ID: 800791
Sample Name:
ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe
Cookbook: default.jbs
Time: 19:53:55
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

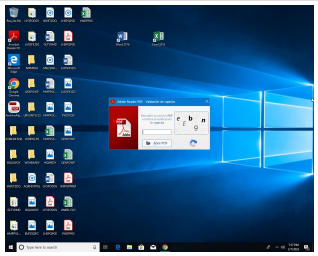
Windows Analysis Report

ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe

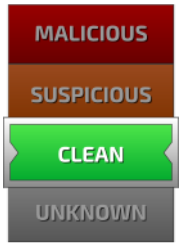
Overview

General Information

Sample Name:	ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe
Analysis ID:	800791
MD5:	a42b37fbf9d9b…
SHA1:	4efa169524085..
SHA256:	348a52936f4a5..
Infos:	



Detection

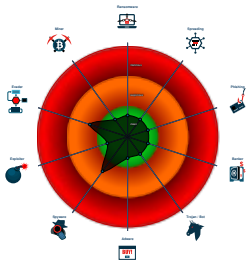


Score:	4
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

Signatures

- Uses 32bit PE files
- Found a high number of Window / U…
- Queries the volume information (nam…
- Installs a raw input device (often for…
- Sample file is different than original …
- PE file contains sections with non-s…
- Sample execution stops while proce…
- PE file contains more sections than…
- Yara detected Keylogger Generic

Classification



Analysis Advice

Sample monitors window changes (e.g. starting applications), analyze the sample with the 'Simulates keyboard and window changes' cookbook

Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")

Sample has functionality to log and monitor keystrokes, analyze it with the 'Simulates keyboard and window changes' cookbook

Process Tree

- **System is w10x64**
- ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe (PID: 3332 cmdline: C:\Users\user\Desktop\ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe MD5: A42B37FBF9D9B46986D062C75C6DA1B5)
  - splwow64.exe (PID: 992 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe PID: 3332	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

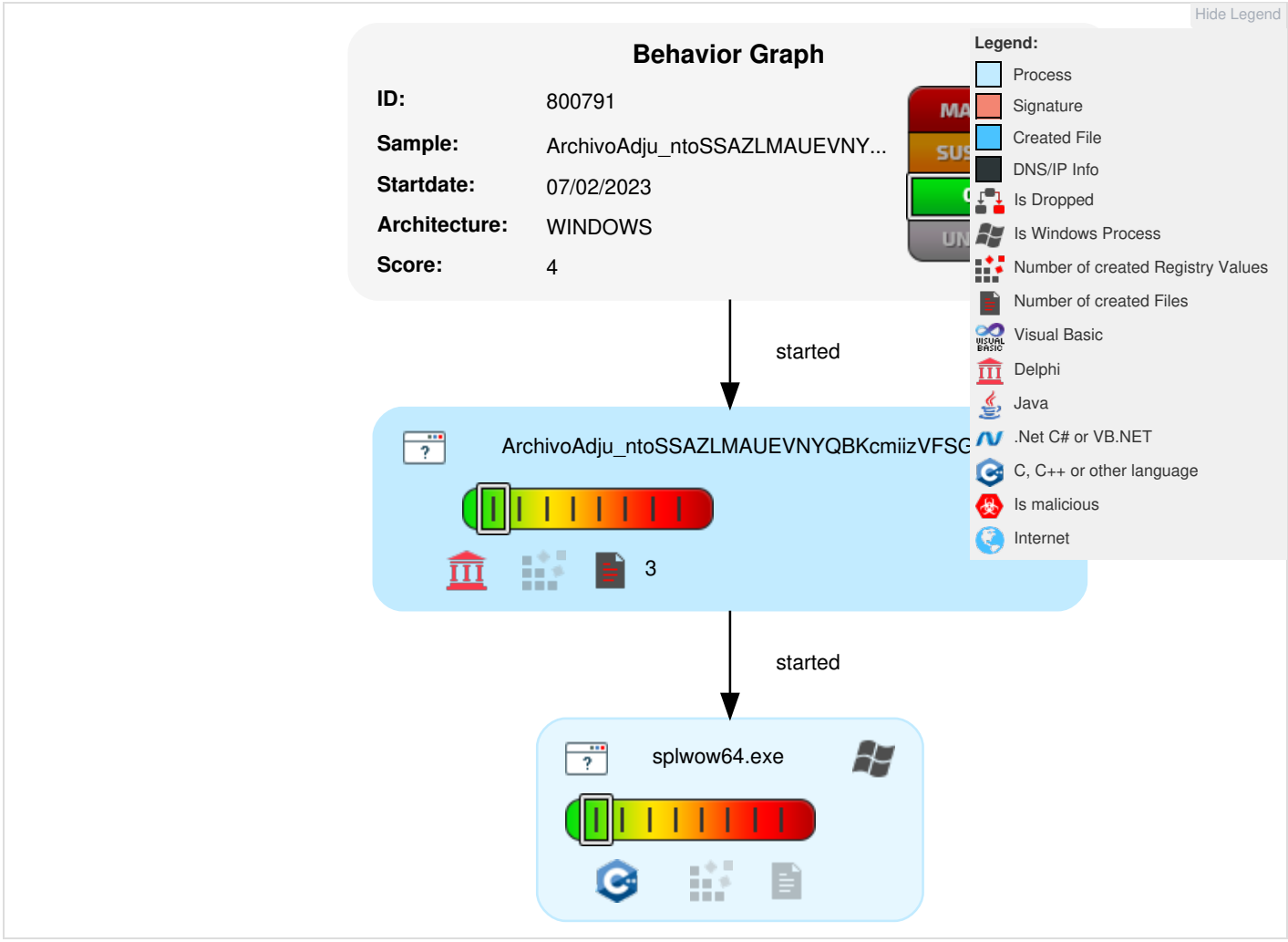
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	2 Process Injection	1 Virtualization/Sandbox Evasion	1 1 Input Capture	1 Process Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 Process Injection	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 1 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

