ID: 632527
Sample Name:
ibaAnalyzerSetup_x64_v7.3.6.exe
Cookbook: default.jbs
Time: 18:41:07
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

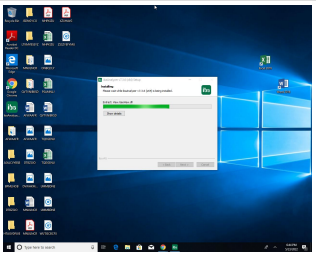
Windows Analysis Report

ibaAnalyzerSetup_x64_v7.3.6.exe

Overview

General Information

Sample Name:	ibaAnalyzerSetup_x64_v7.3.6.exe
Analysis ID:	632527
MD5:	c1ae350f67039c…
SHA1:	6362ba848a6027.
SHA256:	fbf6ebb863e6ee1.
Infos:	



Detection

Score:	24
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

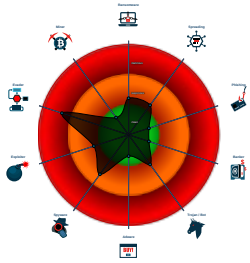
Compliance

Score:	34
Range:	0 - 100

Signatures

- Found evasive API chain (may stop…
- Tries to detect virtualization through…
- Uses 32bit PE files
- Queries the volume information (nam…
- Antivirus or Machine Learning detec…
- Contains functionality to check if a d…
- Contains functionality to query local…
- May sleep (evasive loops) to hinder…
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Found evasive API chain (date chec…
- PE file contains sections with non-s…
- Detected potential crypto function

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox

Sample may be VM or Sandbox-aware, try analysis on a native machine

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Process Tree

- **System is w10x64**
- ibaAnalyzerSetup_x64_v7.3.6.exe (PID: 7052 cmdline: "C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe" MD5: C1AE350F67039CBE69F10DF9B8001371)
  - regsvr32.exe (PID: 3544 cmdline: C:\Windows\system32\regsvr32.exe" /s "C:\Program Files\iba\ibaAnalyzer\ibaHDOfflineActiveX.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
    - regsvr32.exe (PID: 4904 cmdline: /s "C:\Program Files\iba\ibaAnalyzer\ibaHDOfflineActiveX.ocx" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 5848 cmdline: C:\Windows\system32\regsvr32.exe" /s "C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostActiveX.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
    - regsvr32.exe (PID: 6048 cmdline: /s "C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostActiveX.ocx" MD5: D78B75FC68247E8A63ACBA846182740E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Compliance

Uses 32bit PE files

DLL planting / hijacking vulnerabilities found

Found installer window with terms and condition text

Creates license or readme file

Creates a directory in C:\Program Files

PE / OLE file has a valid certificate

Binary contains paths to debug symbols

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking mutex)

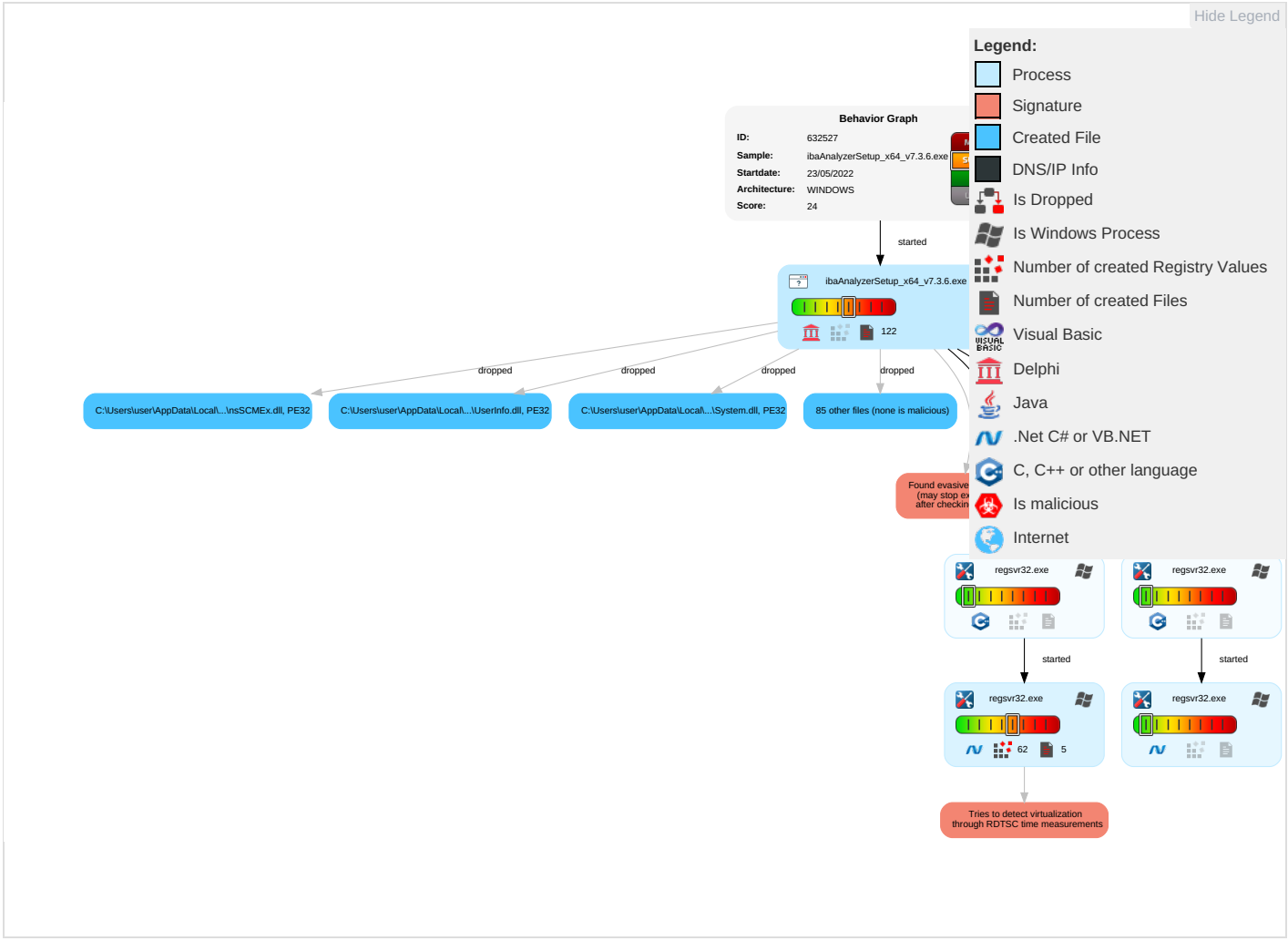
Tries to detect virtualization through RDTSC time measurements

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
1 Valid Accounts	1 3 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 2 Service Execution	1 DLL Search Order Hijacking	1 DLL Search Order Hijacking	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Peripheral Device Discovery	Remote Desktop Protocol	2 Clipboard Data	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 Valid Accounts	1 Valid Accounts	3 Obfuscated Files or Information	Security Account Manager	1 Account 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)	1 2 Windows Service	1 1 Access Token Manipulation	1 Software Packing	NTDS	1 System Service Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 2 Windows Service	1 Timestomp	LSA Secrets	3 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	1 Process Injection	1 DLL Side-Loading	Cached Domain Credentials	1 3 7 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Search Order Hijacking	DCSync	1 Query Registry	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Masquerading	Proc Filesystem	1 4 Security Software Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Valid Accounts	/etc/passwd and /etc/shadow	2 2 Virtualization/Sandbox Evasion	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	2 2 Virtualization/Sandbox Evasion	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 1 Access Token Manipulation	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	1 Process Injection	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

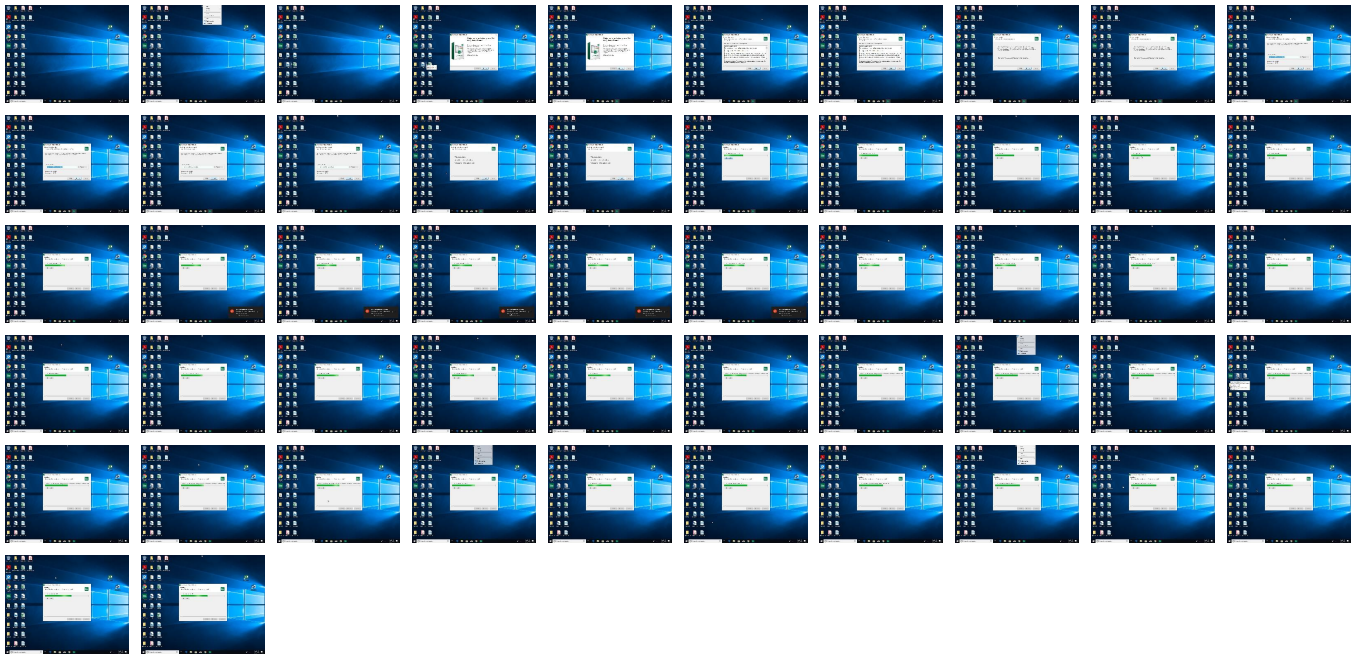
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ibaAnalyzerSetup_x64_v7.3.6.exe	0%	Virustotal		Browse
ibaAnalyzerSetup_x64_v7.3.6.exe	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files\iba\ibaAnalyzer\DevExpress.Data.v16.1.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\DevExpress.Printing.v16.1.Core.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\DevExpress.Sparkline.v16.1.Core.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\DevExpress.Utils.v16.1.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraEditors.v16.1.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraGrid.v16.1.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraPrinting.v16.1.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\DotNetMagic2005.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\GMap.NET.Core.dll	0%	Metadefender		Browse
C:\Program Files\iba\ibaAnalyzer\GMap.NET.Core.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\GMap.NET.WindowsForms.dll	0%	Metadefender		Browse
C:\Program Files\iba\ibaAnalyzer\GMap.NET.WindowsForms.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\ICSharpCode.SharpZipLib.dll	0%	Metadefender		Browse
C:\Program Files\iba\ibaAnalyzer\ICSharpCode.SharpZipLib.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Program Files\iba\ibaAnalyzer\OverlayWindow.dll	0%	ReversingLabs		
C:\Program Files\iba\ibaAnalyzer\Plugins\View.GeoView.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.ibaAnalyzerSetup_x64_v7.3.6.exe.411c52.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.darb.ae/ArcGIS/rest/services/BaseMaps/Q2_2011_NAVTQ_Eng_V5/MapServer/tile/	0%	Avira URL Cloud	safe	
http://www.iba-ag.com.	0%	Virustotal		Browse
http://www.iba-ag.com.	0%	Avira URL Cloud	safe	
http://www.opencyclemap.org/whttp://	0%	Avira URL Cloud	safe	
http://tiles.ump.waw.pl/ump_tiles/	0%	Avira URL Cloud	safe	
http://www.topografix.com/GPX/1/1	0%	Avira URL Cloud	safe	
http://www.4umaps.eu/map.htmu	0%	Avira URL Cloud	safe	
http://https://api.maptiler.com/maps/	0%	Avira URL Cloud	safe	
http://4umaps.eu/	0%	Avira URL Cloud	safe	
http://www.ikarte.lv/default.aspx?lang=en	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://analyzer-doc.iba-ag.com/%TEMP%	0%	Avira URL Cloud	safe	
http://ump.waw.pl/	0%	Avira URL Cloud	safe	
http://https://www.maptiler.com/#providersComboBox	0%	Avira URL Cloud	safe	
http://mapbender.wheregroup.com/cgi-bin/mapserv?map=/data/umn/osm/osm_basic.map&VERSION=1.1.1&REQUES	0%	Avira URL Cloud	safe	
http://www.topografix.com/GPX/1/1T	0%	Avira URL Cloud	safe	
http://https://api.maptiler.com/maps/tiles/Basic?key=_Software	0%	Avira URL Cloud	safe	
http://routes.cloudmade.com/	0%	Avira URL Cloud	safe	
http://www.topografix.com/GPX/1/1D	0%	Avira URL Cloud	safe	
http://ecn.t	0%	Avira URL Cloud	safe	
http://www.dnguard.net/	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://dc5.maps.lt/cache/mapslt_relief_vector/map/_alllayers/L	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://server.arcgisonline.com/ArcGIS/rest/services/ESRI_ShadedRelief_World_2D/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://www.darb.ae/ArcGIS/rest/services/BaseMaps/Q2_2011_NAVTQ_Eng_V5/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/company/iba-italia-srl/	support.htm.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.maps.lt/map/K	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://https://www.xing.com/companies/ibaag-messtechnik-undautomatisierungssysteme	support.htm.0.dr	false		high
http://greatmaps.codeplex.com	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://https://twitter.com/ibaagcom	support.htm.0.dr	false		high
http://https://www.linkedin.com/company/iba-ag/	support.htm.0.dr	false		high
http://server.arcgisonline.com/ArcGIS/rest/services/ESRI_StreetMap_World_2D/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://server.arcgisonline.com/ArcGIS/rest/services/ESRI_Imagery_World_2D/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://www.iba-ag.com.	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000003.498976131.00000000006F6000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://system.data.sqlite.org/X	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://dev.virtualearth.net/REST/v1/Locations?	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://www.opencyclemap.org/whttp://	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://server.arcgisonline.com/ArcGIS/rest/services/World_Shaded_Relief/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://sourceforge.net/projects/nspring).	regsvr32.exe, 0000000F.00000002.665662339.000000001B422000.00000002.00000010.01000000.00000010.sdmp, regsvr32.exe, 00000016.00000002.719288765.00000000025D2000.00000002.00000001.01000000.00000010.sdmp	false		high
http://tiles.ump.waw.pl/ump_tiles/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kso.etjanster.lantmateriet.se/?lang=en#	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=0&fmt=1&type=	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://https://www.linkedin.com/company/begner-agenturer-ab/	support.htm.0.dr	false		high
http://wego.here.com/w	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://www.topografix.com/GPX/1/1	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	DevExpress.Sparkline.v16.1.Core.dll.0.dr	false		high
http://dc5.maps.lt/cache/mapslt/map/_alllayers/L	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://where.yahooapis.com/geocode?q=	GMap.NET.Core.dll.0.dr	false		high
http://www.4umaps.eu/map.htmu	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mapserver.mapy.cz/turist-m/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://sigpac.mapa.es/kmlserver/raster/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://https://api.maptiler.com/maps/	View.GeoView.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kso.etjanster.lantmateriet.se/karta/topowebb/v1.1/wmts?SERVICE=WMTS&REQUEST=GetTile&VERSION=	GMap.NET.Core.dll.0.dr	false		high
http://dc5.maps.lt/cache/mapslt_ortofoto/map/_alllayers/L	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://dc5.maps.lt/cache/mapslt_ortofoto_overlay/map/_alllayers/L	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://server.arcgisonline.com/ArcGIS/rest/services/World_Topo_Map/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://sourceforge.net/projects/nspring)	regsvr32.exe, 0000000F.00000002.665662339.000000001B422000.00000002.00000010.01000000.00000010.sdmp, regsvr32.exe, 00000016.00000002.719288765.00000000025D2000.00000002.00000001.01000000.00000010.sdmp	false		high
http://https://nominatim.openstreetmap.org/search?street=	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://ajax.aspnetcdn.com/ajax/jquery/jquery-1.9.1.min.js	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://nominatim.openstreetmap.org/reverse?format=xml&lat=	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://code.jquery.com/mobile/1.3.2/jquery.mobile-1.3.2.min.css	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://where.yahooapis.com/geocode?country=	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://server.arcgisonline.com/ArcGIS/rest/services/World_Terrain_Base/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://wikimapia.org/S	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://server.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://https://www.linkedin.com/company/adegis/	support.htm.0.dr	false		high
http://4umaps.eu/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.ikarte.lv/default.aspx?lang=en	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	DevExpress.Sparkline.v16.1.Core.dll.0.dr	false	• URL Reputation: safe	unknown
http://openseamap.org/ghttp://tiles.openseamap.org/seamark/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://analyzer-doc.iba-ag.com/%TEMP%	ibaAnalyzer.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://dev.virtualearth.net/REST/V1/Routes/	GMap.NET.Core.dll.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ump.waw.pl/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	ibaAnalyzerSetup_x64_v7.3.6.exe	false		high
http://https://www.linkedin.com/company/ibabeneluxbvba/	support.htm.0.dr	false		high
http://https://www.sqlite.org/copyright.html2	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://dc1.maps.lt/cache/mapslt_25d_vkkp/map/_alllayers/L	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://https://www.maptiler.com/#providersComboBox	View.GeoView.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://ajax.aspnetcdn.com/ajax/jquery.mobile/1.3.2/jquery.mobile-1.3.2.min.css	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://dev.virtualearth.net/REST/V1/Imagery/Metadata/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://services.maps.lt/mapsk_services/rest/services/ikartelv/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://dc1.maps.lt/cache/mapslt_ortofoto_2010/map/_alllayers/L	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://https://nominatim.openstreetmap.org/search?q=	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://server.arcgisonline.com/ArcGIS/rest/services/World_Physical_Map/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://www.yournavigation.org/api/1.0/gosmore.php?format=kml&flat=	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://nsis.sf.net/NSIS_Error	ibaAnalyzerSetup_x64_v7.3.6.exe	false		high
http://www.mapy.cz/I6A1AF99A-84C6-4EF6-91A5-77B9D03257C2	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://mapbender.wheregroup.com/cgi-bin/mapserv?map=/data/umn/osm/osm_basic.map&VERSION=1.1.1&REQUES	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.thawte.com/cps0/	DevExpress.Sparkline.v16.1.Core.dll.0.dr	false		high
http://www.topografix.com/GPX/1/1T	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://maps.yahoo.com/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://https://www.thawte.com/repository0W	DevExpress.Sparkline.v16.1.Core.dll.0.dr	false		high
http://earth.google.com/kml/2.0	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://code.jquery.com/jquery-1.9.1.min.js	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.maptiler.com/maps/tiles/Basic?key=_Software	View.GeoView.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://greatmaps.codeplex.com/discussions/252531	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://code.jquery.com/mobile/1.3.2/jquery.mobile-1.3.2.min.js	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://routes.cloudmade.com/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.topografix.com/GPX/1/1D	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://system.data.sqlite.org/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ajax.aspnetcdn.com/ajax/jquery.mobile/1.3.2/jquery.mobile-1.3.2.min.js	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ecn.t	GMap.NET.Core.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.dnguard.net/	regsvr32.exe, 0000000F.00000002.665556769.000000001B39F000.00000002.00000001.01000000.0000000F.sdmp, ibaRunTime64.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.nearmap.com/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high
http://server.arcgisonline.com/ArcGIS/rest/services/NGS_Topo_US_2D/MapServer/tile/	ibaAnalyzerSetup_x64_v7.3.6.exe, 00000000.00000002.719730623.00000000026E4000.00000004.00000800.00020000.00000000.sdmp, GMap.NET.Core.dll.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632527
Start date and time: 23/05/202218:41:07	2022-05-23 18:41:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ibaAnalyzerSetup_x64_v7.3.6.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:	23
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:	SUS
Classification:	sus24.evad.winEXE@9/99@0/0
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 6.6% (good quality ratio 6.2%) • Quality average: 71.1% • Quality standard deviation: 29.9%

HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target regsvr32.exe, PID 6048 because there are no executed function
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\iba\ibaAnalyzer\DevExpress.Data.v16.1.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5392112
Entropy (8bit):	6.386730970129271
Encrypted:	false
SSDEEP:	49152:7606CzFcJD5WL1S1dFw9jO6XXls/+wNAY2lQgS1Fh8DGQn4larvhBHQ:7aXWL1S1dFAjO6XVsW2yw
MD5:	46D4548EE2FFE0211B4200E08B2BF9A9

SHA1:	AC232FF3F1B0CCDAE4274788FFD7FF7D077B1761
SHA-256:	626D27108093E90ECB3FE3B0909C11008843D379528182360E33FAB823BF9AE6
SHA-512:	957C84FA82219A3907450F130440E5EAAECB74DBE8E28FEADD7664A9BBA421587B21FAFB3390B0B1A86B0A322F9C26FCB8F1A37ACE2EFDC60B1C3B9AB842084F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...El.Y.....!.....&R.....>ER.. ...`R..... ..... R.....@.....DR.K....`R.X.....0R.....R.....CR..... ....H.....text...D%R.. ...&R..... ..`.rsrc...X....`R.....(R. .....@..@.reloc.....R.....R.....@..B..... ER.....H.....2.0.....L...S!.P .....[..S.O...QK....3.i].....Q6.B..Lc.:w....Mj.+D%._.Y.i...'T..J.. b...M.%.T._.F.d...&.!..Q.....YN".....h.zw.=.....<..(....*.s....z..*..(....*..*..s....}.....s....}.....(.....}.....}.....}.....}....*.0..~.....{....(.....o`T..-..*.-).{....,!.{.....o`T..{....(.L.....o.L....-...oaT....o.....,...o`T..otH....-...o`T..{....(.....*...0.....(....,..{.....{.....{.....o....o....*

C:\Program Files\iba\ibaAnalyzer\DevExpress.Printing.v16.1.Core.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3965680
Entropy (8bit):	6.561634542986759
Encrypted:	false
SSDEEP:	49152:3M1tY2g/rmwOhp/tPmmcL8gxeIvpLwkS+ve+hxnReam+o7Hn6ajZZ6n3ZCmte38a:k56KNn5DXgxHpLWoda
MD5:	37A3628DBF140B7B969DD1A81CFEB3FB
SHA1:	7FE4EE7606C52D394310A337AB17DC820D76CF11
SHA-256:	42D84E16224805000DC2FD104023049AF1B07D36F5A02468F3F00FD236687CE7
SHA-512:	5B4A453690F7E489F38DD376C94D8B811AAB20A4FDBA09EC6C74C588DEE00A3F8C81E2B04AE76C9E767785300FD3FE08B318270ABDC131A82E1A1AF1D95F636B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...bl.Y.....!.....b<.....<.. ....<..... .....<..... ..@.....T.<.W.....<.....l<.....<.....<..... ....H.....text....`<.. ...b<..... ..`.rsrc.....<.....d<.....@..@.reloc.....<.....j<.....@..B.....<.....H.....p.....P .....=...5lj?...x$7.?...,I*u*.s..[.za$...J...?]Zp...h'.7..$..@<.....M....>z...U...9`..%l.C..[.9...}Kg.J..,V4U..._.u)..0..-.....,..o....,..o....o.....o.4..*.(.4.....o.....*..{....*2.{....tr...*.*"..(.F..*"..}....*.*.0..3.....(....o7...,..o....*.o.....o.....o.....o.....*.....*.....*.....(....*2.(....us...*j.(....-.~....*.(....ok...*Z.(....-..*.(....oj...*..u[...,...t[...o.=...o....*.

C:\Program Files\iba\ibaAnalyzer\DevExpress.Sparkline.v16.1.Core.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	78576
Entropy (8bit):	5.909591561044907
Encrypted:	false
SSDEEP:	1536:fDTT9ELYGGHN+3qkKCGvOw1e10WcJ/3Z81yDKqlSGcczraGu:T9E++3qkA17J/3ZllSGlnaGu
MD5:	AAAC55F125CB3B0BE4ED9A11C2E9FE82
SHA1:	D4FDA25F10BF63FA52C9FEA50B115A430AD815D9
SHA-256:	99FA3C085BD6F04CE2C62A8F398AD37B41DEC4FAA38A44E4C5469E26C735B789
SHA-512:	6D385343625546BF21AA36E883AB667C18694982611AB07FA81F41BB8247DB7207E1EA53C18F129B8234F7CE661A3BBB51C43478090EF1103DC9080F0881750D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Vl.Y.....!.....0... ...@..... ....@.....0..S....@.....`.....p/..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....0.....H.....L...$.....h...#..P .....E.76...0..+...#OW.}+.y.e...-1.O. ...Y._b#.....x,....*9...,.z._...s.3.z..Go.J...;..6.)...&R.....J{.2.....c#1.)q.T...,...o?...*2.-..*.o>...*....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*J.{.....{....(....*J.{.....{....(....*..{....*~.{.....}.....{....-..(....*..{....*~.{.....}.....{....-..(....*..{....*^.{.....}....

