!.LQ...n.....n.S Y.B.xSTm2..e_..	success or wait	1	430A4D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	86	4577F8	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	4577F8	ReadFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	unknown	1028	success or wait	1	41C715	ReadFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	unknown	1	success or wait	1	41C715	ReadFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	unknown	1	success or wait	57	41C715	ReadFile
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	65536	success or wait	1	43AE3E	ReadFile
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	64456	end of file	1	43AE3E	ReadFile
C:\Users\user\AppData\LocalLow\M8gHzW2avYe.zip	unknown	1181	success or wait	1	430AEE	ReadFile

Analysis Process: cmd.exe PID: 6740 Parent PID: 4516

General

Start time:	18:46:42
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q 'C:\Users\user\Desktop\SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe'
Imagebase:	0x350000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6748 Parent PID: 6740

General

Start time:	18:46:43
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6776 Parent PID: 6740

General

Start time:	18:46:43
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /T 10 /NOBREAK
Imagebase:	0x1050000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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 Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	unknown	16	0d 0a 57 61 69 74 69 6e 67 20 66 6f 72 20 31 30	..Waiting for 10	success or wait	1	1052DA7	fprintf
\Device\Null	unknown	34	20 73 65 63 6f 6e 64 73 2c 20 70 72 65 73 73 20 43 54 52 4c 2b 43 20 74 6f 20 71 75 69 74 20 2e 2e 2e	seconds, press CTRL+C to quit ...	success or wait	1	1052DA7	fprintf
\Device\Null	unknown	4	08 08 20 39	.. 9	success or wait	10	1052DA7	fprintf
\Device\Null	unknown	2	0d 0a	..	success or wait	1	1052DA7	fprintf

Disassembly

Code Analysis