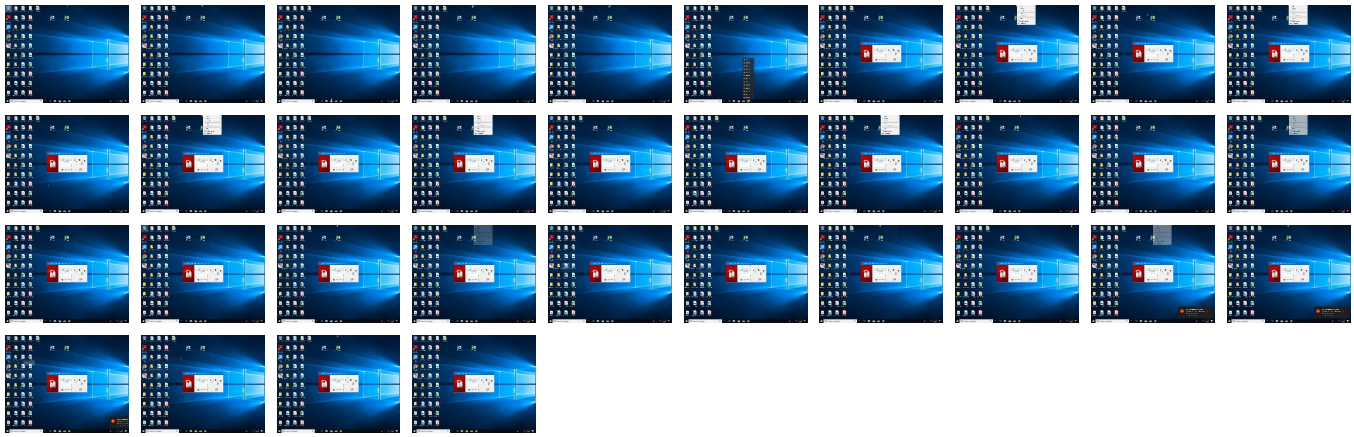
Behavior Graph



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

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.indyproject.org/	0%	URL Reputation	safe	
http://www.indyproject.org/	0%	URL Reputation	safe	
http://www.lmd.de	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.indyproject.org/	ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.lmd.de	ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800791
Start date and time:	2023-02-07 19:53:55 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
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
Sample file name:	ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe
Detection:	CLEAN
Classification:	clean4.winEXE@3/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:55:03	API Interceptor	982x Sleep call for process: splwow64.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	2.855975886001415
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe
File size:	331854848
MD5:	a42b37fbf9d9b46986d062c75c6da1b5
SHA1:	4efa169524085a15b81462dc4a1f34f25b23d4c4
SHA256:	348a52936f4a5bd079510503da07238b850da222cc0bb53f4758877e1c634216
SHA512:	bd8020ba4d896972c965702de7d3cb22a1455722d9f1b9c407c5c23414b9719be7db9cc71520b228ba5f95d182bd9ce03c65e48767e3d2ca8f1012a3512fb606
SSDEEP:	98304:j9mgS1GUfwtWszoq6fgE9GD5plJ52OaQl/zGRJ+cYzf9FCqeNzcLRfTCSyQ6G/Vr:j4gggCJfq5T7IHk
TLSH:	19F83912A2B050E6C0361A35542BB753593BEF132A1A4947EBBC3B5C0F3764D2937AF6
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	c0999126574f87d0

Static PE Info

General

Entrypoint:	0xb8adbc
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x63E1D386 [Tue Feb 7 04:28:54 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	b9ab4777064f6c17ac9b5de4c9f573b5

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00B74D28h
call 00007F73244B057Dh
mov eax, dword ptr [00BB1CF4h]
mov eax, dword ptr [eax]
call 00007F73246E7BADh
call 00007F7324C1294Ch
mov ecx, dword ptr [00BB1190h]
mov eax, dword ptr [00BB1CF4h]
mov eax, dword ptr [eax]
mov edx, dword ptr [00B6C244h]
call 00007F73246E7BA8h
mov eax, dword ptr [00BB1CF4h]
mov eax, dword ptr [eax]
call 00007F73246E7CFCh
call 00007F73244A8777h
mov eax, eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x7c5000	0x9a	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7bf000	0x4790	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x866000	0x13426e00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7c8000	0x9d5fc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x7c7000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7bfc60	0xaf8	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x7c4000	0xd3c	.didata
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	0x783ac4	0x783c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0x785000	0x5e08	0x6000	False	0.4846598307291667	data	6.146152286642337	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x78b000	0x27534	0x27600	False	0.457062251984127	data	6.4061502105155075	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x7b3000	0xb370	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x7bf000	0x4790	0x4800	False	0.3274739583333333	data	5.298490835152809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didata	0x7c4000	0xd3c	0xe00	False	0.3392857142857143	data	4.225694904508243	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0x7c5000	0x9a	0x200	False	0.2578125	data	1.9003166404108416	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0x7c6000	0x54	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x7c7000	0x5d	0x200	False	0.189453125	data	1.376793843926096	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7c8000	0x9d5fc	0x9d600	False	0.5316766158657665	data	6.706346424969919	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x866000	0x13426e00	0x13426e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x86b594	0x134	data	English	United States
RT_CURSOR	0x86b6c8	0x134	data	English	United States
RT_CURSOR	0x86b7fc	0x134	data	English	United States
RT_CURSOR	0x86b930	0x134	Targa image data - Map 64 x 65536 x 1 +32 "\001"	Russian	Russia
RT_CURSOR	0x86ba64	0x134	data		
RT_CURSOR	0x86bb98	0x134	data		
RT_CURSOR	0x86bccc	0x134	data		
RT_CURSOR	0x86be00	0x134	data		
RT_CURSOR	0x86bf34	0x134	data		
RT_CURSOR	0x86c068	0x134	data		
RT_CURSOR	0x86c19c	0x134	data		
RT_CURSOR	0x86c2d0	0x134	data		
RT_CURSOR	0x86c404	0x134	data		
RT_CURSOR	0x86c538	0x134	data		
RT_CURSOR	0x86c66c	0x134	data		