C:\Program Files\iba\ibaAnalyzer\DevExpress.Utils.v16.1.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	8797936
Entropy (8bit):	7.299508908918551
Encrypted:	false
SSDEEP:	98304:W4UGwaQCKWAOfraPaQVndlvlup3OklnBzHF8CZlbV4wx2oE1oT:W4UGwatKWAOfraPzktOklgqlbe7ox

MD5:	427E2B1B94675CAA74F79CFDFC651F5C
SHA1:	3F013FB0AB5F157632638AEA2B4DDEDA2E59FCF6
SHA-256:	B993E395F4F7FAD50956FCC421DF789DA0EF6E27B328016F097D43920C07C8C4
SHA-512:	F48E5BFE7A4F40BC6DA8AA2867C1BD11A684DD53693FA95DCD4556676B6FAD92E79B29626F5E5646E45620F34B67DEFEF718C6D6701593321A58ADCE40BA84C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ml.Y.....!.....=... ...@..... ....@.....=..W....@..h.....(.....`.....L<..... ..... ..H.....text..... ..... ..`.rsrc...h....@..... .....@..@.reloc.....`.....&.....@..B.....=.....H.....4.i..0.....WY.P .....e+,~..\.aA...1C.j.Z<.fv .Z7{. N..x..V..-.....i3.q'.b...*..l..9z.K.....s...o..... ...-.-.v=...zo}w.2..I.../s._.?....!.:0....0.....(....*...}.....(.....}.....}.....}.....}.....}....*.0.....(....*..0.....(....*...}.....(.....}.....}.....}....*.....(....*..{....*..{....*.{....*R.{....,.{.....*.j*..{....*>..}.....}....*..{....*..{....*.n.{....

C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraEditors.v16.1.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4979440
Entropy (8bit):	6.314747424393378
Encrypted:	false
SSDEEP:	49152:UejIKdwMWBEVglDkU7YtHqkSYVK/bV0+b5rJ0F8kkzVRjFqM:5KEVglAOY8kpVGVnbrIm
MD5:	D4F26960AEED922F431858F630B30084
SHA1:	D0E747E4BCA2E58C70E04224766F29C1006CA819
SHA-256:	A9362C3ACC4A27ECA26CA9D0E54D3A4F075B3B3F08DCBE77AEA5A68E435DAB7E
SHA-512:	4187D1D0BED40B9EA7B8475CE20B7A3C979A990E5D81E9AD3A2651C5D22C87419740017C268BBAE903FCFBC5D5AE1AD80E3ECEC746B5580FC0BC3766F12CE320
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...|l.Y.....!.....K.....K.. ....L..... .....@L.....@..@.....K.S.....L.....K..... L.....p.K..... ....H.....text.....K.. ....K..... ..`.rsrc.....L.....K.....@..@.reloc..... L.....K.....@..B.....K.....H.....d.&..l%.....x.....P .....the...2....9.VY'.F.F..=.\.=..#.C[...VK.U`v`....o...A..u9*....E...X.H.a.E...r...y..g:?G..T`...g|...S....S.{.Z...g...Q.3..."..(....*n.(.....u....,..t....}....*J.(.....o....u....*:.(.....o....*..0..F.....(.....+..o....t.....o3....(....,.....o....-....u.....,..o.....*.*.....*1.....0.....u.....-.s.....(.....o....*....0..@.....(.....+..o....t.....u....,.....o....-....u.....,

C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraGrid.v16.1.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3017456
Entropy (8bit):	6.129027003423717
Encrypted:	false
SSDEEP:	24576:Kf3zffyXWmkr8HeKAjJPb4VKuTBSdDtUrbxWO+eFFG5DM/tFyjIyRZPx8m:KTfymceRJPTu7RFFFG5DM/Lyj9
MD5:	225CC9B28CE29257910ADAECD48E22BE
SHA1:	2CC718F0240090000997CCBBF708DF63CDB266433
SHA-256:	0FCF7E006F0444A0660A49DD1F9CE1839852C5766F84ECD0C7F866522215DF5B
SHA-512:	1FA39678C01FBAF320480DA4ACFFF1F23208F01538FFF031FE68A91801740DF18F683124B8FAC3F6136D1B6A3B1EE1C659307C41F06CB459615DED70998080A4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....l.Y.....!.....-.....^.... ... . `.....@.....W.... .....-.....@..... ..... ..H.....text...d.-.. ....-..... ..`.rsrc..... .....-.....@..@.reloc.....@.....-.....@..B.....@.....H.....<4..P .....,_..T.{.....;.L..[...3g...I.:.. -J..|s._.~..i...=.B.F.<....J.WK..L...rgN...)..\k..W..z.0...@.s.d_...Ty....~.z.a9...(.....}.....}.....~....}.....}....*..o.....o....3".(.....o....(.....,...(.....o.....*.*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*"..}....*:.(.....}....*...0..&.....u.....(.....,.-..*.o.....o.....*..{....*"..}....*:.(.....}....*...0..&.....u.....

C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraPrinting.v16.1.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	962800
Entropy (8bit):	6.34004464341254
Encrypted:	false
SSDEEP:	6144:HPlWUIMh5ejOJzduk9JvZ7t2/n1ahHUUrgR3tgeYgJXN5HfdXQ3TI6O92N4CJObs:vnh5+Ov79JvK8jWtgls5HiT2gx3akc+L
MD5:	BECAAA1444E3F6233DCBD211CDA587C0

SHA1:	1676036BC05DFE314A55DF2A0FE9E967784E956A
SHA-256:	0E02A2C63F7A6C004C8751D77FEBB1E12D3E38E5EA002F94D05DCE5790FC041A
SHA-512:	B7350E1F1795CF78A3AEC96A585176989F6C96F9381EDABBDAFDDFAAE42D5E45E73280C020128FC082B4CDEA64D1762DD7DEBB9B80566815F993E9EC5E6618 36
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....l.Y.....!.....~.... ....@.....,...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....`.....H.....=..,o.....`P..h...P .....W'tA.cXZ.k.C.c.....l.w.....K_.q..S...lj.L/F.~K.i....h.?...ARx3.....!....78.~_R.D..HC.P.....l.. *...p-...].G.~..._!E;..(9...*..(....*.*..{....*''..}....*..{....*r..(....-.r...ps;...z..}....*..(<...*2.....(=...*^.,..u....-..u.....*.*..{.....,.{.....2..{.....{....(>...2..*.{.....{....(?...*...0..).....{.....(A...to... ..|.....(...+...3.*....0..).....{.....(C...to.....|.....(...+.

C:\Program Files\iba\ibaAnalyzer\DotNetMagic2005.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1114112
Entropy (8bit):	6.106701577278103
Encrypted:	false
SSDEEP:	24576:tsw6jJGXuM75U8B3QtBcPdOjoRGczhSYMg3kmaJa5B:CwcdM75U8B3QtBcPdOjoRGczhSYMg3ki
MD5:	6A867594FE5479862AC2AC378D6EB0E1
SHA1:	6E0B30E1C934CD011BB965130DE5D6CF1B37F68D
SHA-256:	EAA684BEE01914AD7022567AB154222035495EEE1FC56A25F150C41B64BD2409
SHA-512:	7D5E80E965188755FD70E3F13D7CFA1B2CE102A754A640C19DD2285EB8746BE390DEF31280B0A2E2EFF5FD1D6770487FA9FBA1D92FD6D8F05BBDB7D22C61E1 6B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#`.....`" ..0.....`..... ..... .....@..... ..@.....O.....J..... ..... ..... ..H.....text..... ..... ..`.rsrc....J.....P.....@..@.reloc..... . .....@..B.....

C:\Program Files\iba\ibaAnalyzer\GMap.NET.Core.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	293888
Entropy (8bit):	5.880567896926908
Encrypted:	false
SSDEEP:	6144:LGCf+YJvBTdp6L4Jqr6kp0r2JckgfcNUO7PXw:Z+YpTdpXqDdxb
MD5:	3397F55F2256BFB012EB4F7860E86650
SHA1:	3D37F5CDA00591612CC83A4488C4C9FEC390EB5D
SHA-256:	5FD39F686D700C9959C499AA536B1538CE2EAA0D81D349C65F2E71495D1C6098
SHA-512:	0D1F7E55199043045A2362ADB80CA44D9556DACBF0DCB73829E07F5E6FFDF77E5BA2A2D4F9FD547A342FC178716757887F11CFE5DE0182DD9308A12448F3B5A B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ..@.....O.....h.....T..... ....H.....text....n... ...p..... ..`.rsrc...h.....r.....@..@.reloc .....z.....@..B.....H.....L.....t.....0..\..... ....((..... .....+/....+..._,. .....da.+...d...X...2.~.....X..~.....i2.*v...s).... (....%.}....%.}....*ns....%.}....%.}....%.}....*v.....+..s)....(....%.}....*.0..;.....o*...-.....r...ps+...zs.....}.....}.....o....,..*s,...z..0..5.....{.....3.r'..ps+...z...s).....(-.....(.....o....*....0..... ....{.....3.r'..ps+...z.{....o/...,..{.....{....o/....Yo0.....

C:\Program Files\iba\ibaAnalyzer\GMap.NET.WindowsForms.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	155136
Entropy (8bit):	6.923246431474686
Encrypted:	false
SSDEEP:	3072:Zkf6d53aMCZbfAFYbjluOWcLvVIEYaQ9SDBRGlDUqL63budi94kD:VOb4QIArGloqL63q
MD5:	89ADD49BA2C99BA0CF246943974B93D8

SHA1:	88E7C7827146D13E8D3DE831D34FCCC83A5E7911
SHA-256:	2015A76F954C1137D1ED6493ECA5C06F4D7DA487AFC809403D48F7E087DC37E8
SHA-512:	374AC5FC16B4A37BBBC90E52916069791EF329CA16347A6A519CC051860F9944152CF9526831FF574DBC6736D1227D1F556E47B84BFD70CC9B420CF175192DA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...v....." ..0..R.....6q... ....@.....p..O.....o..T..... ....H.....text....Q... ...R..... ..`.rsrc.....T.....@..@.relo c.....\.....@..B.....q.....H.....@n.. ...`o.....0.....s....}.....}.....s....}.....s....}.....(.....(....(....%{.....s....(....t....}....(....% {.....s ...(....t....}....(....%{!.....s"...(....t....}!....{.....o#....{.....o$....{.....s%...o&....{.....s'...o(....{.....s)...o*...*....0..*.....(+...-!.{....o,...&.....s-.....(....&*...0..*..... (+...-!.{....o/...&.....s-.....(....&*...0..2.....s.....

C:\Program Files\iba\ibaAnalyzer\ICSharpCode.SharpZipLib.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	5.926131598180448
Encrypted:	false
SSDEEP:	3072:d8UMF1fOJCJa+kz7YsEc0oIjvUgAEThOvwhDXEDXUwheEDLKlHsDFchBCckidIjV:DMFlfrqB0ocAEThOEDXEDXUwheEDLKld
MD5:	C3991E3FE72665A29297FDBF8121E336
SHA1:	4F507A57BAFFB37AC71A98CFF257907309CCF73E
SHA-256:	828BA5AAA720F43FA02AFE60D50F7DE1F6117CB2F83BDDA63E183DD00CD3B454
SHA-512:	1792DB805D9C9524C974D53320DDF75788603232F01842038F305F4EAD817C9147E88E9BF526968C69E1F28E9DB2C2C241456DB09ABA3C10FED2FF86D5B0BE1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Q.E....." ..0..... ... .`.....#M.. ..`.....O.... ..t.....@.....T..... ....H.....text..... ....`.rsrc...t.... .....@..@.rel oc.....@.....@..B.....H.....hz.....<.....(....*"..(....*&...(...*2.r...p(....*"..(....*&...(....*2.rE..p(....*"..(....*&...(....*2.r...p(....*".. (....*&...(....*J..r...p(!...(....*v....("....("....("....("...(....*....E...%...%.r...p.%...%.r...p.%...%.r+..p.%...(#...(....*..(....*&...(....*...0..).....{.....($...t.....|.....(...+...3.*....0..).....{..... (&...t.....|.....(...+...3.*....0..%.....{.....,...s.....o.....o..

C:\Program Files\iba\ibaAnalyzer\License_Agreement_ibaAnalyzer.pdf

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PDF document, version 1.7
Category:	dropped
Size (bytes):	87287
Entropy (8bit):	7.8926391328230885
Encrypted:	false
SSDEEP:	1536:nfpOYf1Pe7wZ5td3E29HkBM9/DHcWn8WdrJb3ZgtcnrKi0Eya+9wQJEiiz4wTluO:fpOiMu01Bsb8MbLJrUJEiizTJl
MD5:	A0CEA3A9C3CFE17037F135930A601DA5
SHA1:	C6A9C4D0F2F9D28140110BD70E04255F4AC0C99E
SHA-256:	AE35683A6B9D208A2A36FB5C420777CB1D4B5387012646545E00FEE0B97879FE
SHA-512:	C08D341DEE1D000917CE013336941043CBA125DAC4F4A201F87CE50B788F1BA8BE69F1C661661A2711BC09374A1C8CE5F05EBE16D629F1F697D3E80B81B11F6 6
Malicious:	false
Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(de-DE) /StructTreeRoot 22 0 R/MarkInfo<</Marked true>>/Metadata 95 0 R/ViewerPreferences 96 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 4/Kids[3 0 R 14 0 R 16 0 R 18 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 9 0 R>>/ExtGState<</GS7 7 0 R/GS8 8 0 R>>/ProcSet[/PDF/Text/ImageB/ImageC/ImageI] >>/MediaBox[0 0 612 792] /Contents 4 0 R/Group<</Type/Group/S/Transp arency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>..endobj..4 0 obj..<</Filter/FlateDecode/Length 3368>>..stream..x..[mo.J...).a>.U.z..R...Hs....u..~p....Jm.6.G./.< g<.c|..J.l.g.?...0^.+qu..S..VX....0....u}-nn{....eZ.....O.A..lt~..obu~v39?.0.BJ.r.d~~&i.%..l.].X.....?...c....[.1...%.....q~.5.~~..lN.....=.[ip...~.3..:.o.K.HD.B.].X..#\...../ ..0eA7q.2.....h...m#...Ldt.....`8.|..7...$...s.g.^.y{l..O=!.Z'O.u>..I...^.....$~m...L...<%YxFH.g.$.\.X..J%.,.q.(%fG..R.hf6.R.M..Pp.K.S...mWv.4..

C:\Program Files\iba\ibaAnalyzer\OverlayWindow.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	80384
Entropy (8bit):	5.992824785073126
Encrypted:	false
SSDEEP:	1536:3z+3ShmGPCaAabPVPPPPPPP8Ciu2grhIiWpzzHuxR+G:3z+3wLC9abQiWpHHuxR7
MD5:	251DFC7357EAE23C3D859426D3F5EA17
SHA1:	32E283E06D925D88A1B5E3AF09F7D31EA4B582C8

SHA-256:	0399FD9C706F2DEC9D1C0A60C3096192375119527091 3F815115A61484D84F00
SHA-512:	7626925CDFE137A229274B354DA3BEBE4D9016A49CC4BFA820D949642CA377EBACAE0B98E464813877E26197FFCAD2304EFF81A363E376BF0F2D2265056D6AF 2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C..."..".."..Z}."...J.."..p}."...J.."...J.."...J.."...D.."..".."...K.."...K.."..." y."...K.."..Rich."..... .....PE..d.....`......" .....@.....H.....`.....9.....p.....`.....c..T..... ...c.....`..(.....b..H.....text...s9.....:..... ..`.nep.....P.....>..... ..`.rdata.....`.....D.....@..@.data.....P.....&.....@....pdata.....`..... .,.....@..@.rsrc.....p.....@..@.reloc.....8.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\Plugins\View.GeoView.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	139776
Entropy (8bit):	5.857230726618
Encrypted:	false
SSDEEP:	3072:qICMXV2e1ljiYrQ4QWqcf/Hc5bVOcb9SH:NC648pYXS
MD5:	7BCAC81A4929429C6B669B9B86CFC9CD
SHA1:	79CAA23C70D05F19AD2F655B92FF6A8442253E98
SHA-256:	5281A16869289A2C527831ED7B89E4BD4D23B7E0EC785A3C1B7532CA5B5AA684
SHA-512:	9A5A268464ADD4BE2FF0A9F1561B20BFAFBB3BD01E8C773F8A3F5170B2A7603165A5F7D29D5752A1B68EA9BD388A9368736D139157E96F442FC88E0110451E26
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....." ..0.....7... ...@..... ....`.....7..O....@.....`.....\|6..8..... ....H.....text...(... ....`.rsrc.....@.....@..@.rel oc.....`..... .....@..B.....b7.....H.....@.....0..g.....(...."...As....}.....s....}.....}.....}.....}.....}.....(... ....(.....(.....}.....{....o..... {....o....{.....o.....{.....o.....{.....o.....{....o....{....#.....@o.....{... ....} ....{....o!....{....}"....{.....}#....{.....o$....{.....}%....{....~&...o'....r...ps(...}.....{....{}....{....o*.....j}.....j}.....o+....{.... (,...o-.... . ...(.....{.....s/...o0....{.....

C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaAnalyzerViewHostGraphManager.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	37376
Entropy (8bit):	5.854743156462957
Encrypted:	false
SSDEEP:	768:Glalc7JPLn+JnLTsqhr1NrUJ7YuStTUhlS:GwJnLgURN8Otwu
MD5:	EB412C01E4B89E6619B12BD8FA33206D
SHA1:	3966423594468CC372FB1C77795BC50923A0731B
SHA-256:	DFB8E17724D3C326B710EED367EE614BB011E1AE33EFE5BA9F8C0AEB358921EA
SHA-512:	FA040BC44313A68F55B20EFE75D390EC3FA5FB1A4BB04E7B88268C6D44BC1F986457D84237F69F791851128EBEE4BA0E7AB006ACBC69CAF63835E261B144E47 0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....." ..0..... ....`.....:...O.....P.....h...8..... ..... ..H.....text..... ..... ..`.rsrc...P.....@..@.reloc..... .....@..B.....n.....H.....;..:.....Xv.../.....j.js....}.....j}.....(.....(.....o....*.r...p*....0../.....(.....(....u.....,...o9...(.....{....(....*..0..+... ....s....&.s+.....(.....(....-...(....o9....*.~....*b..d3..s+...*.....(....*Z.{.....,..{....*.{....*6..(....(....*.0..p.....{ ...o!....+E..("...o#...o$....+...(%.....o&....o'...XX...((...-.....o).....(*...- .....o).....*.....".%G.....R`.....*r..}.....(

C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaFFT.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1936896
Entropy (8bit):	5.956495632744587
Encrypted:	false
SSDEEP:	24576:88jY4VgZNLCuiWpTFdADqHM9LT5KN+PhaiOcw99:8acbpxu2H
MD5:	9F17A45BB8D2971ED0002F4967F8ADA9
SHA1:	B8A99FB7BBB8536FD9C7607E06C176A51AEC5D58
SHA-256:	64D510E9B295EA5141278840862F3582595DF845068698B1ECB14B5252C4B899

SHA-512:	0871CB18C8A0BEBE6466BFD2CC93F3055C48CDA0657313C03F52C6DCFDBC25C8E6D91022717BACAD5AA7AF21D5519CD2444B9EECE6BF3F2EB880000413943AD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....N\a....." ..0..... ....`.....O.....t..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....(...~.....z..}.....j/...j}....*..j}....*>..}.....}....*f..{....}.....{....}....*..{.....j..*....0..A.....3..*.....,.....- ..*.{.....{....3..{.....{.....*.*...(.....*....0..3.....,..u....-..*.....{.....{....3..{.....{.....*.*b.|....(.....|....(....a*..{.....{.....{.....{.....*.{.....{.....*..{.....{.....{.....{.....*.{.....{.....*...|....%L.{....XU..| ....%L.{....XU.{.....{....4..

C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaGraphManager.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1202688
Entropy (8bit):	5.908967575659683
Encrypted:	false
SSDEEP:	12288:Gcz2YTNtSeCv2RFby9JMCEVhZwQ2XhtnWTqtx+3Mv8gDx:GczlNtSF2RF3CEzZw1hwTqtxx
MD5:	FFCF3BB31A122AF791B3559832F2D7D6
SHA1:	E5074F0041E85EEAE581AE23F197331E755ECE9B
SHA-256:	79C0EB5FA7E97ED7FA7D55926C4CC8EAD6CC254D1110EF6B399AD480BEB275C1
SHA-512:	7089B37C7B0313506588B3BB4A2CB289CF0011B75A734BC33494213947C07E80ADEF7BFDB11198BF66C9DFAD13F9A57BCD5B4D62E1F6AA38F60640BD38EFA2B7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...M)\a....." ..0..P.....o... ....`.....o..O.....`.....Xn..... ....H.....text....O... ...P..... ..`.rsrc...`.....R.....@..@.rel oc.....X.....@..B.....o.....H.....x...._.....S.....(:...*. ....(:...*..(:...*"..(:...*..(;...*....0..@.....~....}.....}....(<.....(.....{. .....Y.. ....[*.0..i.....(;.....(M...,r...ps=...z.o>...-.r...pr...ps>...z.o<.....s4...}g....o;.....{g...o;.....}i.....}h.....8.....#.....+v.....#.....+.....ZX....X.....2.....Y.....[%.....ZX....{h....._}h.....X.....2.....Y....{i....

C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaOrbit.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	892928
Entropy (8bit):	5.9179936359593
Encrypted:	false
SSDEEP:	12288:7Bk7Rt5S+GZ7j/teU26F0U4tjoIMhtnTf80nXW5Fpg7:Vk40U4BoIMhVf8
MD5:	7A0ACF0CB55F5E358FB8112FC196475C
SHA1:	E33B6CE3D95BE4E022E1CE4A302552FC6B512A28
SHA-256:	C06EC93345A20706C0044E27709A823E6191B329964492FFC5980382A5C280CB
SHA-512:	57A97292730AD49C74939552BC417197C4FB40CA71A0E7C0ADA23D62EEEFB3EA0148D0DE063E6B3A6AA9FDDEC6BB0590BFEEE9EAA9B280F28D505566F1DB53DB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....N\a....." ..0..... ....`.....O.....X..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....0...(.....N..(.....s...}....*j.s....%{.....s...o...*..0..S.....{....o.....{....o.....*..+%.{.....o.....{.....o....o....- ..*..X...{....o....2..*..0.....(.....}.....o;...o.....s.....s.....o.....o.....o;..o.....o....o ....s!...}.....s"...}.....s"...}.....{.....o#....s$...}.....s%...}.....{.....s&...o'...*..{....*.0..\.....s".....{....o@ .....{....o(....Y.+4..{.....o)...o....oQ...o....-...{.....

C:\Program Files\iba\ibaAnalyzer\PowerCollections.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	182784
Entropy (8bit):	5.883620315599388
Encrypted:	false
SSDEEP:	3072:k7ClE8AaUsjQmECRrUpoaFA3HmDweVMoeZ:busUmE6rUC9MwkMo
MD5:	F20ACA91342A4DAD79E87695D2E90E0B
SHA1:	C16E51B1B0114FB6607EF1FF5A1F9C069EAA01B8
SHA-256:	E83483E3966F205B7AD539792C6A0002FB44CF7E1871978F32707C21FFFD5CAB
SHA-512:	A4ACE490B57A7D320AF9D6E64ABD88E8551D72496B4AE9C1812BCD72C44D5805B899C775E0263705235FEC8DB90248657624863D02B84E8FFCA560AD52012E9A
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._......" ..0.....~.... .....I. ....@.....,...O.....h..... ....H.....text...D.... ....`.rsrc...h.....@..@.rel oc.....@..B.....`.....H.....p...m.....0..^.....-.r...psO...z..2...oP...0...oP...3..,.r...psO...z..2...oP...0...X.oP...1.r. ..psO...z...sQ...*...0..R.....-.r#..psO...z..2....i0....i3..,.r...psO...z..2....i0...X..i1.r...psO...z...sR...*2.-..*.sS...*Z.-..*.oT...,..*.sU...*Z.-..*.oV...,..*.sW...*n.-..*.u6...,..t6...*.sX...*n.-..*.u/...,..t/...*.sY...*n.-..*.u9...,..t9...*.sZ...*n.-..*.u....,..t....*.s[...*n.-..*.u....,..t....*.s\...*V.-.r#.

C:\Program Files\iba\ibaAnalyzer\SQLite.Interop.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1688576
Entropy (8bit):	6.536380500683419
Encrypted:	false
SSDEEP:	24576:9i6QnGucgDweNGkfb01HHk2AlZjiwy5Iyt6Wo+/BgJQGFIuHWMdx3eGD+l4V:9i6QGWPb0EhlZjitzlWJquHWGEl4
MD5:	0EC8D85D10FF52827930B1CEC64A0933
SHA1:	90C6D01AEFA10F5488411C84553ED44131372C58
SHA-256:	7F214DFCCF659D8E4C0A08AA6772B2E540F20987AAB2B26B6BAAD2D201554BEC
SHA-512:	650257CF683D030BFA6A8DA7065409B47E994AE86BA96934A1D977C51A48B2D80D8E1BC8A7979DEB089BA243CEF13F9E2707837F9803D691B51C14C07AFF337
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....n.0O*.^.*.^.*.^..K..>.^..K....^..K....^.x.[.4.^.x.Z.$.^.x.].".^..(../.^. *._...^...V.+.^...^.+.^.....+.^...\.+.^.Rich*.^.....PE..d...S%.^....." .....\...d..... `..... )...1...[..<.....<.....X...` ...p.....p.....text...pZ.....\..... ..`.rdata.....p.....`.....@..@.data...@M...p...6...Z.....@....pdata..... ....@..@.rsrc...<.....@..@.reloc..X.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\SciLexer.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1528320
Entropy (8bit):	6.439158645608687
Encrypted:	false
SSDEEP:	24576:nzb5jLexcYWfnyLqMQlJ7mIJR5/1yDnxPBjW+V4T5aIxXYKHQs73K6:hu/WfnekD7mIJRd1yrxPBaWMIiYKw
MD5:	44EFAC6665A774744FDE243E2C961734
SHA1:	850C4DFBA9C6E87CCE688BCF694A3054BF02D4A8
SHA-256:	0FD202C22B3CB6D76435952E9DB460C6FD9FBB6B7E6FBEEC482CF5B7C6A0F5C1
SHA-512:	A0BB432A772001F6A0A32060DFB46C7922620948446CD9F1E8C35918EBA621FA985C8ACD356BE07C32594123959DB955801B276C5349601D2E1B640FFDB21F8F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.a...a...a.....a.....a.....a.....a.....a..W.J..a..W.O..a...a...`..+. ...a..+....a..+.{..a...a...a..+....a..Rich.a.....PE..d....W.^....." .....u.....`.....X.....@....`..X.....d.....p.....pi ..p.....j..(....i.....text..... ..`.rdata...O.....P.....@..@.data... p...0...j.....@....pdata..d..... ....@..@.rsrc...X....`.....0.....@..@.reloc.....p.....6.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\System.Data.SQLite.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	364544
Entropy (8bit):	6.016735753684852
Encrypted:	false
SSDEEP:	6144:oVkOGvp0ezfbg1+w9MCdwqKOoPK3LE4bFNFaFeFOFwcGF6cmFWc0FWc8cIcKcUFb:3pJUBwq9FNFaFeFOFwcGF6cmFWc0FWcH
MD5:	ECAB575DD9FAA510F9D7BB67C55E0213
SHA1:	B9D5AF76D8DF1C4EE4CCBA33B2AFA8300952D923
SHA-256:	19AD18AD0A128F690667C7239DBAF89629ABE43A6BB365BAC295B72A8CC26318
SHA-512:	22BA1F1F9F92510DB76833BAAC3703D144D0B908539BAFC1BF8F9504EED3B5B82D3236D9A914B714E97753C9D7FCD39EC59D3DD090AD1E48371389E6619C145
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....!..... ....6S.. ..@.....S..... ....H.....text...$.... ....`.rsrc... .....@..@.reloc..... .....@..B.....H.....0.....P .....Mf.6..>/..U.....6....B.W.....X..a..l.5.{.....1.6...w..n....0l...R&..l..s...kvM.....G....._.r.3.. P..6...z2j..d.=D.Yy:.(.....}....*..{....*:.(.....}....*..{....*r.(.....}.....}....}....*..0..5.....-..*~.....o.....X...s....~.....o.....o .....*6..(....(....*"..(....*.0..T.....~!...("...-..~#...*./....+...X.... ($...-..~#...*..s.....(%...~.....o&...*Z.~....2..~.....