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x86c7a0	0x134	data		
RT_CURSOR	0x86c8d4	0x134	data	English	United States
RT_CURSOR	0x86ca08	0x134	Targa image data - Map 64 x 65536 x 1 +32 "\001"	English	United States
RT_CURSOR	0x86cb3c	0x134	data	English	United States
RT_CURSOR	0x86cc70	0x134	data	English	United States
RT_CURSOR	0x86cda4	0x134	data	English	United States
RT_CURSOR	0x86ced8	0x134	data	English	United States
RT_CURSOR	0x86d00c	0x134	data	English	United States
RT_CURSOR	0x86d140	0x134	Targa image data - RGB 64 x 65536 x 1 +32 "\001"	English	United States
RT_BITMAP	0x86d274	0xc0	Device independent bitmap graphic, 16 x 11 x 4, image size 88, 16 important colors	English	United States
RT_BITMAP	0x86d334	0xe0	Device independent bitmap graphic, 16 x 15 x 4, image size 120, 16 important colors	English	United States
RT_BITMAP	0x86d414	0xe0	Device independent bitmap graphic, 16 x 15 x 4, image size 120, 16 important colors	English	United States
RT_BITMAP	0x86d4f4	0x4c	Device independent bitmap graphic, 7 x 7 x 1, image size 28		
RT_BITMAP	0x86d540	0x44	Device independent bitmap graphic, 7 x 5 x 1, image size 20		
RT_BITMAP	0x86d584	0x44	Device independent bitmap graphic, 7 x 5 x 1, image size 20		
RT_BITMAP	0x86d5c8	0x88	Device independent bitmap graphic, 8 x 8 x 4, image size 32		
RT_BITMAP	0x86d650	0x1260	Device independent bitmap graphic, 280 x 13 x 8, image size 3640		
RT_BITMAP	0x86e8b0	0xc14	Device independent bitmap graphic, 154 x 13 x 8, image size 2028		
RT_BITMAP	0x86f4c4	0x78	Device independent bitmap graphic, 7 x 4 x 4, image size 16		
RT_BITMAP	0x86f53c	0xc8	Device independent bitmap graphic, 13 x 12 x 4, image size 96		
RT_BITMAP	0x86f604	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104		
RT_BITMAP	0x86f6d4	0xc0	Device independent bitmap graphic, 13 x 11 x 4, image size 88		
RT_BITMAP	0x86f794	0xf8	Device independent bitmap graphic, 20 x 12 x 4, image size 144		
RT_BITMAP	0x86f88c	0xf8	Device independent bitmap graphic, 20 x 12 x 4, image size 144		
RT_BITMAP	0x86f984	0x98	Device independent bitmap graphic, 9 x 6 x 4, image size 48		
RT_BITMAP	0x86fa1c	0x98	Device independent bitmap graphic, 9 x 6 x 4, image size 48		
RT_BITMAP	0x86fab4	0x84	Device independent bitmap graphic, 5 x 7 x 4, image size 28		
RT_BITMAP	0x86fb38	0x7c	Device independent bitmap graphic, 5 x 5 x 4, image size 20		
RT_BITMAP	0x86fbb4	0x84	Device independent bitmap graphic, 5 x 7 x 4, image size 28		
RT_BITMAP	0x86fc38	0x90	Device independent bitmap graphic, 9 x 5 x 4, image size 40		
RT_BITMAP	0x86fcc8	0xe8	Device independent bitmap graphic, 16 x 16 x 4, image size 128		
RT_BITMAP	0x86fdb0	0xe8	Device independent bitmap graphic, 16 x 16 x 4, image size 128		
RT_BITMAP	0x86fe98	0xe0	Device independent bitmap graphic, 16 x 15 x 4, image size 120, 16 important colors	English	United States
RT_BITMAP	0x86ff78	0xc0	Device independent bitmap graphic, 16 x 11 x 4, image size 88, 16 important colors	English	United States
RT_BITMAP	0x870038	0xc0	Device independent bitmap graphic, 16 x 11 x 4, image size 88, 16 important colors	English	United States
RT_BITMAP	0x8700f8	0x928	Device independent bitmap graphic, 24 x 24 x 32, image size 2304		
RT_BITMAP	0x870a20	0x928	Device independent bitmap graphic, 24 x 24 x 32, image size 2304		
RT_BITMAP	0x871348	0x928	Device independent bitmap graphic, 24 x 24 x 32, image size 2304		

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x871c70	0xe0	Device independent bitmap graphic, 16 x 15 x 4, image size 120, 16 important colors	English	United States
RT_BITMAP	0x871d50	0xb0	Device independent bitmap graphic, 9 x 9 x 4, image size 72		
RT_BITMAP	0x871e00	0x828	Device independent bitmap graphic, 64 x 16 x 8, image size 1024, resolution 2835 x 2835 px/m		
RT_BITMAP	0x872628	0xcc4	Device independent bitmap graphic, 114 x 19 x 8, image size 2204, resolution 2835 x 2835 px/m		
RT_BITMAP	0x8732ec	0x138	Device independent bitmap graphic, 28 x 13 x 4, image size 208		
RT_BITMAP	0x873424	0x108	Device independent bitmap graphic, 28 x 10 x 4, image size 160		
RT_BITMAP	0x87352c	0x340	Device independent bitmap graphic, 104 x 14 x 4, image size 728		
RT_BITMAP	0x87386c	0x168	Device independent bitmap graphic, 32 x 16 x 4, image size 256		
RT_BITMAP	0x8739d4	0x828	Device independent bitmap graphic, 32 x 32 x 8, image size 1024		
RT_BITMAP	0x8741fc	0x528	Device independent bitmap graphic, 16 x 16 x 8, image size 256		
RT_BITMAP	0x874724	0xe8	Device independent bitmap graphic, 16 x 16 x 4, image size 128		
RT_BITMAP	0x87480c	0xe8	Device independent bitmap graphic, 16 x 16 x 4, image size 128		
RT_BITMAP	0x8748f4	0xe8	Device independent bitmap graphic, 16 x 16 x 4, image size 128		
RT_BITMAP	0x8749dc	0xe8	Device independent bitmap graphic, 16 x 16 x 4, image size 128	German	Germany
RT_BITMAP	0x874ac4	0xf8	Device independent bitmap graphic, 20 x 12 x 4, image size 144, 16 important colors		
RT_BITMAP	0x874bbc	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x874c94	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x874d6c	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x874e44	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x874f1c	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x874ff4	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x8750cc	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x8751a4	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x87527c	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x875354	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x87542c	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x875504	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112		
RT_BITMAP	0x8755dc	0xf8	Device independent bitmap graphic, 20 x 12 x 4, image size 144, 16 important colors		
RT_BITMAP	0x8756d4	0x64	Device independent bitmap graphic, 5 x 3 x 32, image size 60, resolution 3780 x 3780 px/m	English	United States
RT_BITMAP	0x875738	0x64	Device independent bitmap graphic, 3 x 5 x 32, image size 60, resolution 3780 x 3780 px/m	English	United States
RT_BITMAP	0x87579c	0x64	Device independent bitmap graphic, 3 x 5 x 32, image size 60, resolution 3780 x 3780 px/m	English	United States
RT_BITMAP	0x875800	0x64	Device independent bitmap graphic, 5 x 3 x 32, image size 60, resolution 3780 x 3780 px/m	English	United States