C:\Program Files\iba\ibaAnalyzer\View.ibaEventTable.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	469504
Entropy (8bit):	5.936700714458861
Encrypted:	false
SSDEEP:	6144:H4dybI6lgjv/att7Uiw3pVQOcpKmMYRhyLyn1rdL6kv0:Yd8tt7UNQOo3yL8LK
MD5:	7D576FAFC24FC2BA670F5543CE9ED04E
SHA1:	22A01FE984FA449F1007719643403AD56B82CB1E
SHA-256:	3B53FBFF956DF1E92CBF1A874D5C70771F948E047D6670495DF142D20E7E04F8
SHA-512:	AD8C96E84B844A2DDCEEA30B2F8D261B51472061207976761B6E677712CE4DCAAC87D3D047AB0DBA421D0C160CC47E4A03208870993429A912E6317217A56C5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...g)\a....." ..0.."....@... ...`..... ..`.....?..O...`.....>..... ..... ..H.....text...4 ... ..."..... ..`.rsrc.....`.....$.....@..@.reloc..... .....(.....@..B.....@.....H.....`.....0.....(.....(.....}.....}.....}....:....{....o....{#....o....{ ....o....{'....o.....{.....o.....{%.... o.....9f.....o....}.....{....o.....{....s....o.....{.....o.....{.... ....o ....{.....o!....{.....o"....{.....o#....{....o$....{.....o%....{....o&....o'....{.....s(...o)....{.....s(...o*...s+.....o,....{....o&...o-.... .....s....o/.... ,...o0....s1...}.....{.....s2...o3.

C:\Program Files\iba\ibaAnalyzer\View.ibaGraphManager.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1202688
Entropy (8bit):	5.908967575659683
Encrypted:	false
SSDEEP:	12288:Gcz2YTNtSeCv2RFby9JMCEVhZwQ2XhtnWTqtx+3Mv8gDx:GczlNtSF2RF3CEzZw1hwTqtxx
MD5:	FFCF3BB31A122AF791B3559832F2D7D6
SHA1:	E5074F0041E85EEAE581AE23F197331E755ECE9B
SHA-256:	79C0EB5FA7E97ED7FA7D55926C4CC8EAD6CC254D1110EF6B399AD480BEB275C1
SHA-512:	7089B37C7B0313506588B3BB4A2CB289CF0011B75A734BC33494213947C07E80ADEF7BFDB11198BF66C9DFAD13F9A57BCD5B4D62E1F6AA38F60640BD38EFA2B7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...M)\a....." ..0..P.....o... ....`.....o..O.....`.....Xn..... ....H.....text....O... ...P..... ..`.rsrc...`.....R.....@..@.rel oc.....X.....@..B.....o.....H.....x...._.....S.....(:...*. ....(:...*..(:...*"..(:...*..(;...*....0..@.....~....}.....}....(<.....(.....{. .....Y.. ...[*.0..i.....(;.....(M....,r...ps=...z.o>...-.r...pr...ps>...z.o<.....s4...}g....o;.....{g...o;.....}i.....}h.....8.....#.....+v.....#.....+.....ZX.....X.....2.....Y.....[%.....ZX....{h....._}h.....X.....2.....Y....{i....

C:\Program Files\iba\ibaAnalyzer\de\View.GeoView.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.242601878924758
Encrypted:	false
SSDEEP:	48:6CcQOHTrxVnHbLstI8JEOw92hH1FXHAqTzHFtHWhDkctVnMVq2vmQliM36r:uzXsZm2hTXgq/ltGtN2qa5
MD5:	85047CC9200E66156AC8E2F7BB96C103
SHA1:	E4158F0F13F09A07FAFBB7E3F783EC6817DF0268
SHA-256:	BB9AAE52E419557C83F4576CBAD2D359262FDB857170EA777B7C0E8D51557D99
SHA-512:	E795AA470B4FA7B6F80D25273512C6210EED1605127EE4F6330FBA16DD284DD769DD2EFB88C886474089230DFE681D1690D0EBC93A3DC211B903C025C257082
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?k`.....!.....+... ...@....@.. .....@.....t+..W....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....+.....H.....)..h.....P .....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Cu lture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.C..f.?...b..f....O...c...._:#...(.....s.3"..5!..N...Y...a.>.|....b.. .....;.....y...'...6.....K...m...Z....."C.e.n.t.e.r.M.a.p.O.n.M.a.r.k.e.r.....L.a.b.e.l.....L.a.t.i.t.u.d.e.-....L.o.c.a.t.i.o.n.s.?.

C:\Program Files\iba\ibaAnalyzer\de\View.ibaAnalyzerViewHostGraphManager.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

Size (bytes):	5120
Entropy (8bit):	3.8010929530727506
Encrypted:	false
SSDEEP:	96:OY2uHwtNMawWGqZNwfntwf5wfXvGq7zwOD2:r2DMawkwfntwf5wfX9f
MD5:	CC554E9214E238D44C07F9963E048D51
SHA1:	A8893600A0509D1E3388624A352590C92A320191
SHA-256:	6217A47FE8503DADCBC10F7EA500D9835E9071CA273D03CF969C6301F510A2C4
SHA-512:	335AE9030EA4B183E00BA72C30FF487BCFEC644775AD7E6C86B95A08CB743A520D9EA5D07E505F090C871FE484D451C39421503B68E83AE19717B6F2C294E74E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?k`.....!.....)... ...@....@.. ..... ..@.....`)..K....@..L.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....)....H.....'.....P .....E.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP..*..%.....PS.y....n.....;.....6A.b.s.o.l.u.t.e.T.i.m.e.C.o.n.t.e.x.t.M.e.n.u.T.e.x.t.....O.f.f.l.i.n.e.T.r.e.n.d.D.i.s.p.l.a.y.N.a.m.e.0...<R.e.c.o.r.d.e.r._.A.u.t.o.m.a.t.i.c.Z.o.o.m.X.1._.D.e.s.c.r.<...<R.e.c.o.r.d.e.r.

C:\Program Files\iba\ibaAnalyzer\de\View.ibaEventTable.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	26112
Entropy (8bit):	5.067662870911737
Encrypted:	false
SSDEEP:	384:oRZc7tKHxc5rXwndR/wqaRCJemeDEQP8ykawjXwGFwf+wfrwfvwfwwfewq7EaGXa:oNHWodR+xmeDEQPwGqDp
MD5:	FF5906101B86E639390BF5D86236D7B4
SHA1:	FAF4BD2295D9120D31B894483163094481A3E4AD
SHA-256:	CDA482CBA2F89638778481521AB4C037051866D82D661009D8AB6784DD431ECD
SHA-512:	74024393E06506B91CFF0B7DBC5028932B0EB132B3B3B36581B279FCE025C0630A4CE51286C5618D9E1B072A61B8E7DDE7ED32A82B365B853C29A2808AA5ECD4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!....^.....N|... .....@.. ....@.....{..S..... ....H.....text...T\... ...^..... ..`.rsrc.....`.....@..@.reloc..... .....d.....@..B.....0|.....H.....lq.....P ...Q.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet....D.....PADPADPlh].....N.....,i.V...Y.f..#n.).Z..#.V.....X..9;.....%.m.|..W....P. .....WB..A.....h..`D..".....$..x..sm..q....q.....8oM.:+....X..V....]..._...._..[.....!...!o.B'..-"..5.Q.7...8&E.A..DBc..C..HF+..Q.(rTJ..V

C:\Program Files\iba\ibaAnalyzer\de\View.ibaFFT.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	86528
Entropy (8bit):	5.251852466819867
Encrypted:	false
SSDEEP:	1536:4QS9WLYFWtW3et03etMXbz3et03etTizUzH2dnWGHzt0t3cEzQRXvs:4QSgLYFWkXbGioBGHzs3cEci
MD5:	C750F094A06E21E08BB152E3A7E66511
SHA1:	14251FC6AD157EEAAA6A735002DCCF405467D58F
SHA-256:	BBF04E8FE2AC7F7B2E0592613CC1AAF0305C48FCF10E0872AF0A30D19B49EE79
SHA-512:	D691FCCD1F60C40F73AF00A50E042B6405128ABB9007C7FD157A87CE9B403493D5E43818949472DA7FCBCA1AFB80F69D432ACA79E1B1CFB67A3BCAB4BF77584
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....J.....i... .....@.. ....@.....h..O..... ....H.....text...4I... ...J..... ..`.rsrc.....L.....@..@.reloc.....P.....@..B.....i.....H.....Y..T.....P ..69.....P~.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet....Z.....PADPADP....8..a2.....e.\.R.d!:.g!:..Oa...k.i.P.....7@...S..6. .....E....}M..R..J1...N...K....G.~.V...Kc<..'..G)..+...9g.....7.Q.....2..(`V....s....]......(@&...7.Dyv.....9.B..:q.`...m.1.....3..vR.....R./.G.

C:\Program Files\iba\ibaAnalyzer\de\View.ibaGraphManager.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	62464
Entropy (8bit):	5.213676805749081
Encrypted:	false

SSDEEP:	768:H/xyDDVPOAPepAOrjkudKwgHprLvgQmipRiPSH+MG:5yD8AGuOrjvUzHprLvgPqRiaeMG
MD5:	20A223B0601318ECF54A3D25C9765F2A
SHA1:	3D488C4AD2F5167EB066F73B5F1349E177B0CCC1
SHA-256:	7ED3A6D9E38BF77EF168BA5C67CBD252E94B14EF50FA09712CB2EFCD067078C5
SHA-512:	DD136F066EE144E05916F22355AEAB5EE917E740DEB8D44063F114CA87FAD72483F2001733D320AD9C4EEB4295F16B910BC1BCF01CD629F1A9D487621CCC0D4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....n.... ... .@.. .....`..... ..@..... ...K.... ..|.....@..... ..... ..H.....text...t.... ..... ..`.rsrc..... .....@..@.reloc..... .....@.....@..B.....P.....H.....(.....P .....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.....(.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP9.....2..`.`.I.m.L.">L..L...L.c.R.3.?.

C:\Program Files\iba\ibaAnalyzer\de\View.ibaOrbit.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	33280
Entropy (8bit):	5.1443046601861075
Encrypted:	false
SSDEEP:	384:/ULqa2idF0eqio4Aab0xc7baoXwa6wqpwqbWBawjXw0wfnwqdwqd+N3q4DnqqpRU:Da280FQI8PzV3q+FpncPyZNyvnH
MD5:	DA79ACFC31EE9691DAC8C54C88DF4F92
SHA1:	67C88E60550BA963AE897B321DDD2EE5494D83CE
SHA-256:	C56168652A7AE8B49FEF82CD1D75DBD06C402D7403EEE781A2B302A1A95A6AD0
SHA-512:	94EBAE2F9CC8623B02E7D3078DF50F525BDDDABE2F6BBC30D94F3EB6DC877C9C9C3B15ED156799EDE91426B9286B24148D98EE08A2906343250C836BC2112D02
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....z..... .....@.. ....@.....\...O..... ....H.....text....x... ...z..... ..`.rsrc.....|.....@..@.reloc..... .....@..B.....H.....P ...|.....T.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet....|.....PADPADP..j.v+....j.~.....m.3.../.l.....}M.J1...o_..'..o.....:..~...? ..."...V....F....s..h...r..C....>..w@.].`...&.~_..6.....i.)T..L.#.....O.....g.U.+.....P...^.....{....7...C.....@.W...6)...e.....

C:\Program Files\iba\ibaAnalyzer\de\hdClient.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	48640
Entropy (8bit):	5.162529542594102
Encrypted:	false
SSDEEP:	768:QViwJDgNWmCcKcsBJPfzSjI0sQ67eLuthM8r:QKWmCHcsgPD6blr
MD5:	C17C63B0C0A21690660A0AE8D42B222E
SHA1:	3E77E8473EEC62F28B5C469E576460B5BD7713D9
SHA-256:	D6CCE8944A1EC43DF314CD1DFF4B0841D391F43094A91C2FF8EA6C0DE66E26A9
SHA-512:	582EF03A563196F9EEBA32FD613CAB2703BDD089949C44C8FB5760E75C5C64FA4D8037F8443F12908418B4B2FB2DFD5544EAEC06B7CA10284D503BD261B5159
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....-ab.....!.....^.... .....@.. ....@.....O..... ....H.....text...d.... ....`.rsrc.....@..@.reloc..... .....@..B.....@.....H.....P ..@.....-..|.....BSJB.....v4.0.30319.....l.....#~..@.....#Strings.....#US.....#GUID.....P. ..#Blob.....%3.....!.....*....P.....n.....".....?....e....~.....J.....J.....J...!.J...).J...1.J...9.J...A.J...I.J...Q.J...Y.J.....-... ..6.....U.....h...#.v...+.....3.....;.....C.....K.....S.....[./.....

C:\Program Files\iba\ibaAnalyzer\de\hdCommon.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.3308783906967365
Encrypted:	false
SSDEEP:	96:gvn1+Al6puwaxzSDALasfKpkCbyHKdAfeJVD8oq5Ghrb:Mn/6puwlDALdCpUqfVI/Y
MD5:	A834AD4AA5B0DCF24CF2EAFC1CB5974B
SHA1:	252D31871058C5EB3831D32E6D2AE28DBA15A944
SHA-256:	018AAE15D2DDBB5F45AFF9B8CD021F2FD9D8819C8D1E3B40BFE383DFFDA6EC88

SHA-512:	B903C284B11C28CB65F1D22CBDE39103050E623C312FF916E56D17DDC7E9CE11FDCDF8CE8D3FFA9F6738C978BFA590894F0B62280ECFB9AD4A21679B99E958 0A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...h.Za.....!.....4... ...@....@.. ....@.....H4..S....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....4.....H...../..H.....P .....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Cu lture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet....+.....PADPADPaRS.....4n.H<....8..KS.....).....S.C..U@..g.....:... j...i...Dm..H...i...<....1G!...#L].0RV.;...B..1F..IHG.JH...H.;.L...L...Q.-YX...XY.gb...e#f.v.}.v.....i.....}.....

C:\Program Files\iba\ibaAnalyzer\de\ibaAnalyzerViewHostViewWrapper.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	21504
Entropy (8bit):	5.031920165697022
Encrypted:	false
SSDEEP:	384:D4rKXAxGcoRahKJ56KTFjHM51+LteAecjawjXwFwfkwqxfffCTfff1Rh7p9xkkJm:QKjcTwJ56KTFjHK1+Lph7pLkkjY
MD5:	681F2264378183EB9F1FA2E682EFFA43
SHA1:	2E776BF043FE7176BF54E065487980C3E5D17DA2
SHA-256:	6726DAF26D232FA0F77227C49F3B90641B72E724884A8AE7A6485815F7809E82
SHA-512:	1D0CE0F6680EA0AF887D9209B0DFCD1C399D258E9E2557EFD8FE9CA5BA369F860F689EE492DC4B2B4DD1E557CDAB6A9EE6C475D3E41150A28EF04185E7D91 AF7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?k`.....!.....J.....>h.. .....@.. ..... ..@.....g..S.....\..... ..... ..H.....text...DH... ...J..... ..`.rsrc.....L.....@..@.rel oc.....R.....@..B..... h.....H.....L^.....P ...=.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Cu lture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.....-.....lSystem.Resources.ResourceReader, mscorl ib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP..6.F....y.....|.W.tT.....].f.

C:\Program Files\iba\ibaAnalyzer\de\ibaHDOffline.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	17408
Entropy (8bit):	5.009206061928093
Encrypted:	false
SSDEEP:	384:wpawbwfCyPDL9pDuawxTM3wfjfctawSPCwf/LbyawjXwiuwfOwq4wfhwqOwfmwf2:FL9gTMaPX6
MD5:	2B4A1134AF6F66EFF94E3C9EDB3A588A
SHA1:	18023A380DAFB27BEE46D64AF0C878090A85584B
SHA-256:	443B6BFDE8A85116C73CEB959CC63873DFE110657E4E99F284D0FD538BE84B71
SHA-512:	2F2089D3A5041AF340FB9C629B79C945ED48430A512103D057A9A1135CCB2B0A16D78ADCCEB6C6088A269921E7CEA594A6AF18124487C642AA07C821DBD5A7 6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....-ab.....!.....<.....>[... ...`....@.. ..... ..@.....Z..W....`..... ....H.....text...D;... ...<..... ..`.rsrc.....`.....>.....@..@.rel oc.....B.....@..B..... [.....H.....P .....(...2.....BSJB.....v4.0.30319.....l.....#~..P.....#Strings....D.....#US.L.....#GUI D...\...d...#Blob.....%3.....*.....C.....c.....3.....m.N.....N.....=.....=.....=...!.=...).=...1.=...9.=...A.=. ..I.=...Q.=...Y.=...a.=...i.=...q.=.....2.....7.....@...#._...+.q...3.....;.....C.....K.

C:\Program Files\iba\ibaAnalyzer\de\ibaShared.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32256
Entropy (8bit):	4.940524757862727
Encrypted:	false
SSDEEP:	768:QM33oM+f4o96gnqFW31v0/JfDmKxDxYc/sO8L77SakIR02R/BLZYX2akifbs+OrX:BHoM+j96gl31v0/JfXxDxYc/l8L77Sah
MD5:	759A8ED5BEFADD5D8BF703112EF53A74
SHA1:	10D7CCDE38CD0F844120A95AE593F9D18839FCB3
SHA-256:	E04FB65E5D721A8681F89231C0F75BC0A67CE8056B275BDAA8C4C1613EAB98E3
SHA-512:	C8E814122D9D0760BE0572A9AF791E7F1AE1ED98A4B56790C61AEA4F93C1D8FA273AF51A36B10A500C7B61AC9500E7B317C48F3E742B5980FB1E04726BEC17F D
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....t.....N.... .....@.. ....@.....W..... ....H.....text...Tr... ...t..... ..`.rsrc.....v.....@..@.reloc..... .....|.....@..B.....0.....H.....H.....P ..Zk.....Vk.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP...yk.....~..h..e....].eN...h6...7.`....!...D...f..Z..#.I...R.Q.L. .....4P..6P..7P..&....:...R.]...R{..../...n...^.....`.....w..._.....V.|.f.}.f..]..d.w.+.r.....d.....J.....uy.....E.F...@.....

C:\Program Files\iba\ibaAnalyzer\de\ibaSharedGui.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	76800
Entropy (8bit):	4.984005127858699
Encrypted:	false
SSDEEP:	1536:Udq064Coc6Qab3J+H8CL7W/p8N7T3sePhw1cUTz:Tp4CZ6QaTJ+HNfW/qxT3sADUn
MD5:	591DD0EDAD52AEA641EC6CDEC6C132EE
SHA1:	2AC7C2DD48B6A2A5E422DD5C8DD36422737F4E9C
SHA-256:	63EC6960EB80B4573415ED4E9839979B580300533460 66BDAE2288C6932C9D0D
SHA-512:	5278F48391E288FDC264D9D83A87E575E4C8117E3757DF16087CB8087CAA772E50BF4244CD050BD465868F854D3021B786180E904AF978935F5410CE7AC30209
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....$.....B... ...`....@.. ..... ..@.....B..S....`..... ....H.....text....#... ...$..... ..`.rsrc.....`.....&.....@..@.reloc.....*.....@..B.....B.....H.....`2..H.....P .....p.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADPX.P..BV..zY..<...].bc...;.L...%<...X.f....4...\....7..k.. .@..._.%.j.....J*..oK.....x..V..F0....\.0Y.....2#.../...p.`Vv.'SO...6.D.9.. .....k'.Fe....B..\`..~z.|M...A.....G.....<}..J1.._x..qC..}5G.q.

C:\Program Files\iba\ibaAnalyzer\de\ibaUser.Forms.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14336
Entropy (8bit):	4.897229443132784
Encrypted:	false
SSDEEP:	384:toCW4TCvqSxWI3UGcjawjXwuwfgwqDwfSwq5Z9awjXw/4wf9wqZwfTwqZwf/wqtr:H239iG1
MD5:	A5F3AE915139B7044AAFFB0C9717A7DF
SHA1:	FF9C9A7BE3B0094883F6206FB24A96A0CA7E5F58
SHA-256:	D33C7FAFF10F505F5C5FD2074482F527E10D4DFF341F8107DB40EEA3A4651A4A
SHA-512:	6582ACD3AA3FBF8830166A1AC4F7EB40713EDA67B2EDF9B8C5765FE9DF5E36F9F1EE0F1BA881CB71FB2F489559A2A8B68502B1A696DBA8CA839B92374313EF45
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...j.Za.....!.....0.....NN... ...`....@.. ..... ..@.....M..W...`..... ....H.....text...T.... ...0..... ..`.rsrc.....`.....2.....@..@.reloc.....6.....@..B.....0N.....H.....E.....P ...%.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADPyq@.....j!.L....k(.\|.L.....DF.....TQ.....;!.....Y.#..w$.d.&.. .&...+-.0+.'3(..F...VV..e=..hj.Dmj:.r...|.....[.....c.....:.....P.....T...3.....k...'.....6...i.....

C:\Program Files\iba\ibaAnalyzer\de\ibaUser.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.99578208074871
Encrypted:	false
SSDEEP:	48:6sDQuHKB0zqJ9WXwjjhsuq+z4q3oND8LFqWPr1Dl0GaPogh6d:h3RzEcTD8hq4VZ
MD5:	133B793132E1564A33391017A9359DC9
SHA1:	8E0DEDD3A5D64787AD34AFDF5F9D36F212E78F44
SHA-256:	6EF1856661F9A07FA3F6605108DB7195DC58FA0301872DC8D6A2455F22DE3A74
SHA-512:	91C2137C73C19204EC009E379683D42FA83116CB9B4338765E09509C07BA00248FAB90591F2B65991F616ACC0E968D4D94178402760407AD3964D884CD06E5FD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...i.Za.....!.....(... ...@....@.. ....@.....(..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....(.....H.....L#..T.....P .....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.$..$"p9U.OE..[]..._f.....3.....E.r.r.F.u.l.l.y.Q.u.a.l.i.f.i.e.d.D.o.m.a.i.n.....E.r.r.U.s.e.r.N.o.t.F.o.u.n.d.I.n.D.o.m.a.i.n.....T.e.s.t.A.D.F.a.i.l.....$T.e.s.t.A.D.F.a.i.l.N.o.D.o.m.a.i.n.....T.e.s.t.A.D.O.k

C:\Program Files\iba\ibaAnalyzer\de\ibaViewUtilities.resources.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	18432
Entropy (8bit):	5.05476083841941
Encrypted:	false
SSDEEP:	384:LQWBawjXwCwfLwqdwqBWVDVffGGb5yjigjtxlXw3wqcwqRl/wYawjXwQwf1wqRwC:JZR/NpmtR24A
MD5:	9035D72D7A3DC90F5DDDAB4C859A1DDA
SHA1:	BED6279D287537F619701C65AD14A63BE083CA1C
SHA-256:	B2FBD9CBCDEC23846DC07777874F0E39793AA427D59A5F53B0EC62A047B3F7B0
SHA-512:	A9E26AE0CF7CED5D3C4FC63E4043ACFD9AC824CB52099D31BB29CC6616C0E44006E5BCAE43B51CABD3D5E051EB5D64E5D882050ACFBD7D50E2CC1DBB326CA14F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....>.....]... ...`....@.. ..... ..@.....L]..O....`..<..... ....H.....text....=.. ...>..... ..`.rsrc.....`.....@.....@..@.relococ.....F.....@..B.....]......H.....0R.....P ...1.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....gSystem.Drawing.Point, System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3afSystem.Drawing.Size, System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a.....Q.....O,d.O

C:\Program Files\iba\ibaAnalyzer\fr\View.GeoView.resources.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.6546985477509337
Encrypted:	false
SSDEEP:	48:6yQ4H19H19H19H19H1ZAxN1EJvmQliM36r:Pffff/GNil5
MD5:	B6754A7B748451C0530A25D79384609F
SHA1:	D746C9A96ED58A6D01614097C8504AB371B5EA7B
SHA-256:	9EC8227D0A0C0FCABDEBADE2ED7D7CF7D1437F3619CDC8C5BD722DFA946E067B
SHA-512:	4A127EC4B02115507FDCD4CCAFE2784882E66772C1B85F16F6E2BF3C36CDE0DDBEBB84D79FEF0314F5D3FB538592DB4E050267FE6272C90E679197F0E190FFA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?k`.....!.....&... ...@....@.. ..... ..@.....P&..K....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.relococ.....`.....@..B.....&.....H.....#..h.....P .....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.....lSystem.Resources.Resour

C:\Program Files\iba\ibaAnalyzer\fr\View.ibaAnalyzerViewHostGraphManager.resources.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.1560267824201524
Encrypted:	false
SSDEEP:	24:etGSwpAI+I6HE41VHE41DRlkqM+4jiuVGwaDYoyhKyvxSzZhNbCe/PqvXc2/43GZ:6xIDoH19H1DZPwccJvxSzluOSk2G6r
MD5:	FEEE75BB56239806D8D18C8A7E60B909
SHA1:	C7D1A854E23B80088EF2C1CB20442D450C8146DA
SHA-256:	5F520CC5D66B6E21323C808CDCCF226526039E01AF89D91EF9E6C29991A1ADD2
SHA-512:	4F23254934E7D34B0FE17225BECEC00120163BB205E184C42F2D217222761428ACA1DD5BC239B2D67F81AB0ECA59497DA9F1C6A67ADAB36EA0CEE159057D99C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?k`.....!.....#... ...@....@.. ..... ..@.....#..K....@..L.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.relococ.....`.....@..B.....#.....H.....!.....P ..p.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP....BSJB.....v4.0.30319.....\...p...