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x875864	0x64	Device independent bitmap graphic, 5 x 3 x 32, image size 60, resolution 3780 x 3780 px/m	English	United States
RT_BITMAP	0x8758c8	0x64	Device independent bitmap graphic, 3 x 5 x 32, image size 60, resolution 3780 x 3780 px/m	English	United States
RT_BITMAP	0x87592c	0x64	Device independent bitmap graphic, 3 x 5 x 32, image size 60, resolution 3780 x 3780 px/m	English	United States
RT_BITMAP	0x875990	0x64	Device independent bitmap graphic, 5 x 3 x 32, image size 60, resolution 3780 x 3780 px/m	English	United States
RT_BITMAP	0x8759f4	0xb0	Device independent bitmap graphic, 9 x 9 x 4, image size 72		
RT_BITMAP	0x875aa4	0xc0	Device independent bitmap graphic, 16 x 11 x 4, image size 88, 16 important colors	English	United States
RT_BITMAP	0x875b64	0xe0	Device independent bitmap graphic, 16 x 15 x 4, image size 120, 16 important colors	English	United States
RT_BITMAP	0x875c44	0xb0	Device independent bitmap graphic, 9 x 9 x 4, image size 72		
RT_BITMAP	0x875cf4	0x328	Device independent bitmap graphic, 16 x 16 x 24, image size 768, resolution 2834 x 2834 px/m	Russian	Russia
RT_BITMAP	0x87601c	0xc0	Device independent bitmap graphic, 16 x 11 x 4, image size 88, 16 important colors	English	United States
RT_BITMAP	0x8760dc	0x95c61e8	Device independent bitmap graphic, 9960 x 5256 x 24, image size 157049280	Portuguese	Brazil
RT_BITMAP	0x9e3c2c4	0x9d81e28	Device independent bitmap graphic, 9200 x 5984 x 24, image size 165158400	Portuguese	Brazil
RT_BITMAP	0x13bbe0ec	0xe0	Device independent bitmap graphic, 16 x 15 x 4, image size 120, 16 important colors	English	United States
RT_ICON	0x13bbe1cc	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x13bbe634	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x13bbefbc	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x13bc0064	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x13bc260c	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x13bc6834	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016	English	United States
RT_ICON	0x13bcfcdc	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x13be0504	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 270336	English	United States
RT_ICON	0x13c2252c	0xa5b9	PNG image data, 512 x 512, 8-bit/color RGBA, non-interlaced	English	United States
RT_DIALOG	0x13c2cae8	0x496	data	Russian	Russia
RT_DIALOG	0x13c2cf80	0x48e	data	Russian	Russia
RT_DIALOG	0x13c2d410	0x52	data		
RT_STRING	0x13c2d464	0x19c	data		
RT_STRING	0x13c2d600	0x44	data		
RT_STRING	0x13c2d644	0x154	data		
RT_STRING	0x13c2d798	0x650	data		
RT_STRING	0x13c2dde8	0x200	data		
RT_STRING	0x13c2dfe8	0xf8	data		
RT_STRING	0x13c2e0e0	0x170	data		
RT_STRING	0x13c2e250	0x16c	data		
RT_STRING	0x13c2e3bc	0x12c	data		
RT_STRING	0x13c2e4e8	0x190	data		
RT_STRING	0x13c2e678	0x198	data		
RT_STRING	0x13c2e810	0x1fc	data		
RT_STRING	0x13c2ea0c	0x310	data		
RT_STRING	0x13c2ed1c	0x1c8	data		
RT_STRING	0x13c2eee4	0x478	data		
RT_STRING	0x13c2f35c	0x294	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x13c2f5f0	0x40c	data		
RT_STRING	0x13c2f9fc	0x584	data		
RT_STRING	0x13c2ff80	0x218	data		
RT_STRING	0x13c30198	0x858	data		
RT_STRING	0x13c309f0	0xab0	data		
RT_STRING	0x13c314a0	0x3c0	data		
RT_STRING	0x13c31860	0x424	data		
RT_STRING	0x13c31c84	0x790	data		
RT_STRING	0x13c32414	0x1104	data		
RT_STRING	0x13c33518	0x9d4	data		
RT_STRING	0x13c33eec	0x8d4	data		
RT_STRING	0x13c347c0	0x8a8	data		
RT_STRING	0x13c35068	0x444	data		
RT_STRING	0x13c354ac	0x2ac	data		
RT_STRING	0x13c35758	0x5a4	data		
RT_STRING	0x13c35cfc	0x3d4	data		
RT_STRING	0x13c360d0	0x430	data		
RT_STRING	0x13c36500	0x34c	data		
RT_STRING	0x13c3684c	0x454	data		
RT_STRING	0x13c36ca0	0x370	data		
RT_STRING	0x13c37010	0x390	data		
RT_STRING	0x13c373a0	0x27c	data		
RT_STRING	0x13c3761c	0x3f0	data		
RT_STRING	0x13c37a0c	0x5c4	data		
RT_STRING	0x13c37fd0	0x3d0	data		
RT_STRING	0x13c383a0	0x2d4	data		
RT_STRING	0x13c38674	0x430	data		
RT_STRING	0x13c38aa4	0x4cc	data		
RT_STRING	0x13c38f70	0x43c	data		
RT_STRING	0x13c393ac	0x470	data		
RT_STRING	0x13c3981c	0x4a8	data		
RT_STRING	0x13c39cc4	0x398	data		
RT_STRING	0x13c3a05c	0x3a0	data		
RT_STRING	0x13c3a3fc	0x38c	data		
RT_STRING	0x13c3a788	0xac	data		
RT_STRING	0x13c3a834	0xd0	data		
RT_STRING	0x13c3a904	0x2c8	data		
RT_STRING	0x13c3abcc	0x280	data		
RT_STRING	0x13c3ae4c	0x404	data		
RT_STRING	0x13c3b250	0x3cc	data		
RT_STRING	0x13c3b61c	0x43c	data		
RT_STRING	0x13c3ba58	0x4e0	data		
RT_STRING	0x13c3bf38	0x250	data		
RT_STRING	0x13c3c188	0x3c0	data		
RT_STRING	0x13c3c548	0x434	data		
RT_STRING	0x13c3c97c	0x694	data		
RT_STRING	0x13c3d010	0x490	data		
RT_STRING	0x13c3d4a0	0x300	data		
RT_STRING	0x13c3d7a0	0x388	data		
RT_STRING	0x13c3db28	0x3b8	data		
RT_STRING	0x13c3dee0	0x33c	data		
RT_STRING	0x13c3e21c	0xd0	data		
RT_STRING	0x13c3e2ec	0xa0	data		
RT_STRING	0x13c3e38c	0x300	data		
RT_STRING	0x13c3e68c	0x46c	data		
RT_STRING	0x13c3eaf8	0x2f8	data		
RT_STRING	0x13c3edf0	0x2f0	data		
RT_STRING	0x13c3f0e0	0x378	data		

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x13c3f458	0xd5d	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c401b8	0xd57	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c40f10	0xcfc	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c41c0c	0xcd9	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c428e8	0xd5d	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c43648	0xd57	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c443a0	0xc4e	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c44ff0	0xc4e	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c45c40	0xcb5	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c468f8	0xcb0	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c475a8	0xd56	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c48300	0xd47	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c49048	0xdc2	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c49e0c	0xdc5	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c4abd4	0xcf3	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c4b8c8	0xced	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c4c5b8	0xda9	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c4d364	0xda6	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c4e10c	0xcf3	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c4ee00	0xced	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c4faf0	0xbfe	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c506f0	0xd04	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c513f4	0xc0e	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c52004	0xc1b	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c52c20	0xd36	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c53958	0xd0f	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c54668	0xb07	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c55170	0xb29	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c55c9c	0xb7b	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c56818	0xbd4	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c573ec	0xb8d	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c57f7c	0xc13	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c58b90	0xb1d	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c596b0	0xb45	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c5a1f8	0xb86	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x13c5ad80	0xc00	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c5b980	0xb7a	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c5c4fc	0xbf6	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c5d0f4	0xbeb	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c5dce0	0xc85	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c5e968	0xb83	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c5f4ec	0xc03	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c600f0	0xc2c	PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c60d1c	0xd45	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c61a64	0x10	data		
RT_RCDATA	0x13c61a74	0x24b	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced		
RT_RCDATA	0x13c61cc0	0x30a	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced		
RT_RCDATA	0x13c61fcc	0x312	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced		
RT_RCDATA	0x13c622e0	0x29a	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced		
RT_RCDATA	0x13c6257c	0xa6	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c62624	0xcf	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c626f4	0xef	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c627e4	0xd9	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c628c0	0x10d	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c629d0	0x13f	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c62b10	0x136	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c62c48	0x192	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c62ddc	0x1ca	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c62fa8	0xd7	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c63080	0x10f	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c63190	0x138	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c632c8	0x70	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c63338	0x78	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c633b0	0x7e	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c63430	0xc5	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c634f8	0xec	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c635e4	0x113	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c636f8	0x10e	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c63808	0x163	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c6396c	0x1a3	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c63b10	0x1f5	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x13c63d08	0x2f0	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c63ff8	0x3b3	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c643ac	0x80	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c6442c	0x8a	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c644b8	0x98	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c64550	0xc5	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c64618	0xe1	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c646fc	0x10f	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c6480c	0x17a	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c64988	0x204	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c64b8c	0x215	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c64da4	0x163	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c64f08	0x1b8	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c650c0	0x22e	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c652f0	0xc0	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c653b0	0x105	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c654b8	0x1cd	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c65688	0x134	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c657bc	0x183	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c65940	0x1c8	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c65b08	0xc5	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c65bd0	0xed	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c65cc0	0xe7	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c65da8	0x157	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c65f00	0x1a7	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c660a8	0x209	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c662b4	0x148b	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c67740	0x111e	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c68860	0xd8c	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13c695ec	0x269c	data		
RT_RCDATA	0x13c6bc88	0x2	data	English	United States
RT_RCDATA	0x13c6bc8c	0x20c6	Delphi compiled form 'TElCalculatorForm'		
RT_RCDATA	0x13c6dd54	0x1ce	Delphi compiled form 'TElPromptForm'		
RT_RCDATA	0x13c6df24	0x115c5	Delphi compiled form 'TF000x049050392477771238995439'		
RT_RCDATA	0x13c7f4ec	0x364	Delphi compiled form 'TfrmLMDRichInsertDateTimeDlg'		
RT_RCDATA	0x13c7f850	0x53b	Delphi compiled form 'TfrmLMDRTFCharmapDialog'		
RT_RCDATA	0x13c7fd8c	0x388	Delphi compiled form 'TLMDPrintPreviewForm'		

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x13c80114	0x1e8	Delphi compiled form 'TLMDPrintPreviewModeDialog'		
RT_RCDATA	0x13c802fc	0x23d	Delphi compiled form 'TLMDPrintResDataModule'		
RT_RCDATA	0x13c8053c	0x4b1	Delphi compiled form 'TLMDRichfrmBookMarks'		
RT_RCDATA	0x13c809f0	0x4d3	Delphi compiled form 'TLMDRichfrmLinkDialog'		
RT_RCDATA	0x13c80ec4	0xf57	Delphi compiled form 'TLMDRichfrmParagraph'		
RT_RCDATA	0x13c81e1c	0x2ffc	Delphi compiled form 'TLMDRichfrmPrintPreview'		
RT_RCDATA	0x13c84e18	0x4b1	Delphi compiled form 'TLMDRichfrmTabs'		
RT_RCDATA	0x13c852cc	0x58d	Delphi compiled form 'TLMDRTFStatisticsDlg'		
RT_RCDATA	0x13c8585c	0x430a	Delphi compiled form 'TLMDTemplateEditDialog'		
RT_RCDATA	0x13c89b68	0x488	Delphi compiled form 'TLoginDialog'		
RT_RCDATA	0x13c89ff0	0x3c4	Delphi compiled form 'TPasswordDialog'		
RT_RCDATA	0x13c8a3b4	0x1c6a	Delphi compiled form 'TRTFPrintPreviewMode'		
RT_GROUP_CURSOR	0x13c8c020	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x13c8c034	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x13c8c048	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x13c8c05c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x13c8c070	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x13c8c084	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x13c8c098	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x13c8c0ac	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x13c8c0c0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0x13c8c0d4	0x84	data	English	United States
RT_VERSION	0x13c8c158	0x458	data	English	United States
RT_MANIFEST	0x13c8c5b0	0x70b	XML 1.0 document, ASCII text, with CRLF, LF line terminators	English	United States