C:\Program Files\iba\ibaAnalyzer\fr\View.ibaEventTable.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	31232
Entropy (8bit):	5.130804702227277
Encrypted:	false
SSDEEP:	384:ywm5+EuhbIVA3aPJawNtskNwftf0awi6wf5wfiwfKxXwutWwqVwqC1awkHwfWwfr:UvuGFSbtogw0YFyB3
MD5:	E0DA983D430669B9FF6ECA52403870D0
SHA1:	07A0FFDE8A843FF06154DA167AA04363DD01C552
SHA-256:	9BF5937857CB4E2A05F5D901D803C0E2F9B99737325FAB15BC89DA40EC4485AB
SHA-512:	21EB469C67A5C23C853984C52EC3BA7AD079B0F8D36A6C676D73FA9AC9AD46E448547533882B1BBAB30D5786BA9D31E5FD6450BB26E64E69C4C36E897CA1BE 9E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....r..... .....@.. ....@.....S..... ....H.....text...$p... ...r..... ..`.rsrc.....t.....@..@.reloc..... .....x.....@..B.....H.....<.....P ...d.....`.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Cul ture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet....E.....PADPADPlh].....N.....,.i.V...Y.f..#n...Y.).Z..#.V.....X..9;.....%.m.|..W... .P.....WB..A.....h..`D..".....$..x..sm..q....q.....8oM.:+....X..V....]..._..._..[....!...!o.B'..-"..5.Q.7...8&E.A..DBc..C..HF.(rTJ..V

C:\Program Files\iba\ibaAnalyzer\fr\View.ibaFFT.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	92672
Entropy (8bit):	5.231168881343713
Encrypted:	false
SSDEEP:	1536:c8w1KhW2y5pvxo/bbARXCSjT6t3IGipfGK7i/MJ1x/7iIZ1YgpJskQS03oowMUp:cZ1KhW2y5pvxo/bbTV6wMhi630q
MD5:	1F234E47E36FF2C5B75ED509A3385D65
SHA1:	F226AE479991C42D27CFB8C26C09942F397AC620
SHA-256:	6DE77D7D17E418810B3E37641C1DFBF85CB90678D46573219299A582A62267A3
SHA-512:	F4A2196553F7A4E567AA4075ED281BBF0189C1BAF20D692457DD2E436E6859BEAFE6E41F9F879569CA997C5F8BF4AF0C94751EEC01C81A37DB6907805E93264
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....b..... .....@.. ....@.....S..... ....H.....text....`... ...b..... ..`.rsrc.....d.....@..@.reloc..... .....h.....@..B.....H.....Tp..T.....P ...P.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Cul ture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet....V.....PADPADP....8..a2.....e.\.R.d!:.g!:..Oa...k.i.P.....7@...S..6.....E... .O...R..J1...N...K....G.~.V...Kc<..'..G)..+...9g.....7.Q.....2..(`V....s....]..B.....7.Dyv.....9.B..:q.`...m.1.....3..vR.....R./.G.

C:\Program Files\iba\ibaAnalyzer\fr\View.ibaGraphManager.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	76288
Entropy (8bit):	5.21917028312933
Encrypted:	false
SSDEEP:	768:SGS/ksuEa9+jMN4X5Tt/HA6Vzpia8Dc0VDrixCNiwGdZnc9+Bw:nE6+m4X5Tt/HACtiaywMNiwGnncUG
MD5:	12215D8EBEF1D58F969E289BA7DCE3E2
SHA1:	DDBBD049265D552FB9C35E2C3D231D5BCB5C6D46
SHA-256:	1306B81BB8E652E55AB50AEF187352E034CBCB7F3DEB17463C551CD93699CA7C
SHA-512:	E52653AB86E59CC19C4BA1D71861CE6942BD33A3A450D05502C5718AB6335C900B2EA2AF53A8863B7C1B168DD87F9BE7D5476B622F206D5AC8B42698D483765
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!..... .....n>... ...@....@.. ....@.....>..O....@..|.....`..... ..... ..H.....text...t.... ... ..... ..`.rsrc.....@.....".....@..@.rel oc.....`.....(.....@..B.....P>.....H.....$0.....P .....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Cu lture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.....(.....lSystem.Resources.ResourceReader, mscorl ib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP9.....2..`.`.I.m.L.">L..L...L.c.R.3.?.

C:\Program Files\iba\ibaAnalyzer\fr\View.ibaOrbit.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	5.205911161033409

Encrypted:	false
SSDEEP:	768:HITl64McGExQb/M9O4bpwH7JtHaTZGitIapIKEYYfW/AtX:ln6TtIKYX
MD5:	B7634D69B55F0EDC94DD417ABCC03640
SHA1:	7C2D9998B28E171C6E8B6A6AABBFC8C4B98419BE
SHA-256:	EDFD3F1DC81620B15A9FE59A3A1747BC9A829A4575CB92F8AF72D42F21075DB6
SHA-512:	CB2F9D6E921F08157717A358EAC426FB03DE5BD6923021CC4B52B39DEB7DD6999007806E436F0998B0FF4026498DEF56296AB987498CC0282C80E836F08E696A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....n.... .....@.. ....@.....W..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....P ..C.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet....}.....PADPADP..j.v+....j.~.....m.3.../.l.....O..J1...o_..'..o.....:..~...? ..."...V....F....s..h.. ....r..C....>..w@.].`.}.V.....i.)T..L.#.....O.....g.U.+.....P...^.....{....7....X..C.....@.W...6)...e.....BrY.

C:\Program Files\iba\ibaAnalyzer\fr\hdClient.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	59392
Entropy (8bit):	5.201693622804996
Encrypted:	false
SSDEEP:	768:LTpcG5QI7O3maA8cRFdCzwiSQDXlhQz8CM/bD6Dbd+hgs4D:2IKbA8C0znNnQ6/nid+Ks4D
MD5:	6870CDFAEB0F1410A22F8E3302548A1C
SHA1:	27BDF3C35CBB617BA50C89BED6ED31877D786B38
SHA-256:	799D3B384E9B18291D7D056786267674C47B19971D2A4C223021361D1255C628
SHA-512:	08690E2348653446F66671FA5B4BA551075BE65C121A39D98F9089B96DE74D340E2EDD1536042C99C154B4C865ACB08269095605D659E6ECB59F74854901FB8B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....-ab.....!..... .....@.. .....@..... ..@.....O..... ....H.....text...$.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....P ..@.....-..;.....BSJB.....v4.0.30319.....l.....#~..@.....#Strings.....#US.....#GUID.....P. ..#Blob.....%3.....!.....*....P.....n....."....?....e....~.....J.....J.....J...!.J...).J...1.J...9.J...A.J...I.J...Q.J...Y.J.....-... ..6.....U.....h...#.v...+.....3.....;.....C.....K.....S.....[./.....

C:\Program Files\iba\ibaAnalyzer\fr\hdCommon.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.434682320543308
Encrypted:	false
SSDEEP:	192:6tKF5ps62PlTeMr7+OFaFtQAm43MWxg/i9uqqVI7W:6tKF5y66R7+OsFKAm+MWS/IFq
MD5:	121DA0237FF2829A65A5955AD96A6BFC
SHA1:	933777D05CA505BCD752319E65A29486AF4BDFF8
SHA-256:	E803EAD205B34FD2BCBA513545434E732C881BC1CA1E93FF25DFBB6622AB8146
SHA-512:	CD5A85CEC7B28F7CDC1AE8EFA705DB428DC6B07623DCB906E9330AC2225AC5B370E5198F81F98D32DBF2491EF42D8499B554A906516DF2B87FEDCEB58192DF8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...M.Za.....!.....7... ...@....@.. ....@.....6..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@..... ..@..@.reloc.....`.....@..B.....7.....H.....|1..H.....P ..,.....(.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet....-.....PADPADPaRS.....4n.H<....8..KS.....E..).....S.C..U@. .g.....:...j...i...Dm..H...i...<.....N .1G!...#L].0RV.;...B..1F..IH...H.;.L...L...Q4.,X.-YX...XY.gb...e#f.v.}.v.....i.....}

C:\Program Files\iba\ibaAnalyzer\fr\ibaAnalyzerViewHostViewWrapper.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	13824
Entropy (8bit):	4.931744942889366
Encrypted:	false
SSDEEP:	384:SIiS00SuUw06iWu1SfffffffonhVuVdDkJLpHjjnT:vHtYthVuvDktpHjjnT
MD5:	2092AB5477A34FF2A4B63F81E11812E6
SHA1:	E84CFD0B0B4B8E53F8830DB0CED42C71517D78D4
SHA-256:	CC5FCEFBC8A5D2F0FA76E4BDA21778D5F19FED146DA97DBA1C886B18175B292B

SHA-512:	6F61343ECF9BD5154E42415D0DA3888D4F397B3422EE4C7CB57D181DAF6865EDAB37D96E50FC0A2C5A1F75BB7D203B53F741993534E837FCD5F959BC3AD2A52
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?k`.....!.....,.....K... ...`....@.. ....@.....K..K...`..`..... ....H.....text....+... ...,..... ..`.rsrc.....`.....@..@.reloc..... .....4.....@..B.....K.....H.....A.....P ...!.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet....=.....PADPADPF....y.....|.W...X.....t.....w@..rk.

C:\Program Files\iba\ibaAnalyzer\fr\ibaHDOffline.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	18944
Entropy (8bit):	5.05365942685894
Encrypted:	false
SSDEEP:	384:lnRiJ/8w+OmkOmxsh/awjXwMLe9wfPTwfzwqJwf4wqQwfFwqQwfiwqefAYawjXwb:g8w+Om9gQLFW5JBSj
MD5:	14E909ACF73190A316E2A749C7811237
SHA1:	B015C280859567EDB321A227D33161366F31548D
SHA-256:	5C07E9D82E4C2F2265DA75A2F60DB586384F912DA13E9F6F539D2527044930B2
SHA-512:	0A474C2A8CEE2F4328436B37801EEBADB4F181DFC8382E94C7C7961227AAFC3B837C2500C413D0FA34476B94FDE60897CB82165AF539789AEA8F1BF1358DC9A9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....-ab.....!....B.....~a... .....@.. ....@.....$a..W..... ....H.....text....A... ...B..... ..`.rsrc.....D.....@..@.reloc.....H.....@..B.....`a.....H.....P .....(...9.....BSJB.....v4.0.30319.....l.....#~..P.....#Strings....D.....#US.L.....#GUID...\...d...#Blob.....%3.....*....C.....c.....3.....m.N.....N.....=.....=.....=...!.=...).=...1.=...9.=...A.=. ..I.=...Q.=...Y.=...a.=...i.=...q.=.....2.....7.....@...#._...+.q...3.....;.....C.....K.

C:\Program Files\iba\ibaAnalyzer\fr\ibaShared.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	4.976311231541577
Encrypted:	false
SSDEEP:	768:ObZ7eUgwvlch+gagUneX+nbYDjDiyU+/kQNTFSgst3ONe27l6EiGGpUO+:GZXgweh+EUneX+nbEiyU+/kQNTFSgslq
MD5:	17DB458C9EEF0F883B293282562FA5D6
SHA1:	82441FB5CEB7749A080D2292A34D9F2F1C0DC5F9
SHA-256:	67CBB4E2B427ACBAADFA1E1699498F05BA084A2D2CB4E6C33E262B956D9D5EF8
SHA-512:	915CF52974CADD7AB70D45721BD8A89913CDA1E121D77DEF09CE144E2251E6E449C5694EFD07F25DE3D8CD8D6E08EFDA8FDFAE4847CF9881FC45D6A913A400EA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....v.....N.... .....@.. ....@.....O..... ....H.....text...Tu... ...v..... ..`.rsrc.....x.....@..@.reloc.....~.....@..B.....0.....H.....H.....P ..dn.....`n.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP...yk.....~..h..e....].eN...h6.}...`....!...D...f..#.l...R.Q./fX.L ...4P..6P..7P..&....:...R.]...R{..../...n...^.....`.....w..._.....V...g..]..d.w..@..+.r.....d....J..-.....uy.....E..O..F...@.....

C:\Program Files\iba\ibaAnalyzer\fr\ibaSharedGui.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	86528
Entropy (8bit):	5.021258411884086
Encrypted:	false
SSDEEP:	768:C0Z02QH4p9va/FuExxgVSqlB1NytX0yuQ0pC3IcwMObllfLyYMPkWBEZ3FMchYhp:rK7FFqlZytX2C3x2JkWyZ3GchYT/
MD5:	D673C7F4D8AAB1B3301D480290A0F256
SHA1:	7D51A5641178EA23EA7CCAE2D16D5EC5B75F7D67
SHA-256:	B0D0EF9B6AA202E33E039C21B7801672F4CED3A5F71072B524E66C9FAE5358E3
SHA-512:	94AC2508F4A2F0400B00E325166D54EC822045288C94DAE266C8E31AB7063D106160BB0C9D62971C3ED3947B15764730D170FC470E3B7247C375B2C4A6C690BE
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....J.....h... .....@.. ....@..... .....g..K..... ....H.....text...$H... ...J..... ..`.rsrc.....L.....@..@.rel oc.....P.....@..B.....h.....H.....W..H.....P ..77.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADPX.P..BV..zY..<...].bc...;.L...%<...X.^J=.f.....4...\.....7. .k...@.._.%.j.....J*..oK.....x..V..F0....\.0Y.....2#.../...p.`Vv.'SO...6.D.9.. .....k'.Fe....B..\`..~z.|M...A.....G.....<}..J1.._x..qC..}5G.

C:\Program Files\iba\ibaAnalyzer\fr\ibaUser.Forms.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	18944
Entropy (8bit):	5.050244000392152
Encrypted:	false
SSDEEP:	384:5ofu4waWj0naw8tbqGwfHwfawfHwfvwfgrucjawjXwzwffwqZwfZwqju3awjXwKy:uzqtbqv8UCVj
MD5:	7694E025A9776874A585EC071EFC1D7A
SHA1:	0FAF2664792055390ABAA5BE69F09944DDB7D498
SHA-256:	84A19BE4C0D69B7C5AF51F1CE4852CD5F89D5EFD6AE8E2FCD8F7EAE47348A0A5
SHA-512:	F9AB21428E3F119351EC352CEB0B5B5A6E49758A59E72C6494DB10FEBCCE2CC855A3D4A44B8035A400DAB39FADC1C1E342C19A4E89750C9FCBCD1D16A29D1421
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...O.Za.....!.....B.....a... .....@.. ....@..... `..W..... ..... ..H.....text...4A... ...B..... ..`.rsrc.....D.....@..@.rel oc.....H.....@..B.....a.....H.....X.....P ..g8.....v.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADPyq@.....j!.L....k(.|.L.....DF.....TQ.....;!.....Y.#..w$.d.&.. .&...+-.0+.'3(..F...VV..e=..hj.Dmj:.r...|.....[.....c.....:.....P.....T...3.....k...'.....6...i.....

C:\Program Files\iba\ibaAnalyzer\fr\ibaUser.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.9326256354249263
Encrypted:	false
SSDEEP:	48:6PrQ/eHKB0z6/qmnGsduY1lLouq+zTJq3oND8kVUpPr1Dl0GaPogh:qieRz6/qmLHNl/JTD8kSRVZ
MD5:	0B02E635A4F717BBA0AF147E6269B89B
SHA1:	79992A4FB8533068D063D3985A547CC83B095826
SHA-256:	7CEAC40D6D8B1479E7AD5392B87222EFAD2387649A56BF91FC829F76557F4C8A
SHA-512:	A5F7F864DDFE2C966FAF6D574907444482CBE520FBB4A7CF4B8A696041D1D5CBF08436103DCD7AA03743C41611E31CFE5A24F30B7ADFD698A9ECFFDCE96E814
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...N.Za.....!.....(... ...@....@.. ....@.....(..W....@..... `..... ..... ..H.....text..... ..... ..`.rsrc.....@..... @..@.rel oc.....`.....@..B.....(.....H.....@#..T.....P .....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....PADPADP.$..$"p9U.OE..[]..._f.....3.....E.r.r.F.u.l.l.y.Q.u.a.l.i.f.i.e.d.D.o.m.a.i.n.....E.r.r.U.s.e.r.N.o.t.F.o.u.n.d.I.n.D.o.m.a.i.n.....T.e.s.t.A.D.F.a.i.l.....$T.e.s.t.A.D.F.a.i.l.N.o.D.o.m.a.i.n.....T.e.s.t.A.D.O.k

C:\Program Files\iba\ibaAnalyzer\fr\ibaViewUtilities.resources.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	18432
Entropy (8bit):	5.027911623191694
Encrypted:	false
SSDEEP:	384:ZAXw8wqfcjawjXwo4wfZwqLDg4ffaQbZcfHgLdWd0ffvbdWBawjXw3wf1wqNwfUF:jqyZW8n4sTl58
MD5:	210BBF5541353DC94DEA96620CA11B48
SHA1:	C68E261230EDC586D4AD252A7AB4F3BBF4961B1A
SHA-256:	326848B425995A05070A607988AF2233F6D0608E48B8899607D086F927C2E1C1
SHA-512:	61B52F19C374485EF8EEE6E94D3CA5827348925CDDED53932356280D29AE113AA5F229C9672831AEEA78429840FCE0EE716C9D8D72A46B7253E2B5F08AD9D8EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ta.....!.....>.....>]... ...`....@.. ..... ..@..... \..S....`..<..... ....H.....text...D=... ...>..... ..`.rsrc.....`.....@.....@..@.rel oc.....F.....@..B.....].....H.....Q.....P ..z1.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet.....fSystem.Drawing.Size, System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a.....O.....6...m.....$.t.h.i.s...T.e.x.t.....b.t.A.p.p.l.y...T.e.x.t.....2b.t.A.p.p.l.y.T.o.P.r.e.f.e.r.e.n

C:\Program Files\iba\ibaAnalyzer\hdClient.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4374016
Entropy (8bit):	5.693520481128679
Encrypted:	false
SSDEEP:	49152:+v3UwlrL5XezlA6o9HokJlJ8vMPnalWLBzw+hI7:uNlrFXUxRGftH
MD5:	9F66DB923887B0F63C9018736C8CB021
SHA1:	2A22035B59B323C4E814D7271AA1880D101A28C9
SHA-256:	DEB696E98039FDB442CEDF7FBDA1C757D516227C22BA693CADBA46F10A382932
SHA-512:	3441E85DEC3772991E6372FE30F6118E60D8B6718222BADBF91A173FCD10B56448A6E043477C8193C2561C67580BF3AC19767FC2B07CCDD03E9F4A0C82C24D9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....-ab....."I.....*.....I'.. ...`..... ..... C..... ..`.....I'.W....`'.....'..... ..... ..H.....text....)'.. ...*'..... ..`.rsrc.....`'.....,'.....@..@.reloc..... '.....0'.....@..B.....I'.....H.....M=.....`+..!.....).j.....K.. ..k.%:-..W.=.AG3..y.....:.*.?.".<.>.|..... .*.....*.....*.....*..... .....*.....

C:\Program Files\iba\ibaAnalyzer\hdClientInterfaces.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	27648
Entropy (8bit):	5.452809364163853
Encrypted:	false
SSDEEP:	384:R37raCoAu9/r3mG3K3xrr8RvY+2ssLrPsheqHaaAflLzcFkmbk:0Jp/xHvY+PwPsiaAflPcFkmw
MD5:	321D765B86248DB8009C05421306586F
SHA1:	A6D32D580DA68C13A98656D38C9357F1C176F116
SHA-256:	EF6FAFDCF1D279EB6B664631D6FEF0BD96B49C1E4AB832DBF92A2956A26DC212
SHA-512:	FC257D03C9D6A374F23F633296881DEB3FEF05479E7CA2D0CAF2D081B680F912440C190769B76EE17E8DEA9871E901D7583CDA9DE106AFA46217C53D3843165
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....." ..0..d..... ....`.....O.....T..... ..... ..H.....text....c... ...d..... ..`.rsrc.....f.....@..@.reloc..... .....j.....@..B.....H.....X&...[..... G..._...*.. ...._...*"..._...*"..."_...*.. ...._...*.. ...._...*V @B..... .....*..(.....}"".....}%.....}#.....}$ ...*V.(.....}&.....}'...*:.{(....{*...X*:.{}....{*...X*....0..g.....~....(....,~....(....*.~....(....,~....(....*.~....(....,~....(....*.~....(....,~....(....*.(....*..0.....o.....o.....o.....o.....@.....o....r...po....- ..o....r...po....9.....o.....P...%...:.%....o.....

C:\Program Files\iba\ibaAnalyzer\hdCommon.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	229376
Entropy (8bit):	6.053629328678978
Encrypted:	false
SSDEEP:	6144:O67xzuSPgdXXFbgcrfvDxzyftMwYwFLNk0bv8:O69zDiX1x7pGNb
MD5:	40CA53C3E2A44285B2D02FC4C0420E1F
SHA1:	F709890F15867C5236C29462F4F498A082F3F54E
SHA-256:	9C2A62BC97AB87F0C8A69F7A477E6E85491448320801BAC68A9DAF99EAAE09B9
SHA-512:	4B506FB9CBE77AFCACF0FA7743EB72C885B0DC263FAD34BCDDCF2C7CC7F1EE045B8780B41AE735B89FD7B769BE015A1EE2F70E7D062EC0BAFE4FA57061D2 D099
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Y....." ..0..x.....R.... ....`.....O.....0...T..... ..... ..H.....text...Xw... ...x..... ..`.rsrc.....z.....@..@.rel oc.....~.....@..B.....3.....H.....dy.....(.....V.(%.....}.....}....*..{....*..{....*Z...,..o&...+....(....*J....(.....}....*r.(%.....}.....}.... *....0.....{....-.r...p*r...ps'.....{....o(...o)....8.....o*.....o+...o,....o,...(-...,c.o+....o....s/....o0.....,H.....%.(1.....o2.....+$.....r...po3...,....o4...*...X.....i2..o5....s...r...p*r.{....o6.... {....o6...(7...*..0..@.....o8.....o9.....3.r...p*..,.o:.....X..Y.Y

C:\Program Files\iba\ibaAnalyzer\hdCore.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	dropped
Size (bytes):	314368
Entropy (8bit):	5.388292296651336
Encrypted:	false
SSDEEP:	3072:YlY5uz/xjoFtwIDZvOaE6FEYsRj7LdWdnK+0396N8b3i3A:UuurxutTDZ9S7LdSrK9vT
MD5:	8410C84BD9D997E89ACCC0A3AC0ADB4D
SHA1:	90414737A7563D73AB3EA10D7E3A9B91F0EA82B5
SHA-256:	42C893EE9CCCED46E5168AC9C227A720C94788786481D6ACC409C185706D7101
SHA-512:	0C85A52DA23F0421F34EA34ADC21B9A1CA4A1D0D4A245AB7150E065356EB90A6B3FC306A36B3AAA7789713E6814EFA729CB35E51834A68A602882F53D1FD019D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....-ab.....''!.....R.....p... ....`.....p..S.....X..... ..... ..H.....text....P... ...R..... ..`.rsrc...X.....T.....@..@.reloc...Xs.....t...X.....@..B.....p.....H.....{k.....''.E.\.....*.....*.....*.....*..... .....*.....*.....j..*.....*.....*F.....s.....*..... .....

C:\Program Files\iba\ibaAnalyzer\ibaAnalyzer.exe

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	22382720
Entropy (8bit):	6.976085181314033
Encrypted:	false
SSDEEP:	393216:rUGjsoYcSd222222v222222WyyyyyyqK2Pe6:t7YkyyyyyyqK2PZ
MD5:	9C63B57B74E4002CBCA81596074562EC
SHA1:	1694CCA61E4320C2BC792E719944911110AE5936
SHA-256:	9C410B6FD5A902D7983F68CEFEA2E2AA52B9F34D7CB6841E6DBE435878AD51A7
SHA-512:	4CCFA0249ED018C07ED2559B65C3327838D464ADD43DDB72A1D5C33B1F07E9F2B2A60BCD93327FA34C65BCF375A33F79EE20C6EEF629F905ABA17710062C90A6
Malicious:	false
Preview:	MZ.....@.....h.....!..L.!This program cannot be run in DOS mode....$.....1W.P9..P9..P9..6:..P9..6=..P9..6<.GP9..6?..P9.,....P9..8=..P9..8:..P9...8..P9..8<.'Q9."9=..P9.!98..P9..6>..P9..68..P9...T..P9...<..P9...<..P9..98..P9..P8.MT9...<..P9..9=..P9..9<..Q9..9..P9..P...P9..9;..P9.Rich.P9.....PE..d.....ab .....#.....h.....F_.....@.....W.....v.U... .....0.....(l.....$....fU..''.....m{.T.....n{.(... .z.....h..''.....@..... .....text....h.....h..... ..`.rdata..V.#...h...#...h.....@..@.data.....(...f.....@....pdata..$.....@..@_RDATA..P.....@..@.rsrc...(l.....J.....@..@.....

C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHost.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	34304
Entropy (8bit):	5.61572195985048
Encrypted:	false
SSDEEP:	768:EWy3K6fSyWnPG7q/5wWyvYTuHg7SOqaM2X7s9q1ZGhlO:LUzWnjTuH+SOqamq1ZF
MD5:	01003D05D31AB007F1C4A762D17252C6
SHA1:	2116C949422AF08A54C0F2EE73C01844E8256ACC
SHA-256:	93282A30E5AEAA5F024F0194F6C92CF99728975A490FD66EBE01DE61A22DB473
SHA-512:	2D26D98D2768D5D439CB492316A05C7479CE5C8249585EC9D4C3038A782D3B8304F9F6746381E060C9E44195CF9F187DF70BDD65D788F695BAA8DCF02C27197
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ab.....'' ..0..|..... ....`.....O.....8..... ..... ..H.....text....z... ...|..... ..`.rsrc...8.....~.....@..@.reloc..... .....@..B.....H.....A...U.....s.....*.~....*..(.....}.....s....}.....s....}.....s....}.....}....*..(....o....o....(....r...p(....*.0..A..... {....o.....1.*~....r...p(....s.....(....(...-..(....(!...&(''.....s#...o$....(....r;..p(%.....8.....(&.....('....o(.....9`.....8I.....t.....o)...o*.....+E....o+.....i.3,....o,....^...('...(-...,... ....%.rQ..p...+....X.....i2...o).....(....t....

C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostActiveX.ocx

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	308736
Entropy (8bit):	6.058941654981801
Encrypted:	false

SSDEEP:	6144:pm2U/0tVzINjXDuv8pogZGA21iuYRa76AAA2q:pm2Uo9gZG4Ra79
MD5:	9CF71E605D65209D5F9244F915C98A7C
SHA1:	4BD26854F94F93E0AA32392A04DEEDAE653045AB
SHA-256:	32F31B43B3F44196D6E836248C1C73CA75A513874BCDE3094174A66F1F90D465
SHA-512:	53A9937B9A2E5D1D5C583164CBA76B90B6E0128EC6F21715037A7BA4178B63539ABBD9865925DEFBB996F309E0D4F3F4A69B3C04184E9D708D375D250CB818C D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q.....Q.....Z.....=.....U. .....Rich.....PE..d.....ab.....".....@.....=..... ..... `.....I.....xJ.....x&.....`.....D...T.....(... ....8.....`.....n..H.....text...l0.....2..... ..`.nep.....P.....6..... ..`.rdata..,....`.....D.....@..@.data....Q...p..:...H.....@....pdata..`..... .....@..@.rsrc...x&.....(.....@..@.reloc.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostViewWrapper.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	509440
Entropy (8bit):	6.166093493986349
Encrypted:	false
SSDEEP:	6144:W7mRdLIPnWaKIhQnHhxY6+mQlfuDgEwo5p2od6PJ1VTDBdKumFOVxqr7QTgK:hDaKIhQnHhxY6+NfuDgtFHlEQV+QTgK
MD5:	754D50210E961087427411E4BC35B369
SHA1:	99576B727C008866D53F013DF3396E531F1ED19C
SHA-256:	8150B3743968E6E071A5FD52E5AAFDAF115534B852E2E6E7841BC5CA69019954
SHA-512:	957D92711702D65C7192300DFB00C7CEFA9DF2A3F78293632B94EEFC0278AE81FBB68C14BB9A4976B66424F23248D4BA54A3C302C9095078F9038EA517D38C95
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ab.....".....0..... ....`.....O.....d..... ..... ..H.....text...(.... ..... ..`.rsrc...d.....@..@.reloc..... .....@..B.....H.....S..8.....x.....{#...*..{$...*V.(%.....}#.....}$...*...0..A.....u.....4../(&....{#....{#...o'....,((....{$....{$...o)...*.*.*. .C.)UU.Z(&....{#...o*...X)UU.Z((....{$...o+...X*...0..b.....r...p.....%..{#.....%q.....-.&.+.....o,....%..{$.....%q.....-.&.+.....o,....(-...*..s....}.....(%.....}.....o....o.... (....}....*..{....**.{.....*...3..s....*..3..s....*..3..s....*...3..s....*.*..{....o/.

C:\Program Files\iba\ibaAnalyzer\ibaDataExtractor.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	342016
Entropy (8bit):	6.031228771347023
Encrypted:	false
SSDEEP:	3072:3jHLqibom2HVT8LfVrUHKj46VVGb6rbZG5dcbsVaIw/6et6uXecv9t4X8EU7bDkJ:zHLrbQHVAiHK1VVGOX8cbxICUMi/Urk
MD5:	A1041B0A041C8516C2BE940A011DE30E
SHA1:	E53320494BDD8A90810F456229A5A99A09A565F3
SHA-256:	E9F66DDB9FBFB1769E6E7B0D1EA990B1C9067F9FAD442A4E56A4FDB9E5DA603D
SHA-512:	C7CAB41F529357201EC5C9A8DFCE379D13729E1841E592F679010DBDF6E66899386F0E966C729039D1EC95811D9739298FC9D7CA745D3BFB69DA6BD9FF7B474
Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....\.n.=.=.=.=.=.=.[.<.=.=.[.<[=.=.U.<.=.=.U.<.=.=.U.<.=.=.[.<.=.=.[.<.=.=.[.<.=.=.=U=.=jT.<.=.=jT.<.=.=jT.<.=.=jT.=.=.=.=h=.=.=jT.<.=.=Rich.=.=.....PE..d...B..`.....".....J.....V.....`..... .....@.....@..P>.....#.....`Q.....R..(....Q..... ..x.....text...H..... ..`.orpc...$..... ..`.rdata..... ....@..@.data....3..... .....@....pdata...#.....$.....@..@.rsrc...P>...@...@.....@..@.reloc.....(.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\ibaDataExtractorMC.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	735232
Entropy (8bit):	6.328926037902178
Encrypted:	false
SSDEEP:	12288:YsYilitrkUJNF71p9O33txaDtqPRCqraAsO:Ysxlitr33YxaDtUCq
MD5:	545F33DB0FBCCC60347C8AD380A764DC
SHA1:	57EF11A6188EC2B7F0313E68E05C7EA445CB081F
SHA-256:	2AD2ABD2379AC4DD0720F016A811F7591EFD5B7B5B8B125D8FF745DC3D31DBAE

SHA-512:	16B5071A6465E86F31C8A1F3BB80568EA4A2FF7C41F2CA2B02457501A7B16249BCD8E52D82B3D85EDBB81AF40A30ECCC469307E4984CC766D2249666E5E53FD 8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....n.....n.....Y.....Y.....Y..$...n.....n.....n..... .....}.....Rich.....PE..d.....`....." .....<.....`.....0S.....S.....0...M.....f.....|..T..... .....~..(....}.....text..... ..`.orpc...$..... ..`.rdata.....@..@.data....D...p...(...F.....@....pdata...f.....h. ..n.....@..@.rsrc....M...0...N.....@..@.reloc.....$.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\ibaExpressions.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	221184
Entropy (8bit):	5.879493433652497
Encrypted:	false
SSDEEP:	3072:mO5kH2RWCtFc6WCSTt5aSAsf7xk2qgV+YkAuB1soSlHC:mO5keWCncHTt5aSZ1kM0L7SlH
MD5:	AB6B242752539387AE704E3E64CD37BD
SHA1:	F434704172E54408007E66A7EC6502819EA70EAD
SHA-256:	A9FEB00AC898465A328DB23F4BB1ECF2E85C23F9715E1B696061035837F073F8
SHA-512:	141A1D81DB3A08BC7885B642BD904578B7D1089D94BC117D9C64F811FEB0FAE16992A56BF616D0FBD35D1B23383F87219E96CF90E88BF5B4C429FAC3031750D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...G)\a....." ..0..0... .....A... ...`..... ..... ..`.....8A..O...`..... ..... ..H.....text....!.. ...0..... ..`.rsrc.....`.....@.....@..@.rel oc.....P.....@..B..... ....

C:\Program Files\iba\ibaAnalyzer\ibaHDOffline.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1053184
Entropy (8bit):	5.657040104901371
Encrypted:	false
SSDEEP:	12288:dmGXJFuRN3a8txNaZtmheEkai+Bn4aEdSEjqbUsRoo:dBspaixNutmhSv+aJSEj
MD5:	7AB2F758EB7CA996E56950D75A1BD0D2
SHA1:	7D7A81F34B227523681273A81A7B04293810877D
SHA-256:	435BBB3243D061A6A9D6516611D6F98310320E1A84FBC65BF30A2A592C419087
SHA-512:	B8508D07DCBDB469EFE99F0E7DACA8FC47083F2192168774210E3E2313B0A937D7BAC5C52B0F3F8962B3A8C0C5C5F787CA82A934F7B0EFA2E90D1C2B9305D3 57
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....-ab....."!.....8.....W... ...`..... .....`..... ..`.....V..K....`..... ....H.....text...47... ...8..... ..`.rsrc.....`.....:.....@..@.reloc..... .....>.....@..B.....W.....H.....H....]..... .....D..... .....".E.\.....*... .....*.

C:\Program Files\iba\ibaAnalyzer\ibaHdOfflineActiveX.ocx

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	312832
Entropy (8bit):	5.132821690677885
Encrypted:	false
SSDEEP:	3072:XOT26pfKJvGQsoU8ndX2wUCodiH+oOOQ/eyGeZzaXk:60uXkXWC1yt/eyGeZv
MD5:	EE18C2CE6D57D57EDFE3977D34CFCFE7
SHA1:	B00C2F4FDA23C8DDA1B3CABE6F9077EBFD97B2ED
SHA-256:	D67E35D814734CC971FEBBE6B86790870394AEC904AAA3B5F3B9053D5DDB070C
SHA-512:	105B5A615D63115FE8F73244D38B247B837A472ED84C3D7E848DA28DE6C8959A864004D61AE1EE7E5808E9FE241D6635318A8AA6F5E3B6F38E4DE940AA3F35E 3
Malicious:	false

<table>
<tr><td>Preview:</td><td>MZ......................@................................... ....!..L.!This program cannot be run in DOS mode....$........J.+...+...+...S...+...y...+...@...+...@...+...^...+...^...+...^...+...+...*...^.. .+...^...+...^...+...^c..+...+...+...^...+..Rich.+.........................PE..d...l.ab.........." ....`........................................0l.......l.......... )...... l...............|...4 ..T.......................(.... ..8...............`...............H...........text.............................. ..`.nep....0.......................... ..`.rdata...a.......b.................@..@.data....G...p...2.. .H.............@....pdata..l...........z.............@..@.rsrc...).......*...~.............@..@.reloc..H..........................@..B.. ....</td></tr>
</table>

C:\Program Files\iba\ibaAnalyzer\ibaHdViewUtilities.dll

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe</td></tr>
<tr><td>File Type:</td><td>PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>13312</td></tr>
<tr><td>Entropy (8bit):</td><td>5.112524342692505</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:hMU6VjGsOpM+eGA6p2z721E37EiFhI8NsRm0ebxXdmEYK:hMUuqsOut6QziCAiFhOEpdoK</td></tr>
<tr><td>MD5:</td><td>6EB5907967FDB43DEA73FBD285B6940C</td></tr>
<tr><td>SHA1:</td><td>EB156962701066D3231F9DDF3F23A7366D637A9C</td></tr>
<tr><td>SHA-256:</td><td>A2C68D8193EF6697DD3325786784CEFCD8C409DAD393F722C3C2B78310B222DE</td></tr>
<tr><td>SHA-512:</td><td>B601462FA481C1C657C4CC0FFB5B8250BC8F97503CD03088CF9D8C0BAEB7531374F2509848DC334EFA154C2598282D941145553E8E9AF1FC021321DE6D3473F</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...J)\a.........." ..0..,..........J... ...`....... .................................. ..`................................`J..O....`.............................(I.. ....H...........text....*... ...,................. ..`.rsrc........`.....................@..@.reloc........ ....2.............@..B.................J......H........)..I...........H.. ....0..R.......s......,G......(....o....u..........(....o....u......s.......o-.....o......o.....*...0...........(......o ....%o.....o....*Br...ps.........*.0..)........{.........(....t......|......(...+...3.*....0..)........{.........(....t......|......(...+...3.*....0..)........{.........(....t......|......(...+...3.*....0..)........{.........(....t......|...... (...+...3.*....0..)........{.........(....t...</td></tr>
</table>

C:\Program Files\iba\ibaAnalyzer\ibaLogger.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	192512
Entropy (8bit):	5.535534550972867
Encrypted:	false
SSDEEP:	3072:L6X0ln6sun0wTXsiQcqVWWL8I+OdwW63Yfq1KthjAN:9ZYQVWW4I+Ol63Yfq1A
MD5:	969E7E685724222F59F0917696B1724B
SHA1:	C4225310C4500DD99C2E9F88C964ABEFCDAD4EA5
SHA-256:	E7E1435874533AADF160241953427B0F5439EBE8C0D3057881D0A8C56CF2A666
SHA-512:	6FAC63AC7E358BCD31843D6253362F8D51562F2837F27E3A7E0C7B46517B78B71672789D0EA55605AB35F57C55F51FA7DFA0202EA017D0FECACA3B64DB53611 F
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......]..........." ..0...... ......^.... ....`....................................O.......T........................................................................... .............. ..H...........text........ ..................... ..`.rsrc...T..........................@..@.reloc........ ....@..B... ....

C:\Program Files\iba\ibaAnalyzer\ibaManagedFFT.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	31232
Entropy (8bit):	5.447073331727446
Encrypted:	false
SSDEEP:	768:UWeoDzUnbBahGyUVEv3lbv8i8CdktX7nS2SWrbN:UUsbrvVbSsX7nNV
MD5:	A311488EBCFD191DD3ADF674C47DE82D
SHA1:	752FB4ECE4EE0E10E4A4507538BFDA0341A07AE4
SHA-256:	395FBCA54D8AFEE9B1B3DE5F0E4B236C5980AB3D90977751F259E325AA684EAC
SHA-512:	C80117173760A8203C5AEF8F7A2D8855445ECAD801FEB531C659C2ED8A90944F416CFABF7673E88A9F243F2451767A2EC58B4B29B95F5F5D1663DE5EAB1D1E9 F
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....{*`.........." ..0..r..........V.... ........... ................................. ..`....................................O... ....H...........text...\q... ...r................. ..`.rsrc...............t.............@..@.reloc......... ......x.............@..B...............8.......H........V...9..0..D........(........(....(........}......}......}.......%...}...........}....*&.{.....i*..{....*&.{.....i*F.{....o... .t....*...0..S...........(....;).......(....(.............{....9......i.{.....i/I..+,...{.....{.....i.{....X..iY.X.{.....i]....X....i2...}......}....8......+....{.....{.....X.{.....i]....X...{.....i2...{.....i}......}....+c..i.{..../...+..... {...........X......i2...}......}....+)...+...

C:\Program Files\iba\ibaAnalyzer\ibaPdaPluginInterface.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.9489411534011678
Encrypted:	false
SSDEEP:	96:PE4ieOEyokSG/qi6Q1WDVVV6sy3okeNi8QRtJ:PoeOfSG/qw1WDl6sGxt
MD5:	1AF8726800A9EC1AB2F0BBFD9F22A69D
SHA1:	363395B0C5AF78FAEC24DA7D81BD042B354704DC
SHA-256:	A0431E693105422BD942E1FA0752E1802882F982CED782CAB949D9F6E6ECACC7
SHA-512:	8BDAE0FE2DD0267C241FCFC883A7D3E89593A647E2FE87AF62630CC9EAB77598280FB15E24C351995B15535AEA5F9B599F4CC4E675E3F27042C0B6E13360AD D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...;)\a....." ..0..... .....v.... ...@..... ....@.....$...O....@.,.....`..... ..... ..H.....text...|.... ..... ..`.rsrc...,....@..... .....@..@.rel oc.....`.....0.....@..B.....

C:\Program Files\iba\ibaAnalyzer\ibaPdaServerInterfaces.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	6.1983947016203995
Encrypted:	false
SSDEEP:	6144:R0250Cklz4Hta2B8NvavqzrTI40Blw6clbTjHPdjV5NXYwsumOAVAOyNbXparQL:RHScHtJB8yHBO1D75pYvVYppbL
MD5:	2CE9C8DBB9327B3904A0CB51F3F2EB12
SHA1:	0B24CA4556DB45C7EE06EB4F52645A915CB0D9AB
SHA-256:	3494F09C87B2D84C729D68034F0C3420ABF3EFC0CB6AC33E5B1D1C69A963FF42
SHA-512:	3A0A718F3BFEF002F86FFEFC9479D7AF04C2A0D88B78CB050CDAB33EDA49543F79F404CF548C19C8C7F55BDF519C989FB6EB0BE40AFFB73172BEF4ACD2C63 87B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...<)\a....." ..0..`... .....r... ..... ..`.....Lr..O.....,..... ....H.....text...,S... ...`..... ..`.rsrc...,.....p.....@..@.reloc..... .....@..B.....

C:\Program Files\iba\ibaAnalyzer\ibaRunTime64.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1488896
Entropy (8bit):	6.386579696496501
Encrypted:	false
SSDEEP:	24576:rCInl/liS2Eic0S/ZphOjFeoWDnZYxKml9e6MgwgGpRAJO8i5R46e3AE4LRlpCse:TYS2Eic0uZp28oWDn4pLe4i4vwE43pC5
MD5:	73C656C5E22626B8C1EC1FDE63CB16D7
SHA1:	D95AD3CB6337618747A82726FFC56566DEA1F434
SHA-256:	22BCC97D3C9774418CDA6FC40C43C2918E8588D153418D05A2D4E98F98E62383
SHA-512:	647C2C3C6D2F1C0861A89F4F5AC6C2D9DF0AD9FD6616ABB933DE6868D81050FA60245205DED0113D516523ECE84B90F8D4BB78ED5C5ECF9A7D194713D5458 B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(D.Jl%m.l%m.l%m.....m%m.K...d%m.K....%m.....g%m.l%l. .%m.K....%m.K...m%m.K...m%m.K...m%m.Richl%m.....PE..d.....[....." .....0.....P.....x.... ..v...P....M.. .....-..... .....text..... ..`.rdata.....@..@.data.....X.....@....pdata..8I...P...J..... .....@..@.hvm.....F.....@....hvm0....:.....<...H.....`..`.reloc...-.....@..@.rsrc...v.... .....@..@.....

C:\Program Files\iba\ibaAnalyzer\ibaShared.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	dropped
Size (bytes):	568832
Entropy (8bit):	5.924238171742334
Encrypted:	false
SSDEEP:	6144:4Egkwvdtw/A8LeWfks/PA4x6DTMzUdqZYGaiXPtSYgWvDxL0M6dlxec0Ab36v4c1:4Lc/7p/4gOqtaiVQKRJZFL
MD5:	92AFAE661B4D33E86198219B9B041F3A
SHA1:	21C5EA293C7B54481805E8181AEA6A187B2D0736
SHA-256:	B1FE30EDEA7ADEDD08FC8C6773DC5AF7AE4ED5164FEF5F21A8BD537EE0CA690A
SHA-512:	FC4BC0AAD1D7C42BE7C0B794FB0752E25BBD395B6BE495CC441D1DB7BF6BA9A9774736B4D2828B5733EBA7298F8B909B0B73253FB01C1ACC48E551E28F8F12FD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....N\a....." ..0.....&.... ....`.....O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....\.....>...}.....0.....o.....*.~.....o.....o .....iXs!....~".....+K.....(#...-...r...p($.....($.....o....,.. ..+...o%...&.....X.....i2...o&...o'...*.0.....o.....,*.,...(....*.~.....o.....o .....iXs!....~".....8.....(#...-...r...p($.....($.....o....,....+~.(#...-...o%...&...o....,...+_.....o ... .Y..+2.....o(.....o....,....o%...&....o).....+....Y.....0...o ....

C:\Program Files\iba\ibaAnalyzer\ibaSharedGui.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	939008
Entropy (8bit):	5.892331880687775
Encrypted:	false
SSDEEP:	12288:T1fqsmubFXDqSmYbDXG+drwGIjXe5l0mTABMWZYZuPPTqzm2q1:xZkV0mkMWZYZuPPuzm2q
MD5:	3DB111626FABF8A7C1DFE98E4367E363
SHA1:	6D036704C441705D14628B7760552E0E19743B5A
SHA-256:	2234CA6F4391879EEF084DE43FB57BB46AAE37695E16B34F7EF9CC023D82BE3A
SHA-512:	387C4DF9C963939801D5A54FDDEDD8B803B21B1746B1D063173B4FE9E6ECB658F0C09E7197924BAEBD146B3685F7944439A543CDEA88A6E323A81029271E391
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....." ..0..L.....i.. ....`.....oi..O.....h..8..... ..... ..H.....text....J... ...L..... ..`.rsrc.....N.....@..@.rel oc.....R.....@..B.....i.....H.....S..\4.....(2...*J.r...pr...p(!...&*..0..#.....(....&..o.....ta...o....&..&..*.....0..... .3. .....3. .....(....*...0..3.....(3...(4...}C.....(....&.{D.....*". ...._*....c*J.(.....(....s5...*". ...._*....c*...b*...d*....b*....d*&. ...._h*".....*....*" ...._*..(2...*f.~6...}..... (2.....}....*...0.....o.....(.....*.....{.

C:\Program Files\iba\ibaAnalyzer\ibaThreadSafeNativeFFT.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	136704
Entropy (8bit):	6.32034053650098
Encrypted:	false
SSDEEP:	3072:xr/3tI3wI+sALHCmR/hn3jzRRlnuPl512Xs:JFll+JrR/h3jzRRluj1
MD5:	3D9604F7205734BE4972FD1CB597DF08
SHA1:	1B681527C19C425DF7787E688D850504473982F3
SHA-256:	DF2476A22D8E8CDCBA51DE7897D3CD2DE3E2F9336402410B5F738F0AC95BDEA1
SHA-512:	33482ED9EC8C35353EA397981533DB4D47738BBBBF40717137111021E0C82D26D6E671D48D78E20CE4F8D168FC87C1BCF729B05550B687E1E90DE85A4D897E1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T@..:...:..:.....:...:.....:...?...:...>...:...9...:...:...:...:...:...:...?... .:.....:.....:...8...:.Rich..:.....PE..d....I*_....." .....d.....Gg.....`.....`.....T.....@..p.....P..h .....T..... ....(.....H.....text....X.....Z..... ..`.nep.....p.....^..... ..`.rdata...d.....f...h.....@..@.data.....@ ....pdata.....@..@_RDATA...-.....@..@.rsrc...p....@.....@..@.reloc..h....P.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\ibaUser.Forms.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	192512
Entropy (8bit):	5.779857151933466
Encrypted:	false
SSDEEP:	1536:cRTY61jj8lFP9Ik3pV3N7wvZ5UZD4B2YOXh41GJMRU2YIK6JgQmn0NvqHud4sFBv:Ejj8HG4LWCZD4DOXhUvJYIK0x42b

MD5:	E7156F4CA7E29371F8A9291B6220ADED
SHA1:	379942FD61BECE7ADF57E7D792FAADD9BBEB92F1
SHA-256:	AACE65447C8D9C68207E26D25FC7F419E37A4E92F062E0592774C6170EEEA8F5
SHA-512:	0CE58DFC3053656D3D39A069AAC6E7BAD6C9C86AFF43D45A912E2C6797ED0FAF64F23CFDBA8FA00DA5FA92E65E60A07F069FB3473CEA91CBCDB0F67AD105 97E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H.....'' ..0..... ... .`..... ..`.....}...O.... .....@.....T..... ....H.....text..... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....X.....0..Y.....(.....}.....}.....}.....o.....}.....}.....}.....(.....}.....($...*..{.... *....0..N.....(..... ....0...d.(. .....+*. ,..... .....+.(o...*(p...*(r...*(q...*r...p*..{....*..{....*..{....*..{....*..{....*''..}....*6..o....o....*v..(n...(....-..+..(....o....*>.-.(m...*(n...*R.o.....,(m...*(n...*..{... .*''..}....*>...(...._o....*R..J.(....f_.o....`T*..{....*''..}....*6..(.

C:\Program Files\iba\ibaAnalyzer\ibaUser.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14848
Entropy (8bit):	5.223745338549667
Encrypted:	false
SSDEEP:	384:Tiis9uW8bXmDVl98+aKAVcbrofrT9o1UR:2N8b2DV87G3+N
MD5:	4629FE2BE826F8BFDD936361D88CEA88
SHA1:	0E25BDB2D0452E22065351DDEAC6B6F1B2F657D0
SHA-256:	BFEAE3E4EF7CAB6C4C9A416E00EE6FE700F5BF292BFCB71AAAB9B3026194C4D2
SHA-512:	6C38A0D56EC0771DDDEFA99AA2758C7C44A6FDC63FD261E4C2158AEB3D1F466703E7FF1E8F2429EC71318AEBCF717CB0FC016EFBB89F2BC17EE0630D26E07 D7A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o.....'' ..0..2.....Q... ...`..... ..... ..`.....P..O....`.....P..T..... ..... ..H.....text...41... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....8.....@..B.....Q.....H.....,.H!.....TM.....f.(.....}.....s....}....*...0.....(.....o.....o....r...po....o....u'.....(.....(4....(....Q...D.,. .o.....{....o.....,.(3...Q+..(2....{....o.....o....(....Q.....*.....:A.....KK.:.....0..L.....(.....s.....s.....r%..p..(....(....o.....(.....,..o.....,..o.....*.....(6.....9@.....0.....(..... (....*...0.....(.....s.....s.....r...po ...,..r..

C:\Program Files\iba\ibaAnalyzer\ibaViewInterfaces.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	44032
Entropy (8bit):	5.623918763496899
Encrypted:	false
SSDEEP:	768:CHkp+aUImUc7k01cw79Zi+eVWw1Kf0W9lrD1x4:Ykp+aSL+u9ZiNWMKfxX1x4
MD5:	03A1D6B31124FFA78AF404F1DFFD9BCC
SHA1:	A007C2CB3D6EAEC8EF9738C9DC104B748A9E6F42
SHA-256:	D6EECC6BFBCB9D6761180185F24EF8CD71D754EA8F1523A3781E4853C2BB79BD
SHA-512:	65F86D5FB80E45BA94F03632A5D298AFC3510018EB5EF69031947DC465E1BCD6A630BE29BB77521A3117F44D34C4332D7AEC877896650531483483 6E96189AD6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...;)\a.....'' ..0..... ....@.....|...O.....0.....D..... ....H.....text..... ....`.rsrc...0.....@..@.relo c.....@..B.....H.....*.....>..}.....}....*^..}.....(....X}....*N.{....{....Y(....*J.{....{.....*~.{....{....3..{....{.....*.*..{.... {....3..{....{.....*.*...0.....q.....(....*v.{.... @B..j[.{....{....YXi*...{....{....(....}.....{....{....(....}....*...0..e.....{....(.....{....(....r...p..r...p(.....r...p(....(.....$&r...p.{.....M....{..... M...(.....*.....??.$....6.....o....*..