Imports

DLL	Import
mpr.dll	WNetGetConnectionW
winmm.dll	sndPlaySoundW, PlaySoundW, timeGetTime, timeSetEvent, timeKillEvent, waveOutGetNumDevs
winspool.drv	DocumentPropertiesW, ClosePrinter, OpenPrinterW, GetDefaultPrinterW, EnumPrintersW
comdlg32.dll	PageSetupDlgW, ChooseFontW, CommDlgExtendedError, ChooseColorW, GetSaveFileNameW, GetOpenFileNameW, PrintDlgW
comctl32.dll	ImageList_GetImageInfo, FlatSB_SetScrollInfo, InitCommonControls, ImageList_DragMove, ImageList_Destroy, _TrackMouseEvent, ImageList_DragShowNolock, ImageList_Add, FlatSB_SetScrollProp, ImageList_GetDragImage, ImageList_Create, ImageList_EndDrag, ImageList_DrawEx, ImageList_SetImageCount, FlatSB_GetScrollPos, FlatSB_SetScrollPos, InitializeFlatSB, ImageList_Copy, FlatSB_GetScrollInfo, ImageList_Write, ImageList_DrawIndirect, ImageList_SetBkColor, ImageList_GetBkColor, ImageList_BeginDrag, ImageList_GetIcon, ImageList_Replace, ImageList_GetImageCount, ImageList_DragEnter, ImageList_GetIconSize, ImageList_SetIconSize, ImageList_Read, ImageList_DragLeave, ImageList_LoadImageW, ImageList_Draw, ImageList_Remove, ImageList_ReplaceIcon, ImageList_SetOverlayImage
shell32.dll	SHBrowseForFolderW, DragQueryFileW, SHGetSpecialFolderLocation, Shell_NotifyIconW, DragAcceptFiles, ShellExecuteExW, SHGetPathFromIDListW, DragFinish, SHGetFileInfoW, SHGetMalloc, SHGetDesktopFolder, SHAppBarMessage, ShellExecuteW

DLL	Import
user32.dll	CopyImage, MoveWindow, SetMenuItemInfoW, GetMenuItemInfoW, DefFrameProcW, SetCaretPos, GetCaretPos, ScrollWindowEx, GetDlgCtrlID, FrameRect, RegisterWindowMessageW, GetMenuStringW, FillRect, SendMessageA, IsClipboardFormatAvailable, EnumWindows, ShowOwnedPopups, GetClassInfoW, GetScrollRange, SetActiveWindow, GetActiveWindow, DrawEdge, GetKeyboardLayoutList, OemToCharBuffA, LoadBitmapW, EnumChildWindows, GetScrollBarInfo, UnhookWindowsHookEx, SetCapture, GetCapture, CreatePopupMenu, LoadMenuW, ShowCaret, GetMenuItemID, DestroyCaret, CharLowerBuffW, PostMessageW, SetWindowLongW, IsZoomed, SetParent, DrawMenuBar, GetClientRect, IsChild, SendDlgItemMessageW, IntersectRect, IsIconic, CallNextHookEx, ShowWindow, SetForegroundWindow, GetWindowTextW, IsDialogMessageW, DestroyWindow, RegisterClassW, EndMenu, CharNextW, GetFocus, GetDC, SetFocus, ReleaseDC, ExitWindowsEx, GetClassLongW, CharToOemBuffA, SetScrollRange, DrawTextW, PeekMessageA, MessageBeep, SetClassLongW, SetRectEmpty, RemovePropW, GetSubMenu, DestroyIcon, IsWindowVisible, IsCharUpperW, CharPrevW, PtInRect, DispatchMessageA, UnregisterClassW, GetTopWindow, SendMessageW, GetMessageTime, CreateMenu, LoadStringW, CharLowerW, IsCharLowerW, SetWindowRgn, SetWindowPos, GetMenuItemCount, GetSysColorBrush, GetWindowDC, DrawTextExW, CharLowerBuffA, EnumClipboardFormats, GetScrollInfo, SetWindowTextW, GetMessageExtraInfo, GetSysColor, EnableScrollBar, TrackPopupMenu, DrawIconEx, GetClassNameW, GetMessagePos, GetIconInfo, SetScrollInfo, GetKeyNameTextW, GetDesktopWindow, SetCursorPos, GetCursorPos, SetMenu, GetMenuState, GetMenu, SetRect, GetKeyState, IsRectEmpty, ValidateRect, IsCharAlphaW, GetCursor, KillTimer, WaitMessage, TranslateMDISysAccel, GetWindowPlacement, GetClipboardFormatNameW, CreateIconIndirect, CreateWindowExW, GetDCEx, PeekMessageW, MonitorFromWindow, GetUpdateRect, SetTimer, WindowFromPoint, BeginPaint, RegisterClipboardFormatW, MapVirtualKeyW, OffsetRect, IsWindowUnicode, CharToOemA, DispatchMessageW, CreateAcceleratorTableW, DefMDIChildProcW, GetSystemMenu, SetScrollPos, GetScrollPos, InflateRect, DrawFocusRect, ReleaseCapture, LoadCursorW, ScrollWindow, GetLastActivePopup, GetSystemMetrics, CharUpperBuffW, ClientToScreen, SetClipboardData, GetClipboardData, SetWindowPlacement, SetCaretBlinkTime, GetCaretBlinkTime, InvertRect, GetMonitorInfoW, CheckMenuItem, CharUpperW, DefWindowProcW, GetForegroundWindow, EnableWindow, GetWindowThreadProcessId, RedrawWindow, EndPaint, MsgWaitForMultipleObjectsEx, LoadKeyboardLayoutW, ActivateKeyboardLayout, DestroyAcceleratorTable, GetParent, CreateCaret, MonitorFromRect, InsertMenuItemW, GetPropW, MessageBoxW, SetPropW, UpdateWindow, MsgWaitForMultipleObjects, OemToCharA, DestroyMenu, SetWindowsHookExW, GetDoubleClickTime, EmptyClipboard, GetDlgItem, AdjustWindowRectEx, IsWindow, DrawIcon, EnumThreadWindows, InvalidateRect, SetKeyboardState, GetKeyboardState, ScreenToClient, DrawFrameControl, IsCharAlphaNumericW, SetCursor, CreateIcon, GetDialogBaseUnits, RemoveMenu, SubtractRect, GetKeyboardLayoutNameW, OpenClipboard, TranslateMessage, MapWindowPoints, EnumDisplayMonitors, CallWindowProcW, CountClipboardFormats, CloseClipboard, DestroyCursor, CharUpperBuffA, CopyIcon, PostQuitMessage, ShowScrollBar, EnableMenuItem, HideCaret, FindWindowExW, MonitorFromPoint, LoadIconW, SystemParametersInfoW, GetWindow, GetWindowLongW, GetWindowRect, ToUnicode, InsertMenuW, IsWindowEnabled, IsDialogMessageA, FindWindowW, DeleteMenu, GetKeyboardLayout
version.dll	GetFileVersionInfoSizeW, VerQueryValueW, GetFileVersionInfoW
oledlg.dll	OleUIPasteSpecialW, OleUIObjectPropertiesW, OleUIInsertObjectA
oleaut32.dll	SafeArrayPutElement, SetErrorInfo, GetErrorInfo, VariantInit, VariantClear, SysFreeString, SafeArrayAccessData, SysReAllocStringLen, SafeArrayCreate, CreateErrorInfo, SafeArrayGetElement, SysAllocStringLen, SafeArrayUnaccessData, SafeArrayPtrOfIndex, VariantCopy, SafeArrayGetUBound, SafeArrayGetLBound, VariantCopyInd, VariantChangeType
advapi32.dll	RegSetValueExW, RegConnectRegistryW, RegEnumKeyExW, RegLoadKeyW, AdjustTokenPrivileges, GetUserNameW, RegDeleteKeyW, LookupPrivilegeValueW, OpenProcessToken, RegOpenKeyExW, RegQueryInfoKeyW, RegUnLoadKeyW, RegSaveKeyW, RegDeleteValueW, RegReplaceKeyW, RegFlushKey, RegQueryValueExW, RegEnumValueW, RegCloseKey, RegCreateKeyExW, RegRestoreKeyW
msvcrt.dll	memcpy, memset
kernel32.dll	SetFileAttributesW, GetFileType, SetFileTime, QueryDosDeviceW, GetACP, CloseHandle, LocalFree, GetCurrentProcessId, SizeofResource, VirtualProtect, ReadProcessMemory, OpenFileMappingW, QueryPerformanceFrequency, IsDebuggerPresent, FindNextFileW, FlushInstructionCache, GetFullPathNameW, VirtualFree, HeapAlloc, ExitProcess, GetCPInfoExW, GlobalSize, GetSystemTime, WriteProcessMemory, RtlUnwind, GetCPInfo, EnumSystemLocalesW, GetStdHandle, GetTimeZoneInformation, FileTimeToLocalFileTime, SystemTimeToTzSpecificLocalTime, GetModuleHandleW, FreeLibrary, TryEnterCriticalSection, HeapDestroy, FileTimeToDosDateTime, ReadFile, DosDateTimeToFileTime, GetUserDefaultLCID, IsBadCodePtr, GetLastError, GetModuleFileNameW, SetLastError, GlobalAlloc, GlobalUnlock, DisableThreadLibraryCalls, FindResourceW, CreateThread, CompareStringW, CopyFileW, MapViewOfFile, CreateMutexW, LoadLibraryA, GetVolumeInformationW, ResetEvent, MulDiv, FreeResource, GetDriveTypeW, GetVersion, RaiseException, MoveFileW, GlobalAddAtomW, FormatMessageW, OpenProcess, SwitchToThread, GetExitCodeThread, OutputDebugStringW, GetCurrentThread, GetLogicalDrives, LocalFileTimeToFileTime, GetFileAttributesExW, LoadLibraryExW, LockResource, FileTimeToSystemTime, GetCurrentThreadId, UnhandledExceptionFilter, GlobalFindAtomW, VirtualQuery, GlobalFree, VirtualQueryEx, Sleep, SetVolumeLabelW, EnterCriticalSection, SetFilePointer, FlushFileBuffers, LoadResource, SuspendThread, GetTickCount, WritePrivateProfileStringW, GetTempFileNameW, GetFileSize, GlobalDeleteAtom, GetStartupInfoW, GetFileAttributesW, GetCurrentDirectoryW, SetCurrentDirectoryW, InitializeCriticalSection, GetThreadPriority, GetCurrentProcess, GlobalLock, SetThreadPriority, VirtualAlloc, GetTempPathW, GetCommandLineW, GetSystemInfo, DuplicateHandle, LeaveCriticalSection, GetProcAddress, ResumeThread, GetLogicalDriveStringsW, GetVersionExW, VerifyVersionInfoW, HeapCreate, GetWindowsDirectoryW, LCMapStringW, GetDiskFreeSpaceW, VerSetConditionMask, FindFirstFileW, GetUserDefaultUILanguage, GetConsoleOutputCP, UnmapViewOfFile, GetConsoleCP, lstrlenW, SetEndOfFile, QueryPerformanceCounter, lstrcmpW, HeapFree, WideCharToMultiByte, FindClose, MultiByteToWideChar, LoadLibraryW, SetEvent, GetLocaleInfoW, CreateFileW, SystemTimeToFileTime, EnumResourceNamesW, GetSystemDirectoryW, DeleteFileW, IsDBCSLeadByteEx, GetEnvironmentVariableW, GetLocalTime, WaitForSingleObject, WriteFile, CreateFileMappingW, ExitThread, DeleteCriticalSection, GetDateFormatW, GetTimeFormatW, TlsGetValue, SetErrorMode, GetComputerNameW, TzSpecificLocalTimeToSystemTime, IsValidLocale, TlsSetValue, CreateDirectoryW, GetSystemDefaultUILanguage, EnumCalendarInfoW, LocalAlloc, RemoveDirectoryW, CreateEventW, GetPrivateProfileStringW, WaitForMultipleObjectsEx, GetThreadLocale, SetThreadLocale
SHFolder.dll	SHGetFolderPathW
wsock32.dll	htons, ntohs, setsockopt, WSAStartup, WSACleanup, listen, gethostbyname, gethostname, closesocket, inet_ntoa, socket, recv, ioctlsocket, WSAGetLastError, shutdown, inet_addr, WSACancelAsyncRequest, send, WSAAsyncGetHostByName
ole32.dll	StgCreateDocfileOnILockBytes, CreateBindCtx, MkParseDisplayName, CoCreateGuid, OleCreateStaticFromData, CoCreateInstance, IsEqualGUID, CreateILockBytesOnHGlobal, StringFromGUID2, OleCreateFromData, CLSIDFromProgID, CoInitialize, CoTaskMemAlloc, DoDragDrop, RevokeDragDrop, OleGetIconOfClass, CoUninitialize, RegisterDragDrop, OleInitialize, OleSetContainedObject, OleUninitialize, CoInitializeEx, OleCreateLinkFromData, CoTaskMemFree, OleSetMenuDescriptor