C:\Program Files\iba\ibaAnalyzer\ibaViewUtilities.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	423424
Entropy (8bit):	6.119668757985366
Encrypted:	false
SSDEEP:	6144:Qk+WOQ3WpCUD03DIcViVsnajsvZ2i02MsJ2LLThsQXMNfwH6P0:QkykUDszViWnawhQXMNfd
MD5:	D52F6A7EB456EB6C955FB3EF2270795C
SHA1:	F99C40293432566010E67EE62BB43CA54B49DF5E
SHA-256:	7AF5D17BEAB6BBE635ECA98B2CACE90BF295B38A0C25027A4D448A9259CAC3FD

SHA-512:	92A7EA730751EC5879BCC951DF0D23723253AD5639CAEF83C26B21D15A66F3B51EC7DBBCADF1E30ADABDA46384449F39E4B29E113B86CD301BD650C4CB46A 540
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B)\a....." ..0..l..... ....@.....x...O..... .....@..... ....H.....text...0j... ...l..... ..`.rsrc... .....n.....@..@.relo c.....t.....@..B.....H.....:..L.....p.....sl...}.....s-...}.....(.....}....*....0.....(.....{.....o/....om...*....0.....s.....oK.... {....o0...o1....+M..(2.....{.....o3.....o.....o4...,*.o.....o5.....o6....on...(7...,....op.....(8...-.....o9....*.....Zx.....0..._.....s:.....{....o0...o1....+ ..(2.....{.....o3...oo...o;.....(8...-.... .....o9.....s....oK...*.....-D.....0..|.....{.....{.....oj.....om..

C:\Program Files\iba\ibaAnalyzer\libiomp5md.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1177288
Entropy (8bit):	6.420824331145782
Encrypted:	false
SSDEEP:	12288:NzXTfLhPVxmFiyeBHc+h/xHZJDkyEHzZF9t7gRfChPr9ZfW:NzXvhT8+NtZJDkyETZF37gRerzW
MD5:	B9ECA4A35B09CCF41870A20EF791952A
SHA1:	5C441C11682018ABC98000820D68F9566F84B193
SHA-256:	5F14C93BFFC32B50EE291402F56453F22469E798FA086D472A2D3D87B93B9D36
SHA-512:	A0B16E821C4E068B7B774FFBC70A7EA5B7609FB743E6E193631B460DA45A65EACA48D34CD95C1B74BF5DA7137A26B12A52279F935A8BF920132A24E7A9948DD 0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.X...X...X...Q...[...X..."...F..Z.....Y...7...z...7.....C...Y...X...g...7.T.. .7.Y...7.Y...7.Y...RichX.....PE..d...>/gV....." .....<...\.....@.....U{.....(....."....."....!...T.... .....P.....text...:.....<..... ..`.rdata.....P.....@.....@..@.data....j...p.....X.....@....pdata..... @..@.data1.....@..._RDATA.....@..@.rsrc.....@..@.reloc..R-.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\mkl64_parallel.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37510144
Entropy (8bit):	6.686180554028836
Encrypted:	false
SSDEEP:	196608:slvlOzfHW36EHyFEsaoCQnwePnbrU/FMKMe6ZH7DnrZxmK63dI9S2bOkSve3ebPi:4uKl6ZXnrZtOkS05n
MD5:	6B81FDC3D10F3C4DD9673B266A7BDD41
SHA1:	23A9E98E2D39F1A6A759DC38397DD92E58EDF364
SHA-256:	D69F563AFAC5966ADDC734CF8F592A7181082AC48D78378403834EC7C6621660
SHA-512:	95AC71CB251D7813C8CE5C0955BDC048320EF314F7521E71744F215B3AA1DEB563512254076277DB1A9AE1AA31D0EAC62AFC9C2DFAD9D0A78C0B2FD2F0C945 02
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z..t>.'>.'>.'[..&2.'[..&-.'[..&..'[..&=.'l..&#.'l..&..'l..&6.'>.'..'Q.$'<.'...'..' >.'}.'...&?.'..G'?.'...&?.'Rich>.'.....PE..d....g._.....' .....'....!.....@.....hF=...`.....a4.....Lc4.<....P@.....p:.D.....`@..W.. .*.....@.*.....P.....text....9.....:..... ..`.rdata.....P... ...>.....@..@.data...p....p4.....^4.....@....pdata..D....p:..... 6..... ..@..@.rsrc.....P@.....;.....@..@.reloc...W...`@..X....<.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\msvcp100.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	608080
Entropy (8bit):	6.297676823354886
Encrypted:	false
SSDEEP:	12288:koBFUsQ1H5FH3YUTd/df0RA7XkNvEKZm+aWodEEiblHN/:dFUsQ1H5FHdGKkNvEKZm+aWodEEcHN/
MD5:	D029339C0F59CF662094EDDF8C42B2B5
SHA1:	A0B6DE44255CE7BFADE9A5B559DD04F2972BFDC8
SHA-256:	934D882EFD3C0F3F1EFBC238EF87708F3879F5BB456D30AF62F3368D58B6AA4C
SHA-512:	021D9AF52E68CB7A3B0042D9ED6C9418552EE16DF966F9CCEDD458567C47D70471CB8851A69D3982D64571369664FAEEAE3BE90E2E88A909005B9CDB73679C 2
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$..-`..~`..~`..~i.4~b..~{.;~c..~`..~...~..?~a..~{.9~a..~{..~P..~{..~Y..~{..~e..~{.<~a..~{.=~a..~{.:~a..~Rich`..~.....PE..d.....M......" .....f.....q.....cy.....@.....m.....<....P.....=.. .0..P....`.....text..... ..`.rdata..-.....@..@.data...0L.....8.....@....pdata...=.....>..... .....@..@.rsrc.....P.....@..@.reloc..R....`.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\msvcr100.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	829264
Entropy (8bit):	6.553848816796836
Encrypted:	false
SSDEEP:	12288:QgzGPEett9Mw9HfBCddjMb2NQVmTW75JfmyyKWeHQGoko+1:HzJetPMw9HfBCrMb2Kc6dmyyKWewGzB1
MD5:	366FD6F3A451351B5DF2D7C4ECF4C73A
SHA1:	50DB750522B9630757F91B53DF377FD4ED4E2D66
SHA-256:	AE3CB6C6AFBA9A4AA5C85F66023C35338CA579B30326DD02918F9D55259503D5
SHA-512:	2DE764772B68A85204B7435C87E9409D753C2196CF5B2F46E7796C99A33943E167F62A92E8753EAA184CD81FB14361E83228EB1B474E0C3349ED387EC93E6130
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....pm...>...>...>..>...>...>F..>...>...>...>..>...>..>...>D..>...>...>... >...>...>...>Rich...>.....PE..d.....M.....” .....sy..... .....A.....@.....pt.....`..(.....pb.....P..... .....text...F..... ..`.rdata.....@..@.data...L}... ...R.....@....pdata..pb.....d...Z.....@..@_ CONST.....@...text.....2... ...4.....@.. data.....`.....@..@.rsrc.....v.....@..@.reloc.....z.....@..B..... .....

C:\Program Files\iba\ibaAnalyzer\reg_dataextractor.bat

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.529549786187404
Encrypted:	false
SSDEEP:	3:vBimAFFFFFxwLuI/E3yeKrn:vBqNULV/xVrn
MD5:	5A2771E49D1C1E14736910C94FDB1966
SHA1:	A9F8511CD4CBC3150280776487FF49D26E1CC178
SHA-256:	31500328F2377CABCA90B8C1A3CD8C6C1E41211FEB839C95011547595B729314
SHA-512:	7E9C563D7A0E49C22E20E61D3E1B9521E1239B36B3F69E8977400727D0498EED82EFAE2F4EF2B6B74E6184414E6F7E80111DE2E66D996D84E514B4302D34322C
Malicious:	false
Preview:	pushd "%CD%" ..CD /D "%~dp0"....regsvr32 ibadataextractor.dll....popd

C:\Program Files\iba\ibaAnalyzer\reg_dataextractorMC.bat

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	76
Entropy (8bit):	4.5759834031694036
Encrypted:	false
SSDEEP:	3:vBimAFFFFFxwLuI/E3YQJJovGKrn:vBqNULV/4Jydrn
MD5:	E98207961C995F066CF7C62E92506883
SHA1:	DCBC155B28E87511DA042CB7005E2DC154E2DC69
SHA-256:	6EF4A0171DFC3C9CA6BE3E92FCF21BD36EE01E4BE9C216A890FC4CA5F67FB230
SHA-512:	BAE292E69418CAFCF5D1A98852ED4AD8A59B2E35EE4F4FF65B9F904A2DF1398C39E279F389B4FCFBF97E76E1EEA3C0C95CE2B7DD0DA4EF6B8EA4718FAA96E277
Malicious:	false
Preview:	pushd "%CD%" ..CD /D "%~dp0"....regsvr32 ibadataextractorMC.dll....popd

C:\Program Files\iba\ibaAnalyzer\support.htm

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	45027

Entropy (8bit):	5.351882502356651
Encrypted:	false
SSDEEP:	384:+BF/pCHHS6zKe2TZK+9V7mUPyS/pQTNm0cHW0G2jYVRG/CmHHA/eAct2MisMd9ln:+BFoL7KVpimwTmHHt4VRYkQxMK0jvDvf
MD5:	12441363165020A84B4624746A56F1A5
SHA1:	3C7CFE8637575B4EF07465014C966EA3AEE2F9C2
SHA-256:	4D43B6E1C6F08352BAD65724F4D0FE891CDD03FD187E32CFFD89C30E31CD69EA
SHA-512:	CCFB61A5D326C4D989F820AABDB87E4B18B6C07BC6EB2DFC3629686871C78FD0676B4283B0C89CB064708B6E3B55C05F2D498ADA21136900D5C39E33C08682 8
Malicious:	false
Preview:	<!DOCTYPE html>.<html lang="en">. <head>...<title>iba Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. <style>. body {. margin-top: 20px;. }.. * {. font-family: "Arial", sans-serif;. }.. .col-lg-7,. .col-lg-5 {. padding-left: 20px;. }.. h1 {. color: #037748;. font-size: 26px;. padding-left: 25px;. }.. h3 {. color: #aaa;. font-size: 22px;. padding-left: 25px;. }.. h5 {. color: #037748;. font-size: 14px;. padding-left: 20px;. }.. .container {. width: 320px;. display: inline-flex;. border-top: 2px solid #f4f4f4;. margin: 5px;. }..

C:\Program Files\iba\ibaAnalyzer\versions.htm

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	311791
Entropy (8bit):	4.535690207805419
Encrypted:	false
SSDEEP:	6144:Nvr4RMUkOH98c1QGCfcL6rvbXtluI4B/WnFAXUbhNdUwc2sX7t6OSoT:l0tkiecmjtluNB/WnFAXUbhNdUwc2sXP
MD5:	C9AA499AB7EB9800B956EFD5B2D59D65
SHA1:	BAEB133A67AE7A406EADB87D3745DA64C176F78B
SHA-256:	D929BD0CF7E91AAB6FEDBD7057D33813D323FF315B19C2037D920B9DD981246A
SHA-512:	EE9E280CB5F78DE32A8F5E2F74A32C9EB68339F283BFF76669A55BE3788C319117B1D5FF71454F65A856D15C708804B68C46F5A2FFEE22A72800D64181F69918
Malicious:	false
Preview:	.<HTML> ..<HEAD> ..<style type="text/css"> .. body...{background-color: white; font-family: Tahoma, Helvetica, Arial; font-size: 13px}.. .title..{color: navy; font-size: 26px; font-weight: bold}.. .header1..{color: white; background-color: #315BA9; font-size: 16px; font-weight: bold; margin: 0px; padding: 2px}.. .header2..{color: black; font-size: 14px; font-weight: bold}.. .warning {color: red; font-size: 14px; font-weight: bold}.. .btn_selected.{cursor: pointer; cursor: hand; color: white; background-color: #00AA00; font-size: 20px; font-weight: bold; padding: 4px}.. .btn_normal.{cursor: pointer; cursor: hand; color: white; background-color: #006600; font-size: 20p

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\regsvr32.exe.log

Process:	C:\Windows\System32\regsvr32.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1281
Entropy (8bit):	5.367899416177239
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPz:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1Q
MD5:	7115A3215A4C22EF20AB9AF4160EE8F5
SHA1:	A4CAB34355971C1FBAABECEFA91458C4936F2C24
SHA-256:	A4A689E8149166591F94A8C84E99BE744992B9E80BDB7A0713453EB6C59BBBB2
SHA-512:	2CEF2BCD284265B147ABF300A4D26AD1AAC743EFE0B47A394FB614B6843A60B9F918E56261A56334078D0D9681132F3403FB734EE66E1915CF76F29411D5CE2(
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

C:\Users\user\AppData\Local\Temp\nss310.tmp\InstallOptions.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14848
Entropy (8bit):	5.550299117674118
Encrypted:	false
SSDEEP:	192:86d+dHXLHQOPiY53uiUdigyU+WsPdc/A1A+2jwK72dwF7dBEnbok:86UdHXcIiY535zBt2jw+BEnbo

MD5:	325B008AEC81E5AAA57096F05D4212B5
SHA1:	27A2D89747A20305B6518438EFF5B9F57F7DF5C3
SHA-256:	C9CD5C9609E70005926AE5171726A4142FFBCCCC771D307EFCD195DAFC1E6B4B
SHA-512:	18362B3AEE529A27E85CC087627ECF6E2D21196D725F499C4A185CB3A380999F43FF1833A8EBEC3F5BA1D3A113EF83185770E663854121F2D8B885790115AFDF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L.p..q.,.q.,.q.,.q.,@q.,.~C,.q.,\R.,.q.,\R/,.q.,.w.,.q.,.Q.,.q.,Rich.q., ...PE..L.....K.....!.....<.....).....0.....8..p...81.....p.....@.....0..8.... .....text...@..... ..`.rdata.....0..... .....@..@.data... (...@.....*.....@....rsrc.....p.....2.....@..@.reloc.....4.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nss310.tmp\SimpleSC.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	62976
Entropy (8bit):	6.324320451317714
Encrypted:	false
SSDEEP:	1536:i/qXv1si+Xsp9MNptZ8KMT6+nMA4fx+kmA:Bv1EXZnLMT5M3x+km
MD5:	D63975CE28F801F236C4ACA5AF726961
SHA1:	3D93AD9816D3B3DBA1E63DFCBFA3BD05F787A8C9
SHA-256:	E0C580BBE48A483075C21277C6E0F23F3CBD6CE3EB2CCD3BF48CF68F05628F43
SHA-512:	8357E1955560BF0C42A8F4091550C87C19B4939BF1E6A53A54173D1C163B133B9C517014AF6F7614EDDC0C9BBF93B3B987C4977B024B10B05B3DC4EB20141810
Malicious:	false
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....4.....`.....@.....0.....R.... ..... .....CODE....x..... ..`DATA....@.....@...BSS.....y.....idata..R.....@....edata.....@..P.reloc .....@..P.rsrc..... .....@..P.....0.....@..P..... .....

C:\Users\user\AppData\Local\Temp\nss310.tmp\System.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.568877095847681
Encrypted:	false
SSDEEP:	192:7DKnJZCv6VmbJQC+tFiUdK7ckD4gRXKQx+LQ2CSF:7ViJrtFRdbmXK8+PCw
MD5:	C17103AE9072A06DA581DEC998343FC1
SHA1:	B72148C6BDFAADA8B8C3F950E610EE7CF1DA1F8D
SHA-256:	DC58D8AD81CACB0C1ED72E33BFF8F23EA40B5252B5BB55D393A0903E6819AE2F
SHA-512:	D32A71AAEF18E993F28096D536E41C4D016850721B31171513CE28BBD805A54FD290B7C3E9D935F72E676A1ACFB4F0DCC89D95040A0DD29F2B6975855C18986
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j....l.9..i....l.Richm.....PE..L.....K.. .....!.....0).....0.....`.....p2.....t0..P.....P.....0..X.....text...1..... ..... ..`.rdata.....0.....".....@..@.data...d....@.....&.....@....reloc.....P.....(.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nss310.tmp\UserInfo.dll

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.331979080664426
Encrypted:	false
SSDEEP:	48:iViF7LLM4wXqQH1wRrOpArXMVyjlZSXRN:ky7EcQHu4tVy4R
MD5:	7579ADE7AE1747A31960A228CE02E666
SHA1:	8EC8571A296737E819DCF86353A43FCF8EC63351
SHA-256:	564C80DEC62D76C53497C40094DB360FF8A36E0DC1BDA8383D0F9583138997F5
SHA-512:	A88BC56E938374C333B0E33CB72951635B5D5A98B9CB2D6785073CBCAD23BF4C0F9F69D3B7E87B46C76EB03CED9BB786844CE87656A9E3DF4CA24ACF43D7A5B
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4.....Rich.....PE..L.....K.....!..... ....P..... "..... L ..<.....@..d..... ..L.....text..... ..`.rd ata..... .....@..@.data...X....0.....@....reloc.....@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nss310.tmp\databaseoptions.ini

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	493
Entropy (8bit):	5.105955790691739
Encrypted:	false
SSDEEP:	12:ZYrltNY1Q9uQ3QD2SUsUoUXQ3QB2VSfLNMv:ZYi1+uyUZUs2Xy4W6LNu
MD5:	47B11716B703AA82956A84F494F16222
SHA1:	D54F91B482F544420F058FEE4B158A910B547FD0
SHA-256:	44B107479B06FB6AB4706B64E9E28BE915AFFF5F7D017CB181228665C04EB9C5
SHA-512:	0C3A1308FCCB214F3750BDEB4547F5F5423719D97DDD8ECB32E27F1363DA32C3020AFC6FE5C48AE3207AB69BCF81A082A9908D36FDE7C58717FE8A4F5128F3A
Malicious:	false
Preview:	; Ini file generated by the HM NIS Edit IO designer...[Settings]..NumFields=3..RTL=0..State=0....[Field 1]..Type=RadioButton..Text=no database support..Left=16..Right=288..Top=20..Bottom=31..State=1..HWND=459330....[Field 2]..Type=RadioButton..Text=install the Extractor database library..Left=16..Right=289..Top=40..Bottom=51..State=0..HWND=1114204....[Field 3]..Type=RadioButton..Text=install the MC Extractor database library..Left=16..Right=289..Top=60..Bottom=71....State=0..HWND=524858..

C:\Users\user\AppData\Local\Temp\nss310.tmp\ioSpecial.ini

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	786
Entropy (8bit):	5.318020615769567
Encrypted:	false
SSDEEP:	12:lOO8VTXAgQRvA4ZEh6H4gNo4f1hb+s+7mjp4gNRhIoiX4GXWkNzD6lrVf6QD/:kTsRvA42hw1O42s+g1ViXxmkNHQVCQD/
MD5:	968BDD1066CDB9F12E83DC962ED1F931
SHA1:	46CA6CB78EBFEF29AA678206A3C8A18E41871A2A
SHA-256:	67FCE4D3967DF10862E881BC2889EBAFFEDD9526BA10741E7F856D8B66AB244A
SHA-512:	074AE6B7ACF472E9144169EA36B8E33F6C26CBBAC23828CCA347B1CF7058EBAC8AF3A706BED8698E460EED403A1F5C06D8961E2FEF2CFABA12B300CBF0A1FB61
Malicious:	false
Preview:	[Settings]..Rect=1044..NumFields=3..BackEnabled=0..RTL=0..NextButtonText=..CancelEnabled=..State=0....[Field 1]..Type=bitmap..Left=0..Right=109..Top=0..Bottom=193..Flags=RESIZETOFIT..Text=C:\Users\user\AppData\Local\Temp\nss310.tmp\modern-wizard.bmp..HWND=132022....[Field 2]..Type=label..Left=120..Right=315..Top=9..Bottom=48..Text=Welcome to the ibaAnalyzer v7.3.6 (x64) Setup Wizard..HWND=132026....[Field 3]..Type=label..Left=120..Right=315..Top=55..Bottom=185....Text=This wizard will guide you through the installation of ibaAnalyzer v7.3.6 (x64).\r\n\r\nIt is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.\r\n\r\nClick Next to continue...HWND=132028..

C:\Users\user\AppData\Local\Temp\nss310.tmp\licenseserveroptions.ini

Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	729
Entropy (8bit):	5.022967999468027
Encrypted:	false
SSDEEP:	12:lNNwpZEGXvz6g8CFJKdX+PjDKyHQc506pdNgF46k+uvcTKSv35hwEwqm:pwV/z18eKE7WyHJ97gFfFTvoEwqm
MD5:	9381BA9CDE37F9F745AB52B7C79BBF8B
SHA1:	3B7EA51AA38151EB9FED44CC824245A84FFA0796
SHA-256:	E93C088744103641C50799E22B3974928C01BD40908269EC4437FBCBBE5975F7
SHA-512:	C185CE2C6D9210AAB0FA4794B1E54DCAE497B8F5731984ABBEBEFB16060D59B7D9205D6A3A5587F38945B7F38CC6D79935C8ABCE848DB0D8CEA67DE360A6CC23
Malicious:	false
Preview:	[Settings]..NumFields=2..RTL=0..State=0....[Field 1]..Type=Label..Text=This version of ibaAnalyzer is NOT compatible with the old license service (ibaLicenseService). If you use licensed components of ibaAnalyzer handled by a license service, please contact your local iba support to update your license service to ibaLicenseService-V2.\....You can safely ignore this message if you do not require any licensed components of ibaAnalyzer or if the licensing for ibaAnalyzer is handled by a locally attached dongle...Left=16..Right=288..Top=20..Bottom=90..HWND=524836....[Field 2]..Type=Checkbox..Text=Do not show this page again in future ibaAnalyzer installations...Left=16..Right=288..Top=91..Bottom=102..State=0..HWND=1769576..

C:\Users\user\AppData\Local\Temp\nss310.tmp\modern-header.bmp	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PC bitmap, Windows 3.x format, 150 x 57 x 24
Category:	dropped
Size (bytes):	25820
Entropy (8bit):	2.0503212840436267
Encrypted:	false
SSDEEP:	48:aXVERfRyriqayRIUHN7q4ldlVl3CZ38J1MLJF7IWoNe1T:aMYr0XEq4DvBqEOJFlT
MD5:	BACF7C26EF8F85D3AB86670B59605F5B
SHA1:	E461A2CC770155F24532F41E275E97ED7DACB47F
SHA-256:	BAB75066C6CCEF8FE6070E8C0A354E24439AB6D988EF49C4CF2B5924EF7F83FF
SHA-512:	5061A5D91902109AC3E91E1828A279E79E96DDF4B1D972D64E7A1D631058222628FE6F2FE1DF19D5180FB35624B96443E253132773DB669D31DB5C4FE33AEF57
Malicious:	false
Preview:	BM.d.....6...(.....9.....d..... .....?..... ....?.....

C:\Users\user\AppData\Local\Temp\nss310.tmp\modern-wizard.bmp	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PC bitmap, Windows 3.x format, 164 x 314 x 24
Category:	dropped
Size (bytes):	154542
Entropy (8bit):	3.3322603686910237
Encrypted:	false
SSDEEP:	768:2DpLES1HgquaaW3ClVJkgNKTf5/PR50Ogm2:2FLES1ubWSl7IfpH0V
MD5:	DE4F933E003528B0376766A4666EDFC5
SHA1:	5BCD485EA0279CD577EACA55B8A8510C83146634
SHA-256:	07B81FDA0231FA03BD265F3A2665E12C99CF7679D054BBAB92EE34DFE66CA6AE
SHA-512:	F3E44BCDA1F458735EE58DF0A89F04641A40DD685BF3263963E87D54921344B6A46ED1550A157F8198C0F303682097589C245843830554BB9945D0D8FECF7A45
Malicious:	false
Preview:	BM.[.....6...(.....: ....

C:\Users\user\AppData\Local\Temp\nss310.tmp\nsSCMEx.dll	
Process:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	330240
Entropy (8bit):	6.783443040903562
Encrypted:	false
SSDEEP:	6144:UOAFF2QXiZEoeRiwgMbvSwyZyyB5ErpvuTLkRiAj0Grm5+Gl:UOAFXXsoiwgMbvSwyZL5wuXkRBjHVGl
MD5:	F4D7CAB85C4452407C5861E5E864DAC6
SHA1:	896CF8D8B18AF75C3AE51E24A24DD6214C8DBBA9
SHA-256:	7C35F19E09F182CEDC27AA5E73E3D1FA1AB9642471DCB1A817EF64D844AA3005
SHA-512:	3CBE203B4FF4D9CB30D9561019F8DCBC7C7023138795B553BE459931912E06C875434B356F5589703E1CEC8C7AF3DAE014F65D833FFE163DB7EDEDB961FBFCF
Malicious:	false
Preview:	MZ.....@.....0.....!..L.!This program cannot be run in DOS mode....$.....oKf.+*..+*..+*..NL..:*..NL...*.....-*..yB...*..yB..;*..yB..2*..NL..=*...e.**...t..**...t../*..NL..<*..+*...+...C..**...C..'*...C..**...C..**..+*..**...C..**..Rich+*.....PE..L...v.ga.....!.....`..... .....@.....P...7.....T.....@.....$.....text...*..... ..`.rdata.....@..@.data..... .....@.. ..rsrc.....@.....@..@.reloc...7...P...8.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.999990419784602
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	ibaAnalyzerSetup_x64_v7.3.6.exe
File size:	69983376
MD5:	c1ae350f67039cbe69f10df9b8001371
SHA1:	6362ba848a6027939c642d4b405994ca5a96272c
SHA256:	fbf6ebb863e6ee15a9fbe144116fc568d929cdb560ad1380a45c71f761946cd1
SHA512:	032cde395658b300fc1d6e79a04c6da04169d35cfbd277ec6cb5044f391ae8ed88d31ec653be87cbfc8823e2a21918d2d269217c8e4f04e30138907243d7b635
SSDEEP:	1572864:tzpBbJ2s2nciVKOUmUQyja9kAdvnyRe/WhIS:L2RciCmUjaiAdvEhhIS
TLSH:	4FE733D85E1E8039E2684475D46AB8F11F3458F6A438C0932607BFFFD78F3E66026699
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	822648dad6d26992

Static PE Info

General

Entrypoint:	0x40323c
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 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:	099c0646ea7282d232219f8807883be0

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 11/24/2021 4:00:00 PM 11/26/2024 3:59:59 PM
Subject Chain	• CN=iba AG, OU=iba AG, O=iba AG, L=FÃ¼rth, C=DE
Version:	3
Thumbprint MD5:	CB5010FA85020150A3B61712597B8B2E
Thumbprint SHA-1:	ED30F5B2E756DD3CAFB89E5055E5823BD9D82FE3
Thumbprint SHA-256:	062CF22CB3B0087BBB7D6F3193B43CDA8A2C76E205310D729B82D8557C675D8D
Serial:	0DB533CEF828D7CC61E6D2ABB9AFECE1

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx

Instruction
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409130h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B4h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [00423F58h], eax
call 00007FF708BCF82Eh
mov dword ptr [00423EA4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F458h
call dword ptr [00407158h]
push 004091B8h
push 004236A0h
call 00007FF708BCF4E1h
call dword ptr [004070B0h]
mov edi, 00429000h
push eax
push edi
call 00007FF708BCF4CFh
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423EA0h], eax
mov eax, edi
jne 00007FF708BCCC2Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007FF708BCEFC2h
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007FF708BCCC85h
cmp cl, 00000020h
jne 00007FF708BCCC28h
inc eax
cmp byte ptr [eax], 00000020h
je 00007FF708BCCC1Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73a4	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x30000	0x65d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x42bba10	0x2280	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x28c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0xc000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x30000	0x65d0	0x6600	False	0.37779564951	data	5.22258519203	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x302c8	0x25a8	data	English	United States
RT_ICON	0x32870	0x1bd9	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x34450	0x10a8	data	English	United States
RT_ICON	0x354f8	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x35960	0xb4	data	English	United States
RT_DIALOG	0x35a18	0x120	data	English	United States
RT_DIALOG	0x35b38	0x200	data	English	United States
RT_DIALOG	0x35d38	0xf8	data	English	United States
RT_DIALOG	0x35e30	0xee	data	English	United States
RT_GROUP_ICON	0x35f20	0x3e	data	English	United States
RT_VERSION	0x35f60	0x2ac	data	English	United States
RT_MANIFEST	0x36210	0x3ba	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetFileTime, GetTempPathA, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetWindowsDirectoryA

DLL	Import
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Version Infos

Description	Data
LegalCopyright	iba AG. All rights reserved
FileVersion	7.3.6.0
CompanyName	iba AG
LegalTrademarks	
Comments	
ProductName	ibaAnalyzer (x64)
ProductVersion	7.3.6
FileDescription	ibaAnalyzer installer
Translation	0x0409 0x0000

Possible Origin

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

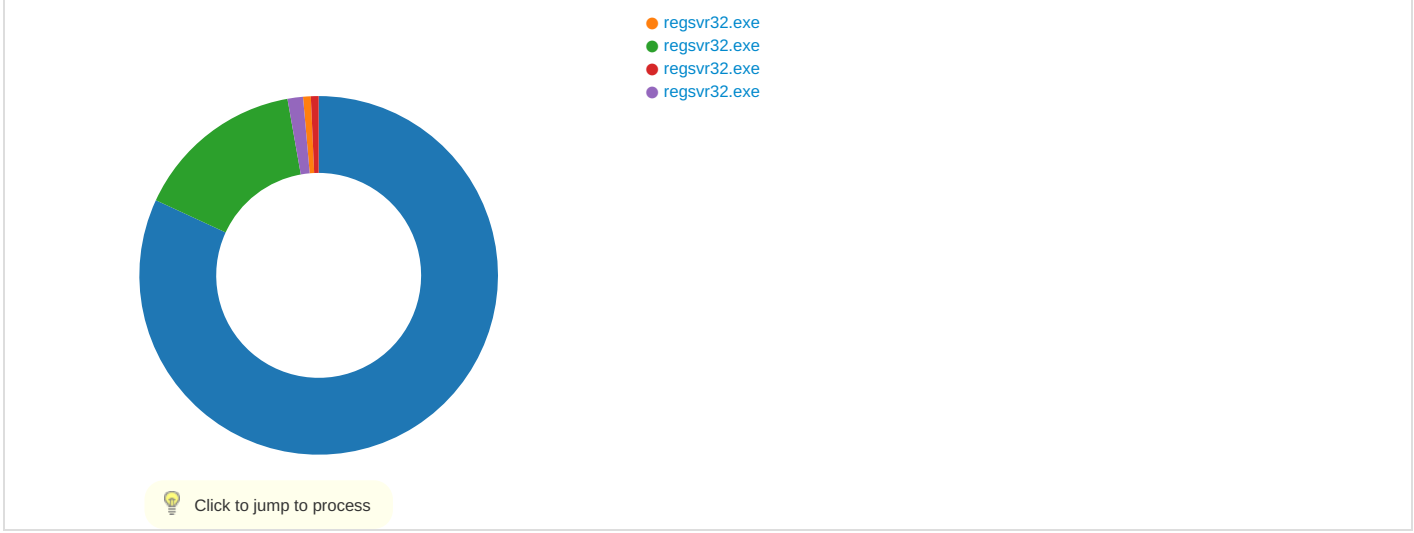
Network Behavior

No network behavior found

Statistics

Behavior

● ibaAnalyzerSetup_x64_v7.3.6.exe



System Behavior

Analysis Process: ibaAnalyzerSetup_x64_v7.3.6.exe PID: 7052, Parent PID: 5860

General

Target ID:	0
Start time:	18:42:27
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe"
Imagebase:	0x400000
File size:	69983376 bytes
MD5 hash:	C1AE350F67039CBE69F10DF9B8001371
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40322F	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nshAD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40589F	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nss30F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40589F	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nss310.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40589F	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA

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	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss310.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss310.tmp\licenseserveroptions.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\databaseoptions.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\ioSpecial.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\modern-wizard.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\modern-header.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\nsSCMEx.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\nsSCMEx.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	2	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\UserInfo.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\UserInfo.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\InstallOptions.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\InstallOptions.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\SimpleSC.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	5	405869	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4015E1	CreateDirectoryA
C:\Program Files\iba	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Program Files\iba\ibaAnalyzer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzer.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\SciLexer.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\versions.htm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\License_Agreement_ibaAnalyzer.pdf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\support.htm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaDataExtractor.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaDataExtractorMC.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\reg_dataextractorMC.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\reg_dataextractor.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\mkl64_parallel.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\libiomp5md.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\msvcr100.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\msvcp100.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\DevExpress.Data.v16.1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\DevExpress.Printing.v16.1.Core.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\DevExpress.Sparkline.v16.1.Core.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\DevExpress.Utils.v16.1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraEditors.v16.1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraGrid.v16.1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraPrinting.v16.1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\DotNetMagic2005.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\hdClientInterfaces.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\hdCommon.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaUser.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaUser.Forms.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaHdViewUtilities.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaLogger.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ICSharpCode.SharpZipLib.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaViewInterfaces.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaViewUtilities.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaPdaServerInterfaces.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaExpressions.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaPdaPluginInterface.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\OverlayWindow.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\PowerCollections.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\View.ibaEventTable.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\View.ibaGraphManager.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaHDOffline.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaHdOfflineActiveX.ocx	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\hdClient.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\hdCore.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaRunTime64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	4015E1	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	4015E1	CreateDirectoryA
C:\Program Files\iba\ibaAnalyzer\de	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Program Files\iba\ibaAnalyzer\de\hdClient.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\ibaHDOffline.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\hdCommon.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\ibaUser.Forms.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\ibaUser.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\ibaViewUtilities.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\View.ibaEventTable.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\View.ibaGraphManager.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\ibaShared.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\ibaSharedGui.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\View.ibaFFT.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\View.ibaOrbit.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\View.GeoView.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\ibaAnalyzerViewHostViewWrapper.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\de\View.ibaAnalyzerViewHostGraphManager.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Program Files\iba\ibaAnalyzer\fr\hdClient.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\ibaHDOffline.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\hdCommon.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\ibaUser.Forms.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\fr\ibaUser.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\ibaViewUtilities.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaEventTable.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaGraphManager.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\ibaShared.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\ibaSharedGui.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaFFT.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaOrbit.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\View.GeoView.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\ibaAnalyzerViewHostViewWrapper.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaAnalyzerViewHost GraphManager.resources.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHost.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostViewWrapper.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostActiveX.ocx	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaShared.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaSharedGui.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaManagedFFT.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\ibaThreadSafeNativeFFT.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\GMap.NET.Core.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\GMap.NET.WindowsForms.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\System.Data.SQLite.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\SQLite.Interop.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\Plugins	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaFFT.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaOrbit.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaGraphManager.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaAnalyzerViewHostGraphManager.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA
C:\Program Files\iba\ibaAnalyzer\Plugins\View.GeoView.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405869	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshAD.tmp	success or wait	1	4033B5	DeleteFileA
C:\Users\user\AppData\Local\Temp\nss310.tmp	success or wait	1	4054AF	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	30	40314B	WriteFile
C:\Users\user\AppData\Local\Temp\nss310.tmp\licenseserveroptions.ini	0	191	5b 53 65 74 74 69 6e 67 73 5d 0d 0a 4e 75 6d 46 69 65 6c 64 73 3d 32 0d 0a 52 54 4c 3d 30 0d 0a 53 74 61 74 65 3d 30 0d 0a 0d 0a 5b 46 69 65 6c 64 20 31 5d 0d 0a 54 79 70 65 3d 4c 61 62 65 6c 0d 0a 54 65 78 74 3d 54 68 69 73 20 76 65 72 73 69 6f 6e 20 6f 66 20 69 62 61 41 6e 61 6c 79 7a 65 72 20 69 73 20 4e 4f 54 20 63 6f 6d 70 61 74 69 62 6c 65 20 77 69 74 68 20 74 68 65 20 6f 6c 64 20 6c 69 63 65 6e 73 65 20 73 65 72 76 69 63 65 20 28 69 62 61 4c 69 63 65 6e 73 65 53 65 72 76 69 63 65 29 2e 20 49 66 20 79 6f 75 20 75 73 65 20 6c 69 63 65 6e 73 65 64 20 63 6f 6d 70	[Settings]NumFields=2RTL=0State=0[Field 1]Type=LabelText=This version of ibaAnalyzer is NOT compatible with the old license service (ibaLicenseService). If you use licensed comp	success or wait	1	402FE4	WriteFile
C:\Users\user\AppData\Local\Temp\nss310.tmp\databaseoptions.ini	0	394	3b 20 49 6e 69 20 66 69 6c 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 74 68 65 20 48 4d 20 4e 49 53 20 45 64 69 74 20 49 4f 20 64 65 73 69 67 6e 65 72 2e 0d 0a 5b 53 65 74 74 69 6e 67 73 5d 0d 0a 4e 75 6d 46 69 65 6c 64 73 3d 33 0d 0a 52 54 4c 3d 30 0d 0a 53 74 61 74 65 3d 30 0d 0a 0d 0a 5b 46 69 65 6c 64 20 31 5d 0d 0a 54 79 70 65 3d 52 61 64 69 6f 42 75 74 74 6f 6e 0d 0a 54 65 78 74 3d 6e 6f 20 64 61 74 61 62 61 73 65 20 73 75 70 70 6f 72 74 0d 0a 4c 65 66 74 3d 31 36 0d 0a 52 69 67 68 74 3d 32 38 38 0d 0a 54 6f 70 3d 32 30 0d 0a 42 6f 74 74 6f 6d 3d 33 31 0d 0a 53 74 61 74 65 3d 31 0d 0a 48 57 4e 44 3d 34 35 39 33 33 30 0d 0a 0d 0a 5b 46 69 65 6c 64 20 32 5d 0d 0a 54 79 70 65 3d 52 61 64 69 6f 42 75 74 74 6f 6e 0d 0a 54 65 78 74 3d 69 6e 73 74 61 6c	; Ini file generated by the HM NIS Edit IO designer. [Settings]NumFields=3RTL=0State=0[Field 1]Type=RadioButtonText=no database supportLeft=16Right=288Top=20Bottom=31State=1HWND=459330[Field 2]Type=RadioButtonText=instal	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nss310.tmp\ioSpecial.ini	0	263	5b 53 65 74 74 69 6e 67 73 5d 0d 0a 52 65 63 74 3d 31 30 34 34 0d 0a 4e 75 6d 46 69 65 6c 64 73 3d 33 0d 0a 42 61 63 6b 45 6e 61 62 6c 65 64 3d 30 0d 0a 52 54 4c 3d 30 0d 0a 4e 65 78 74 42 75 74 74 6f 6e 54 65 78 74 3d 0d 0a 43 61 6e 63 65 6c 45 6e 61 62 6c 65 64 3d 0d 0a 53 74 61 74 65 3d 30 0d 0a 0d 0a 5b 46 69 65 6c 64 20 31 5d 0d 0a 54 79 70 65 3d 62 69 74 6d 61 70 0d 0a 4c 65 66 74 3d 30 0d 0a 52 69 67 68 74 3d 31 30 39 0d 0a 54 6f 70 3d 30 0d 0a 42 6f 74 74 6f 6d 3d 31 39 33 0d 0a 46 6c 61 67 73 3d 52 45 53 49 5a 45 54 4f 46 49 54 0d 0a 54 65 78 74 3d 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6e 73 73 33 31 30 2e 74 6d 70 5c 6d 6f 64 65 72 6e 2d 77 69 7a 61 72 64 2e 62 6d 70 0d 0a 48 57	[Settings]Rect=1044NumFields=3BackEnabled=0RTL=0NextButtonText=CancelEnabled=State=0[Field 1]Type=bitmapLeft=0Right=109Top=0Bottom=193Flags=RESIZETOFITText=C:\Users\user\AppData\Local\Temp\nss310.tmp\modern-wizard.bmpHW	success or wait	1	402FE4	WriteFile
C:\Users\user\AppData\Local\Temp\nss310.tmp\modern-wizard.bmp	0	16384	42 4d fd 5b 02 00 00 00 00 00 36 00 00 00 28 00 00 00 fd 00 00 00 3a 01 00 00 01 00 18 00 00 00 00 00 00 00 00 00 12 0b 00 00 12 0b 00 00 00 00 00 00 00 00 00 00 fd	BM[6(:	success or wait	10	402FE4	WriteFile
C:\Users\user\AppData\Local\Temp\nss310.tmp\modern-header.bmp	0	16384	42 4d fd 64 00 00 00 00 00 00 36 00 00 00 28 00 00 00 fd 00 00 00 39 00 00 00 01 00 18 00 00 00 00 00 fd 64 00 00 fd 0e 00 00 fd 0e 00 00 00 00 00 00 00 00 00 00 fd	BMd6(9d	success or wait	2	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nss310.tmp\nsSCMEx.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6f 4b 66 fd 2b 2a 08 fd 2b 2a 08 fd 2b 2a 08 fd 4e 4c 0b fd 3a 2a 08 fd 4e 4c 0d fd fd 2a 08 fd fd fd de 2d 2a 08 fd 79 42 0d fd 0e 2a 08 fd 79 42 0c fd 3b 2a 08 fd 79 42 0b fd 32 2a 08 fd 4e 4c 0c fd 3d 2a 08 fd 0c fd 65 fd 2a 2a 08 fd 10 74 0d fd 2a 2a 08 fd fd 74 0d fd 2f 2a 08 fd 4e 4c 09 fd 3c 2a 08 fd 2b 2a 09 fd 04 2b 08 fd fd 43 0c fd 2a 2a 08 fd fd 43 0d fd 27 2a 08	MZ@0!L!This program cannot be run in DOS mode.$oKf+*+*+*NL:*NL*-*yB*yB;*yB2*NL=*e**t**t/*NL<*+*+C**C'*	success or wait	21	402FE4	WriteFile
C:\Users\user\AppData\Local\Temp\nss310.tmp\UserInfo.dll	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd f7 fd f7 fd f7 fd b7 fd f7 34 fd b7 fd f7 fd ef fd fd f7 08 1b fd fd f7 52 69 63 68 fd f7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd 1a 4b 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 04 00 00 00 08 00 00 00 00 00 00 fd 12 00 00 00 10 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$4RichPELK!	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nss310.tmp\System.dll	0	11264	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 29 fd fd fd 6d fd 6d fd 6d fd fd bd 6b fd 6d fd 7e b3 6e fd fd 6a fd 0e 16 fd 6c fd 39 4c fd 69 b3 52 b8 fd 6c fd 52 69 63 68 6d fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd 1a 4b 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 1e 00	MZ@!L!This program cannot be run in DOS mode.$)mmmkm~jl9ilRichmPELK!	success or wait	1	402FE4	WriteFile
C:\Users\user\AppData\Local\Temp\nss310.tmp\InstallOptions.dll	0	14848	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4c 10 70 7f 08 71 1e 2c 08 71 1e 2c 08 71 1e 2c 08 71 1f 2c 40 71 1e 2c fd 7e 43 2c 05 71 1e 2c 5c 52 2e 2c 09 71 1e 2c 5c 52 2f 2c 09 71 1e 2c fd 77 18 2c 09 71 1e 2c fd 51 1a 2c 09 71 1e 2c 52 69 63 68 08 71 1e 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 1a 4b 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 1c 00	MZ@!L!This program cannot be run in DOS mode.$Lpq,q,q,q,@q,~C,q,\R.,q,\R/,q,w,q,Q,q,Richq,PELK!	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nss310.tmp\SimpleSC.dll	0	16384	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 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 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	4	402FE4	WriteFile
unknown	727910	16290	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5251	40314B	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzer.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 57 fd 50 39 fd fd 50 39 fd fd 50 39 fd fd 36 3a fd fd 50 39 fd fd 36 3d fd fd 50 39 fd fd 36 3c fd 47 50 39 fd fd 36 3f fd fd 50 39 fd 2c fd fd fd fd 50 39 fd fd 38 3d fd fd 50 39 fd fd 38 3a fd fd 50 39 fd 03 0e 38 fd fd 50 39 fd fd 38 3c fd 27 51 39 fd 22 39 3d fd fd 50 39 fd 21 39 38 fd fd 50 39 fd fd 36 3e fd fd 50 39 fd fd 36 38 fd fd 50 39 fd fd fd 54 fd fd 50 39	MZ@h!L!This program cannot be run in DOS mode.$1WP9P9P96:P96=P96<GP96?P9,P98=P98:P98P98<'Q9"9=P9!98P96>P968P9TP9	success or wait	1367	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\SciLexer.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 00 fd 5f fd 61 fd 0c fd 61 fd 0c fd 61 fd 0c fd 19 17 0c fd 61 fd 0c fd 09 fd 0d fd 61 fd 0c fd 09 fd 0d fd 61 fd 0c fd 09 fd 0d fd 61 fd 0c fd 09 fd 0d fd 61 fd 0c 57 fd 4a 0c fd 61 fd 0c 57 fd 4f 0c fd 61 fd 0c fd 61 fd 0c fd 60 fd 0c 2b 08 fd 0d 1d 61 fd 0c 2b 08 fd 0d fd 61 fd 0c 2b 08 7b 0c fd 61 fd 0c fd 61 13 0c fd 61 fd 0c 2b 08 fd 0d fd 61 fd 0c 52 69 63 68 fd 61 fd	MZ@!L!This program cannot be run in DOS mode.$_aaaaaaaaWJaWOaa`+a+a+{aaa+aRicha	success or wait	94	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\versions.htm	0	16384	ff 3c 48 54 4d 4c 3e 20 0d 0a 3c 48 45 41 44 3e 20 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74	<HTML> <HEAD> <style type="t	success or wait	20	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\License_Agreement_ibaAnalyzer.pdf	0	16384	25 50 44 46 2d 31 2e 37 0d 0a 25 fd fd fd fd 0d 0a 31 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 54 79 70 65 2f 43 61 74 61 6c 6f 67 2f 50 61 67 65 73 20 32 20 30 20 52 2f 4c 61 6e 67 28 64 65 2d 44 45 29 20 2f 53 74 72 75 63 74 54 72 65 65 52 6f 6f 74 20 32 32 20 30 20 52 2f 4d 61 72 6b 49 6e 66 6f 3c 3c 2f 4d 61 72 6b 65 64 20 74 72 75 65 3e 3e 2f 4d 65 74 61 64 61 74 61 20 39 35 20 30 20 52 2f 56 69 65 77 65 72 50 72 65 66 65 72 65 6e 63 65 73 20 39 36 20 30 20 52 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 32 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 54 79 70 65 2f 50 61 67 65 73 2f 43 6f 75 6e 74 20 34 2f 4b 69 64 73 5b 20 33 20 30 20 52 20 31 34 20 30 20 52 20 31 36 20 30 20 52 20 31 38 20 30 20 52 5d 20 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 33 20 30 20 6f 62 6a 0d 0a 3c 3c 2f	%PDF-1.7%1 0 obj<</Type/Catalog/Pages 2 0 R/Lang(de-DE) /StructTreeRoot 22 0 R/MarkInfo<</Marked true>>/Metadata 95 0 R/ViewerPreferences 96 0 R>>endobj2 0 obj<</Type/Pages/Count 4/Kids[3 0 R 14 0 R 16 0 R 18 0 R] >>endobj3 0 obj<</	success or wait	6	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\support.htm	0	16384	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 09 09 3c 74 69 74 6c 65 3e 69 62 61 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 32 30 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2a 20 7b 0a 20 20 20 20 20 20	<!DOCTYPE html><html lang="en"> <head> <title>iba Support</title> <meta http-equi v="Content-Type" content="text/html; charset=utf-8"> <style> body { margin-top: 20px; } * {	success or wait	3	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaDataExtractor.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 5c fd 6e fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 5b fd 3c fd 3d fd 3d fd 5b fd 3c 5b 3d fd 3d fd 55 fd 3c fd 3d fd 3d fd 55 fd 3c fd 3d fd 3d fd 55 fd 3c fd 3d fd 3d fd 5b fd 3c fd 3d fd 3d fd 5b fd 3c fd 3d fd 3d fd 5b fd 3c fd 3d fd 3d fd 3d fd 3d 55 3d fd 3d 6a 54 fd 3c fd 3d fd 3d 6a 54 fd 3c fd 3d fd 3d 6a 54 fd 3c fd 3d fd 3d 6a 54 00 3d fd 3d fd 3d fd 3d 68 3d fd 3d fd	MZ@ !L!This program cannot be run in DOS mode.$\n======[<==[<[==U<==U<==U<==[<==[<==[<====U==jT<==jT<==jT<==jT====h==	success or wait	21	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaDataExtractorMC.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4f fd fd fd 0b fd fd fd 0b fd fd fd 0b fd fd fd 6e 41 fd 0c fd fd fd 6e 47 fd fd fd fd fd 59 c6 fd 1b fd fd fd 59 c1 fd 03 fd fd fd 59 c7 fd 24 fd fd fd 6e 44 fd 09 fd fd fd 6e 46 fd 04 fd fd fd 6e 43 fd 06 fd fd fd 0b fd fd fd fd fd fd fd fd 86 fd 0a fd fd fd fd 87 fd 0c fd fd fd fd 82 fd 0a fd fd fd fd fd 7d fd 0a fd fd fd 0b fd 15 fd 0a fd fd	MZ@!L!This program cannot be run in DOS mode.$OnnYYY$nnn}	success or wait	45	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\reg_dataextractorMC.bat	0	76	70 75 73 68 64 20 22 25 43 44 25 22 20 20 20 20 20 20 0d 0a 43 44 20 2f 44 20 22 25 7e 64 70 30 22 0d 0a 0d 0a 72 65 67 73 76 72 33 32 20 69 62 61 64 61 74 61 65 78 74 72 61 63 74 6f 72 4d 43 2e 64 6c 6c 0d 0a 0d 0a 70 6f 70 64	pushd "%CD%" CD /D "%~dp0"regsvr32 ibadataextractorMC.dllpopd	success or wait	1	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\reg_dataextractor.bat	0	74	70 75 73 68 64 20 22 25 43 44 25 22 20 20 20 20 20 20 0d 0a 43 44 20 2f 44 20 22 25 7e 64 70 30 22 0d 0a 0d 0a 72 65 67 73 76 72 33 32 20 69 62 61 64 61 74 61 65 78 74 72 61 63 74 6f 72 2e 64 6c 6c 0d 0a 0d 0a 70 6f 70 64	pushd "%CD%" CD /D "%~dp0"regsvr32 ibadataextractor.dllpopd	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\mkl64_parallel.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7a fd fd 74 3e b8 27 3e b8 27 3e b8 27 5b fd fd 26 32 b8 27 5b fd fd 26 2d b8 27 5b fd fd 26 fd b8 27 5b fd fd 26 3d b8 27 6c fd fd 26 23 b8 27 6c fd fd 26 2e b8 27 6c fd fd 26 36 b8 27 3e b9 27 fd b8 27 51 fd 24 27 3c b8 27 19 18 fd 27 fd b8 27 3e b8 27 7d f8 27 fd fd fd 26 3f b8 27 fd fd 47 27 3f b8 27 fd fd fd 26 3f b8	MZ@!L!This program cannot be run in DOS mode.$zt>'>'>'[&2'[&-'[&'[&='l&#'l&.'l&6'>"Q$'<"'>'}'&?'G'?'&?	success or wait	2290	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\libiomp5md.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1c fd 7d fd 58 fd 13 fd 58 fd 13 fd 58 fd 13 fd 51 fd fd fd 5b fd 13 fd 58 fd 12 fd 22 fd 13 fd 46 06 fd 5a fd 13 fd fd 0b fd 59 fd 13 fd 37 fd fd fd 7a fd 13 fd 37 fd fd fd 82 13 fd 43 1f fd fd 59 fd 13 fd 58 fd 13 fd 67 fd 13 fd 37 fd 54 fd 13 fd 37 fd 59 fd 13 fd 37 fd 59 fd 13 fd 37 fd 59 fd 13 fd 52 69 63 68 58 fd 13 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$}XXXQ[X"FZY7z7CYXg7T7Y7Y7YRichX	success or wait	72	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\msvcr100.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 70 6d fd fd 1e 3e fd fd 1e 3e fd fd 1e 3e fd fd 3e fd fd 1e 3e fd fd 1f 3e 46 fd 1e 3e fd 0b fd 3e 08 fd 1e 3e fd 0b fd 3e d6 1e 3e fd 0b fd 3e 56 1e 3e fd 0b fd 3e 44 fd 1e 3e fd 0b fd 3e fd fd 1e 3e fd 0b fd 3e fd fd 1e 3e fd 0b fd 3e fd fd 1e 3e 52 69 63 68 fd fd 1e 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 09	MZ@!L!This program cannot be run in DOS mode.$pm>>>>>>F>>>> > >>>D>>>>>>>Rich>PEd	success or wait	51	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\msvcp100.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 24 fd fd 2d 60 fd fd 7e 60 fd fd 7e 60 fd fd 7e 69 fd 34 7e 62 fd fd 7e 7b 1d 3b 7e 63 fd fd 7e 60 fd fd 7e fd fd fd 7e fd fd 3f 7e 61 fd fd 7e 7b 1d 39 7e 61 fd fd 7e 7b 1d 0c 7e 50 fd fd 7e 7b 1d 0d 7e 59 fd fd 7e 7b 1d 08 7e 65 fd fd 7e 7b 1d 3c 7e 61 fd fd 7e 7b 1d 3d 7e 61 fd fd 7e 7b 1d 3a 7e 61 fd fd 7e 52 69 63 68 60 fd fd 7e 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.$$-`~`~`~i4~b~{ ;~c~`~~?~a~{9~a~{~P~ {~Y~{~e~{<~a~{=~a~ {:~a~Rich`~	success or wait	38	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\DevExpress.Data.v16.1.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 45 6c fd 59 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 26 52 00 00 08 00 00 00 00 00 00 3e 45 52 00 00 20 00 00 00 60 52 00 00 00 00 11 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 52 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELElY!&R>ER ` R R@	success or wait	330	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\DevExpress.Printing.v16.1.Core.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 62 6c fd 59 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 62 3c 00 00 08 00 00 00 00 00 00 fd fd 3c 00 00 20 00 00 00 fd 3c 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 3c 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELblY!b<< < <@	success or wait	243	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\DevExpress.Sparkline.v16.1.Core.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 56 6c fd 59 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 12 01 00 00 08 00 00 00 00 00 00 fd 30 01 00 00 20 00 00 00 40 01 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELVlY!0 @ @	success or wait	5	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\DevExpress.Utils.v16.1.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6d 6c fd 59 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 1e fd 00 00 08 00 00 00 00 00 00 fd 3d fd 00 00 20 00 00 00 40 fd 00 00 00 00 11 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd fd 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELmlY!= @ @	success or wait	537	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraEditors.v16.1.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7c 6c fd 59 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 fd 4b 00 00 08 00 00 00 00 00 00 fd fd 4b 00 00 20 00 00 00 00 4c 00 00 00 00 11 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 4c 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL|lY!KK L @L @	success or wait	304	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraGrid.v16.1.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 6c fd 59 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 fd 2d 00 00 08 00 00 00 00 00 00 5e 08 2e 00 00 20 00 00 00 20 2e 00 00 00 00 11 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 2e 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELlY!-^. . `.@	success or wait	185	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\DevExpress.XtraPrinting.v16.1.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 6c fd 59 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 fd 0e 00 00 08 00 00 00 00 00 00 7e fd 0e 00 00 20 00 00 00 fd 0e 00 00 00 00 11 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0f 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELlY!~ @	success or wait	59	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\DotNetMagic2005.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 16 fd 23 60 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 10 00 00 60 00 00 00 00 00 00 1e fd 10 00 00 20 00 00 00 fd 10 00 00 00 00 11 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 11 00 00 10 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL#`" 0` @@	success or wait	68	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\hdClientInterfaces.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 97 fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 64 00 00 00 06 00 00 00 00 00 00 12 fd 00 00 00 20 00 00 00 fd 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL" 0d `	success or wait	2	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\hdCommon.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 59 1b fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 78 03 00 00 06 00 00 00 00 00 00 52 fd 03 00 00 20 00 00 00 fd 03 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELY" 0xR `	success or wait	14	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaUser.dll	0	14848	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6f fd fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 32 00 00 00 06 00 00 00 00 00 00 2e 51 00 00 00 20 00 00 00 60 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELo" 02.Q ` `	success or wait	1	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaUser.Forms.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 48 0c fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 02 00 00 06 00 00 00 00 00 00 fd 07 03 00 00 20 00 00 00 20 03 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 03 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELH" 0 ` `	success or wait	12	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaHdViewUtilities.dll	0	13312	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4a 29 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 2c 00 00 00 06 00 00 00 00 00 00 fd 4a 00 00 00 20 00 00 00 60 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELJ)\a" 0,J ` `	success or wait	1	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaLogger.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd 03 5d 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 02 00 00 20 00 00 00 00 00 00 5e fd 02 00 00 20 00 00 00 fd 02 00 00 00 00 11 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 03 00 00 10 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL]" 0 ^ `	success or wait	12	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ICSharpCode.SharpZipLib.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 51 09 45 fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 02 00 00 0a 00 00 00 00 00 00 06 00 03 00 00 20 00 00 00 20 03 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 03 00 00 02 00 00 23 4d 03 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELQE" 0 `#M`	success or wait	12	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaViewInterfaces.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3b 29 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 00 00 00 08 00 00 00 00 00 00 fd fd 00 00 00 20 00 00 00 fd 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL;)\a" 0 @	success or wait	3	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaViewUtilities.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 42 29 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 6c 06 00 00 08 00 00 00 00 00 00 89 06 00 00 20 00 00 00 fd 06 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 06 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELB)\a" 0l @	success or wait	26	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaPdaServerInterfaces.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3c 29 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 60 07 00 00 20 00 00 00 00 00 00 fd 72 07 00 00 20 00 00 00 fd 07 00 00 00 00 11 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 07 00 00 10 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL<)\a" 0` r  `	success or wait	31	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaExpressions.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 47 29 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 30 03 00 00 20 00 00 00 00 00 00 fd 41 03 00 00 20 00 00 00 60 03 00 00 00 00 11 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 03 00 00 10 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELG)\a" 00 A ` `	success or wait	14	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaPdaPluginInterface.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3b 29 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 10 00 00 00 20 00 00 00 00 00 00 76 2e 00 00 00 20 00 00 00 40 00 00 00 00 00 11 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 10 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL;)\a" 0 v. @ @	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\OverlayWindow.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 43 fd fd fd 22 fd 77 22 fd 77 22 fd 7e 5a 7d 75 22 fd fd fd 4a fd 35 22 fd 69 70 7d 75 22 fd fd fd 4a fd 38 22 fd fd fd 4a fd 30 22 fd fd fd 4a fd 36 22 fd fd fd 44 fd 30 22 fd 77 22 fd 48 22 fd fd 14 4b fd 30 22 fd fd 14 4b 11 76 22 fd 77 22 79 76 22 fd fd 14 4b fd 36 22 fd fd 52 69 63 68 fd 22 fd fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$C"""Z}"J"p}"J" J"J"D"""K"K""y"K"Rich"	success or wait	5	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\PowerCollections.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd 1a 5f 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 02 00 00 08 00 00 00 00 00 00 7e fd 02 00 00 20 00 00 00 fd 02 00 00 00 fd 49 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 03 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL_" 0~ I @	success or wait	12	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\View.ibaEventTable.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 67 29 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 22 07 00 00 06 00 00 00 00 00 00 2e 40 07 00 00 20 00 00 00 60 07 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 07 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELg)\a" 0".@ ` `	success or wait	29	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\View.ibaGraphManager.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4d 29 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 50 12 00 00 08 00 00 00 00 00 00 fd 6f 12 00 00 20 00 00 00 fd 12 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 12 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELM)\a" 0Po `	success or wait	74	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaHDOffline.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2d 61 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0b 00 00 38 09 00 00 06 00 00 00 00 00 00 2e 57 09 00 00 20 00 00 00 60 09 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 10 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL-ab"!8.W ` ``	success or wait	65	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaHdOfflineActiveX.ocx	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 4a fd 2b fd fd fd 2b fd fd fd 2b fd fd fd 53 0f fd fd 2b fd fd fd 79 0f fd fd 2b fd fd fd 40 fd fd fd 2b fd fd fd 40 fd fd fd 2b fd fd fd 5e fd fd fd 2b fd fd fd 5e fd fd fd 2b fd fd fd 5e fd fd fd 2b fd fd fd 2b fd fd 10 2a fd fd fd 5e fd fd fd 2b fd fd 17 5e fd fd fd 2b fd fd 17 5e fd fd fd 2b fd fd 17 5e 63 fd fd 2b fd fd fd 2b 0b fd fd 2b fd fd 17 5e fd fd fd 2b fd	MZ@ !L!This program cannot be run in DOS mode.$J+++S+y+@+@+^+^+^++*^+^+^+^c+++^+	success or wait	20	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\hdClient.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2d 61 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0b 00 00 2a 27 00 00 06 00 00 00 00 00 00 fd 49 27 00 00 20 00 00 00 60 27 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 43 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL-ab"!*'I' `' C`	success or wait	267	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\hdCore.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2d 61 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0b 00 00 52 02 00 00 06 00 00 00 00 00 00 fd 70 02 00 00 20 00 00 00 fd 02 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 05 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL-ab"!Rp `	success or wait	20	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaRunTime64.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 28 44 03 4a 6c 25 6d 19 6c 25 6d 19 6c 25 6d 19 fd fd 13 19 6d 25 6d 19 4b fd 10 19 64 25 6d 19 4b fd 00 19 fd 25 6d 19 1a fd 16 19 67 25 6d 19 6c 25 6c 19 fd 25 6d 19 4b fd 03 19 0a 25 6d 19 4b fd 17 19 6d 25 6d 19 4b fd 11 19 6d 25 6d 19 4b fd 15 19 6d 25 6d 19 52 69 63 68 6c 25 6d 19 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 fd fd fd 5b 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$(DJl%ml%ml%m m% mKd%mK%mg%ml%l% mK%mKm%mKm%mKm %mRichl%mPEd["	success or wait	91	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\de\hdClient.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2d 61 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 fd 00 00 00 06 00 00 00 00 00 00 5e fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL-ab!^ @ @	success or wait	3	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\de\ibaHDOffline.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2d 61 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 3c 00 00 00 06 00 00 00 00 00 00 3e 5b 00 00 00 20 00 00 00 60 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL-ab!<>[`@ @	success or wait	2	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\de\hdCommon.resources.dll	0	7680	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 68 fd 5a 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 16 00 00 00 06 00 00 00 00 00 00 fd 34 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELhZa!4 @@ @	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\de\ibaUser.Forms.resources.dll	0	14336	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6a fd 5a 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 30 00 00 00 08 00 00 00 00 00 00 4e 4e 00 00 00 20 00 00 00 60 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELjZa!0NN `@ @	success or wait	1	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\de\ibaUser.resources.dll	0	4608	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 69 fd 5a 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 0a 00 00 00 06 00 00 00 00 00 00 fd 28 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELiZa!(@@ @	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\de\ibaViewUtilities.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 3e 00 00 00 08 00 00 00 00 00 00 fd 5d 00 00 00 20 00 00 00 60 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!>] `@ @	success or wait	2	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\de\View.ibaEventTable.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 5e 00 00 00 06 00 00 00 00 00 00 4e 7c 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!^N| @ @	success or wait	2	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\de\View.ibaGraphManager.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 fd 00 00 00 08 00 00 00 00 00 00 6e 09 01 00 00 20 00 00 00 20 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!n @ `@	success or wait	4	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\de\ibaShared.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 74 00 00 00 08 00 00 00 00 00 00 4e fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!tN @ @	success or wait	2	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\de\ibaSharedGui.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 24 01 00 00 06 00 00 00 00 00 00 fd 42 01 00 00 20 00 00 00 60 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!$B `@ @	success or wait	5	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\de\View.ibaFFT.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 4a 01 00 00 06 00 00 00 00 00 00 2e 69 01 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!J.i @ @	success or wait	6	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\de\View.ibaOrbit.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 7a 00 00 00 06 00 00 00 00 00 00 fd fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!z @ @	success or wait	3	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\de\View.GeoView.resources.dll	0	5120	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 3f 6b 60 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 0c 00 00 00 06 00 00 00 00 00 00 fd 2b 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL?k`!+ @@ @	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\de\ibaAnalyzerViewHostViewWrapper.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 3f 6b 60 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 4a 00 00 00 08 00 00 00 00 00 00 3e 68 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL?k`!J>h @ @	success or wait	2	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\de\View.ibaAnalyzerViewHostGraphManager.resources.dll	0	5120	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 3f 6b 60 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 0a 00 00 00 06 00 00 00 00 00 00 fd 29 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL?k`!) @@ @	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\fr\hdClient.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2d 61 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 fd 00 00 00 06 00 00 00 00 00 00 1e fd 00 00 00 20 00 00 00 00 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL-ab! @ @@	success or wait	4	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\fr\ibaHDOffline.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2d 61 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 42 00 00 00 06 00 00 00 00 00 00 7e 61 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL-ab!B~a @ @	success or wait	2	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\fr\hdCommon.resources.dll	0	8192	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4d fd 5a 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 18 00 00 00 06 00 00 00 00 00 00 1e 37 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELMZa!7 @@ @	success or wait	1	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\fr\ibaUser.Forms.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4f fd 5a 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 42 00 00 00 08 00 00 00 00 00 00 2e 61 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELOZa!B.a @ @	success or wait	2	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\fr\ibaUser.resources.dll	0	4608	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4e fd 5a 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 0a 00 00 00 06 00 00 00 00 00 00 fd 28 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELNZa!(@@ @	success or wait	1	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\fr\ibaViewUtilities.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 3e 00 00 00 08 00 00 00 00 00 00 3e 5d 00 00 00 20 00 00 00 60 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!>>] `@ @	success or wait	2	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaEventTable.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 72 00 00 00 06 00 00 00 00 00 00 1e fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!r @ @	success or wait	2	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaGraphManager.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 20 01 00 00 08 00 00 00 00 00 00 6e 3e 01 00 00 20 00 00 00 40 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta! n> @@ @	success or wait	5	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\fr\ibaShared.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 76 00 00 00 08 00 00 00 00 00 00 4e fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!vN @ @	success or wait	2	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\fr\ibaSharedGui.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 4a 01 00 00 06 00 00 00 00 00 00 1e 68 01 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!Jh @ @	success or wait	6	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaFFT.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 62 01 00 00 06 00 00 00 00 00 00 fd 7f 01 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!b @ @	success or wait	6	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaOrbit.resources.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 54 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 fd 00 00 00 06 00 00 00 00 00 00 6e fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL.Ta!n @ @	success or wait	3	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\fr\View.GeoView.resources.dll	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 3f 6b 60 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 08 00 00 00 06 00 00 00 00 00 00 fd 26 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL?k`!& @@ @	success or wait	1	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\fr\ibaAnalyzerViewHostViewWrapper.resources.dll	0	13824	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 3f 6b 60 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 2c 00 00 00 08 00 00 00 00 00 00 fd 4b 00 00 00 20 00 00 00 60 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL?k`!,K `@ @	success or wait	1	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\fr\View.ibaAnalyzerViewHostGraphManager.resources.dll	0	3584	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 3f 6b 60 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 04 00 00 00 06 00 00 00 00 00 00 fd 23 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL?k`!# @@ @	success or wait	1	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHost.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 1f 61 62 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 7c 00 00 00 08 00 00 00 00 00 00 12 fd 00 00 00 20 00 00 00 fd 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab" 0| `	success or wait	3	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostViewWrapper.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 1f 61 62 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 07 00 00 08 00 00 00 00 00 00 12 fd 07 00 00 20 00 00 00 fd 07 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 08 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab" 0 `	success or wait	32	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostActiveX.ocx	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2b fd fd fd fd fd 10 fd fd 10 fd fd 19 fd 51 16 fd fd 0e fd 51 12 fd fd 04 fd fd 52 fd fd 04 fd fd 5a fd fd fd bf fd 53 fd fd fd bf fd 59 fd fd fd bf fd 75 fd fd 10 fd fd fd 5a fd fd fd bf fd 5b fd fd fd 2e fd fd 42 fd fd fd 2e fd fd 51 fd fd fd 2e fd 3d 11 fd fd 10 fd 55 11 fd fd fd 2e fd fd 51 fd fd	MZ@!L!This program cannot be run in DOS mode.$QQZ...=U.	success or wait	19	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaShared.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 4e 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 08 00 00 06 00 00 00 00 00 00 26 fd 08 00 00 20 00 00 00 fd 08 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 09 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELN\a" 0& `	success or wait	35	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaSharedGui.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 1d fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 4c 0e 00 00 06 00 00 00 00 00 00 fd 69 0e 00 00 20 00 00 00 fd 0e 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 0e 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL" 0Li `	success or wait	58	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaManagedFFT.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 13 7b 2a 60 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 72 00 00 00 06 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL{*`" 0rV `	success or wait	2	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\ibaThreadSafeNativeFFT.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 54 40 fd fd 3a 13 fd fd 3a 13 fd fd 3a 13 fd 69 13 fd fd 3a 13 fd fd 3b 12 fd fd 3a 13 fd fd fd 13 fd fd 3a 13 fd fd 3f 12 fd fd 3a 13 fd fd 3e 12 fd fd 3a 13 fd fd 39 12 fd fd 3a 13 fd fd 3b 12 fd fd 3a 13 2e fd 3b 12 fd fd 3a 13 fd fd 3b 13 fd fd 3a 13 2e fd 3f 12 fd fd 3a 13 2e fd fd 13 fd fd 3a 13 fd fd fd 13 fd fd 3a 13 2e fd 38 12 fd fd 3a 13 52 69 63 68 fd fd 3a	MZ@!L!This program cannot be run in DOS mode.$T@::::;::?:>:9 ::;:.;::;:.?:.::.8:Rich:	success or wait	9	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\GMap.NET.Core.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 01 fd fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 70 04 00 00 0a 00 00 00 00 00 00 3a fd 04 00 00 20 00 00 00 fd 04 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 04 00 00 02 00 00 fd 35 05 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL" 0p: 5@	success or wait	18	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\GMap.NET.WindowsForms.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 76 db fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 52 02 00 00 0a 00 00 00 00 00 00 36 71 02 00 00 20 00 00 00 fd 02 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 02 00 00 02 00 00 fd fd 02 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELv" 0R6q @	success or wait	10	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\System.Data.SQLite.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 15 1f fd 5e 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0b 00 00 fd 05 00 00 08 00 00 00 00 00 00 1e fd 05 00 00 20 00 00 00 fd 05 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 06 00 00 02 00 00 36 53 06 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL^! 6S@	success or wait	23	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\SQLite.Interop.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6e fd 30 4f 2a fd 5e 1c 2a fd 5e 1c 2a fd 5e 1c fd 4b fd 1c 3e fd 5e 1c fd 4b fd 1c fd fd 5e 1c fd 4b fd 1c 09 fd 5e 1c 78 fd 5b 1d 34 fd 5e 1c 78 fd 5a 1d 24 fd 5e 1c 78 fd 5d 1d 22 fd 5e 1c fd 28 fd 1c 2f fd 5e 1c 2a fd 5f 1c fd fd 5e 1c fd fd 56 1d 2b fd 5e 1c fd fd 5e 1d 2b fd 5e 1c fd fd fd 1c 2b fd 5e 1c fd fd 5c 1d 2b fd 5e 1c 52 69 63 68 2a fd 5e 1c 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$n0O*^*^*^K>^K^K^x[4^xZ$^x]"^(/^*_^V+^^+^+^\+^Rich*^	success or wait	104	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaFFT.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 4e 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 1d 00 00 06 00 00 00 00 00 00 fd fd 1d 00 00 20 00 00 00 fd 1d 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 1e 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELN\a" 0 `	success or wait	119	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaOrbit.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 4e 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 0d 00 00 06 00 00 00 00 00 00 fd 0d 00 00 20 00 00 00 fd 0d 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 0e 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELN\a" 0 `	success or wait	55	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaGraphManager.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4d 29 5c 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 50 12 00 00 08 00 00 00 00 00 00 fd 6f 12 00 00 20 00 00 00 fd 12 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 12 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELM)\a" 0Po `	success or wait	74	402FE4	WriteFile
C:\Program Files\iba\ibaAnalyzer\Plugins\View.ibaAnalyzerViewHostGraphManager.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 00 00 00 08 00 00 00 00 00 00 fd fd 00 00 00 20 00 00 00 fd 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 01 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL" 0 `	success or wait	3	402FE4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\Plugins\View.GeoView.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 1a 02 00 00 06 00 00 00 00 00 00 fd 37 02 00 00 20 00 00 00 40 02 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 02 00 00 02 00 00 00 00 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL" 07 @ `	success or wait	9	402FE4	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe	unknown	512	success or wait	2245	4031DC	ReadFile
C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe	unknown	4	success or wait	1	4031DC	ReadFile
C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe	unknown	16384	success or wait	15	4031DC	ReadFile
C:\Users\user\AppData\Local\Temp\nss30F.tmp	unknown	4	success or wait	1	402F6E	ReadFile
C:\Users\user\AppData\Local\Temp\nss30F.tmp	unknown	77407	success or wait	1	403024	ReadFile
C:\Users\user\AppData\Local\Temp\nss30F.tmp	unknown	4	success or wait	4	402F6E	ReadFile
C:\Users\user\AppData\Local\Temp\nss30F.tmp	unknown	4	success or wait	3	402F6E	ReadFile
C:\Users\user\AppData\Local\Temp\nss30F.tmp	unknown	4	success or wait	3	402F6E	ReadFile
C:\Users\user\AppData\Local\Temp\nss30F.tmp	unknown	16384	success or wait	23	402FC8	ReadFile
C:\Users\user\Desktop\ibaAnalyzerSetup_x64_v7.3.6.exe	unknown	16384	success or wait	2390	4031DC	ReadFile
C:\Users\user\AppData\Local\Temp\nss30F.tmp	unknown	4	success or wait	88	402F6E	ReadFile
C:\Users\user\AppData\Local\Temp\nss30F.tmp	unknown	16384	success or wait	7097	402FC8	ReadFile

Analysis Process: regsvr32.exe PID: **3544**, Parent PID: **7052**

General

Target ID:	14
Start time:	18:43:53
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\regsvr32.exe" /s "C:\Program Files\iba\ibaAnalyzer\ibaHDOfflineActiveX.ocx
Imagebase:	0x1290000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaHdOfflineActiveX.ocx	unknown	64	success or wait	1	1291909	ReadFile
C:\Program Files\iba\ibaAnalyzer\ibaHdOfflineActiveX.ocx	unknown	248	success or wait	1	1291942	ReadFile

Analysis Process: regsvr32.exe PID: **4904**, Parent PID: **3544**

General

Target ID:	15
Start time:	18:43:56
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	/s "C:\Program Files\iba\ibaAnalyzer\ibaHDOfflineActiveX.ocx"
Imagebase:	0x7ff73dea0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	7FFA4DD9F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4DD9F1E9	unknown
C:\Users\user\AppData\Roaming\iba	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4CBCF35D	CreateDirectoryW
C:\Users\user\AppData\Roaming\iba\ibaAnalyzer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4CBCF35D	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\regsvr32.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA4E2086ED	CreateFileW

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\Local\Microsoft\CLR_v4.0\UsageLogs\regsvr32.exe.log	0	1281	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Drawing, Version=4.	success or wait	1	7FFA4E208769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4DC6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA4DC6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA4DD412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4DC72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFA4DD412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA4DD412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFA4DD412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA4DD412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA4DD412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA4DD412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4DC6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA4DC6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4CBCB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4CBCB526	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{5C5417F9-71C1-43B1-8900-2AE7CC09158D}	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\ibaHDOfflineActiveX.DLL	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}	success or wait	1	7FF9EE5F2478	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}\Programmable	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}\InprocServer32	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}\TypeLib	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}\Version	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}\Programmable	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}\InprocServer32	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}\TypeLib	success or wait	1	7FF9EE5F2478	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}\Version	success or wait	1	7FF9EE5F2478	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{5C5417F9-71C1-43B1-8900-2AE7CC09158D}	NULL	unicode	ibaHDOfflineActiveX	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\ibaHDOfflineActiveX.DLL	AppID	unicode	{5C5417F9-71C1-43B1-8900-2AE7CC09158D}	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}	NULL	unicode	ConditionQueryWorker Class	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}\InprocServer32	NULL	unicode	C:\Program Files\iba\ibaAnalyzer\ibaHDOfflineActiveX.ocx	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}\InprocServer32	ThreadingModel	unicode	Apartment	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}\TypeLib	NULL	unicode	{C7A14696-C255-4756-8B9D-5E0AFD0C809B}	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2EE757A5-8656-4B9D-98BE-CB4FA368CFC9}\Version	NULL	unicode	1.0	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}	NULL	unicode	PseudoDatFileCore Class	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}\InprocServer32	NULL	unicode	C:\Program Files\iba\ibaAnalyzer\ibaHDOfflineActiveX.ocx	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}\InprocServer32	ThreadingModel	unicode	Apartment	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}\TypeLib	NULL	unicode	{C7A14696-C255-4756-8B9D-5E0AFD0C809B}	success or wait	1	7FF9EE5F3078	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E8EE2541-7E30-4F18-9297-7E36C67D224D}\Version	NULL	unicode	1.0	success or wait	1	7FF9EE5F3078	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5848**, Parent PID: **7052**

General

Target ID:	21
Start time:	18:44:30
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\regsvr32.exe" /s "C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostActiveX.ocx
Imagebase:	0x1290000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostActiveX.ocx	unknown	64	success or wait	1	1291909	ReadFile
C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostActiveX.ocx	unknown	248	success or wait	1	1291942	ReadFile

Analysis Process: regsvr32.exe PID: **6048**, Parent PID: **5848**

General

Target ID:	22
Start time:	18:44:31
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	/s "C:\Program Files\iba\ibaAnalyzer\ibaAnalyzerViewHostActiveX.ocx"
Imagebase:	0x7ff73dea0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4DC6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA4DC6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA4DD412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4DC72625	ReadFile

Disassembly

No disassembly