DLL	Import
gdi32.dll	AddFontMemResourceEx, Pie, SetBkMode, CreateCompatibleBitmap, CreatePolygonRgn, BeginPath, GetEnhMetaFileHeader, CloseEnhMetaFile, RectVisible, AngleArc, ResizePalette, SetAbortProc, SetTextColor, GetTextColor, StretchBlt, ExtSelectClipRgn, RoundRect, SelectClipRgn, RestoreDC, SetRectRgn, GetTextMetricsW, GetWindowOrgEx, CreatePalette, CreateDCW, CreateICW, CreatePen, PolyBezierTo, GetStockObject, CreateSolidBrush, Polygon, MoveToEx, PlayEnhMetaFile, Ellipse, StartPage, GetBitmapBits, SetTextCharacterExtra, StartDocW, AbortDoc, GetSystemPaletteEntries, GetEnhMetaFileBits, CreatePenIndirect, GetEnhMetaFilePaletteEntries, SetMapMode, GetMapMode, CreateFontIndirectW, PolyBezier, ExtCreatePen, DeleteMetaFile, EndDoc, GetObjectW, GetWinMetaFileBits, SetROP2, GetTextExtentExPointW, GetEnhMetaFileDescriptionW, ArcTo, CreateEnhMetaFileW, Arc, CreateRectRgnIndirect, TextOutW, SelectPalette, ExcludeClipRect, SetWindowOrgEx, MaskBlt, EndPath, EndPage, DeleteEnhMetaFile, Chord, SetDIBits, SetViewportOrgEx, CreateRectRgn, RealizePalette, SetDIBColorTable, GetDIBColorTable, OffsetClipRgn, CreateBrushIndirect, PatBlt, StrokePath, SetEnhMetaFileBits, CreateEllipticRgn, Rectangle, DeleteDC, SaveDC, BitBlt, FrameRgn, GetDeviceCaps, GetTextExtentPoint32W, PtInRegion, GetClipBox, GetClipRgn, Polyline, IntersectClipRect, CreateBitmap, CombineRgn, SetWinMetaFileBits, CreateDIBitmap, GetStretchBltMode, CreateDIBSection, SetStretchBltMode, GetDIBits, LineTo, GetRgnBox, EnumFontsW, EnumFontFamiliesW, SetWindowExtEx, CreateHalftonePalette, DeleteObject, SelectObject, ExtFloodFill, UnrealizeObject, CopyEnhMetaFileW, OffsetRgn, SetBkColor, GetBkColor, CreateCompatibleDC, GetBrushOrgEx, GetCurrentPositionEx, GetNearestPaletteIndex, SetTextAlign, GetTextAlign, RemoveFontMemResourceEx, GetTextExtentPointW, ExtTextOutW, SetBrushOrgEx, GetPixel, GdiFlush, SetViewportExtEx, SetPixel, PolyPolyline, EnumFontFamiliesExW, StretchDIBits, GetPaletteEntries

Exports

Name	Ordinal	Address
TMethodImplementationIntercept	3	0x4771e8
__dbk_fcall_wrapper	2	0x412758
dbkFCallWrapperAddr	1	0xbb663c

Possible Origin

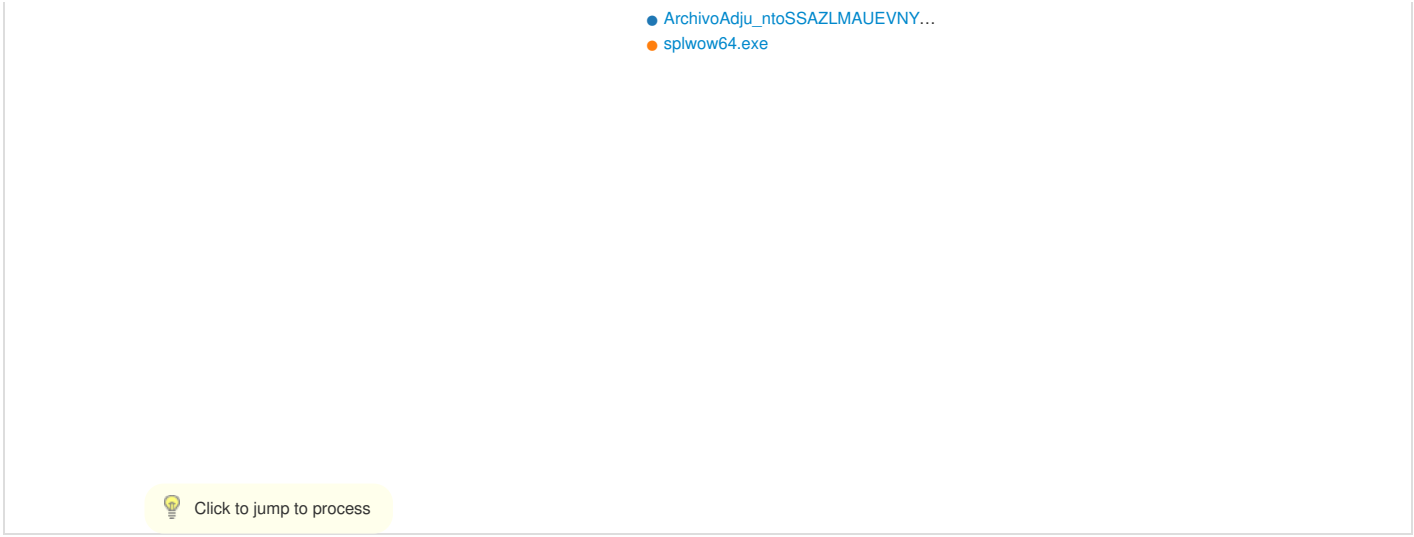
Language of compilation system	Country where language is spoken	Map
English	United States	
Russian	Russia	
German	Germany	
Portuguese	Brazil	

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe PID: 3332, Parent PID: 3528

General

Target ID:	0
Start time:	19:55:00
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ArchivoAdju_ntoSSAZLMAUEVNYQBKcmiizVFSGC.exe
Imagebase:	0x400000
File size:	331854848 bytes
MD5 hash:	A42B37FBF9D9B46986D062C75C6DA1B5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: splwow64.exe PID: 992, Parent PID: 3332

General

Target ID:	1
Start time:	19:55:03
Start date:	07/02/2023
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff607170000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true

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

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly