ID: 708232
Sample Name:
JabraDirectSetup.exe
Cookbook: default.jbs
Time: 07:48:52
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

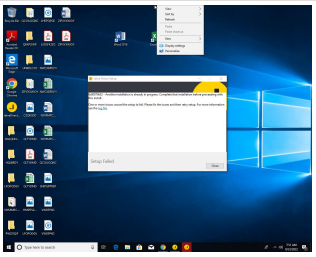
Windows Analysis Report

JabraDirectSetup.exe

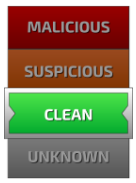
Overview

General Information

Sample Name:	JabraDirectSetup.exe
Analysis ID:	708232
MD5:	df71bfab12e144a.
SHA1:	700b1257e4bdc3..
SHA256:	98ececd8b2573b..
Infos:	



Detection



Score:	8
Range:	0 - 100
Whitelisted:	false
Confidence:	0%

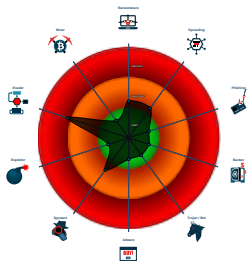
Compliance

Score:	50
Range:	0 - 100

Signatures

- Uses 32bit PE files
- Queries the volume information (nam…
- Drops PE files to the application pro…
- Contains functionality to check if a d…
- Very long cmdline option found, this…
- Deletes files inside the Windows fol…
- Uses code obfuscation techniques (…
- Found evasive API chain (date chec…
- Creates files inside the system direc…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…
- Found potential string decryption / a…

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox
Sample is looking for USB drives. Launch the sample with the USB Fake Disk cookbook
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
Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")
Sample searches for specific file, try point organization specific fake files to the analysis machine

Process Tree

- **System is w10x64**
- JabraDirectSetup.exe (PID: 2040 cmdline: "C:\Users\user\Desktop\JabraDirectSetup.exe" MD5: DF71BFAB12E144A002D85D07C0FA0FD8)
  - JabraDirectSetup.exe (PID: 1120 cmdline: "C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe" -burn.clean.room="C:\Users\user\Desktop\JabraDirectSetup.exe" -burn.filehandle.attached=572 -burn.filehandle.self=568 MD5: 6D9E7D60EE823CDB1AEA3F0C4C5B6C56)
    - JabraDirectSetup.exe (PID: 4216 cmdline: "C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe" -q -burn.elevated BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8} {D37BA658-0E76-49AC-BEF7-9E23554C8C54} 1120 MD5: 6D9E7D60EE823CDB1AEA3F0C4C5B6C56)
- JabraDirectSetup.exe (PID: 1128 cmdline: "C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" /burn.runonce MD5: 6D9E7D60EE823CDB1AEA3F0C4C5B6C56)
  - JabraDirectSetup.exe (PID: 5340 cmdline: C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" /burn.log.append "C:\Users\user\AppData\Local\Temp\Jabra_Direct_20220923074951.log MD5: 6D9E7D60EE823CDB1AEA3F0C4C5B6C56)
    - JabraDirectSetup.exe (PID: 1240 cmdline: C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" -burn.clean.room="C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" -burn.filehandle.attached=560 -burn.filehandle.self=580 /burn.log.append "C:\Users\user\AppData\Local\Temp\Jabra_Direct_20220923074951.log MD5: 6D9E7D60EE823CDB1AEA3F0C4C5B6C56)
      - JabraDirectSetup.exe (PID: 5136 cmdline: "C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" -q -burn.elevated BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D} {3D1A53A5-B618-4AC6-9F29-86FEE8B34C1A} 1240 MD5: 6D9E7D60EE823CDB1AEA3F0C4C5B6C56)
- msiexec.exe (PID: 5384 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 3960 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 094F350B1881CEA527676BAF5570DA2D MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
    - taskkill.exe (PID: 5268 cmdline: "C:\Windows\\System32\taskkill.exe" /F /IM jabra-direct.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
      - conhost.exe (PID: 5984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - svchost.exe (PID: 5268 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **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

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

Compliance

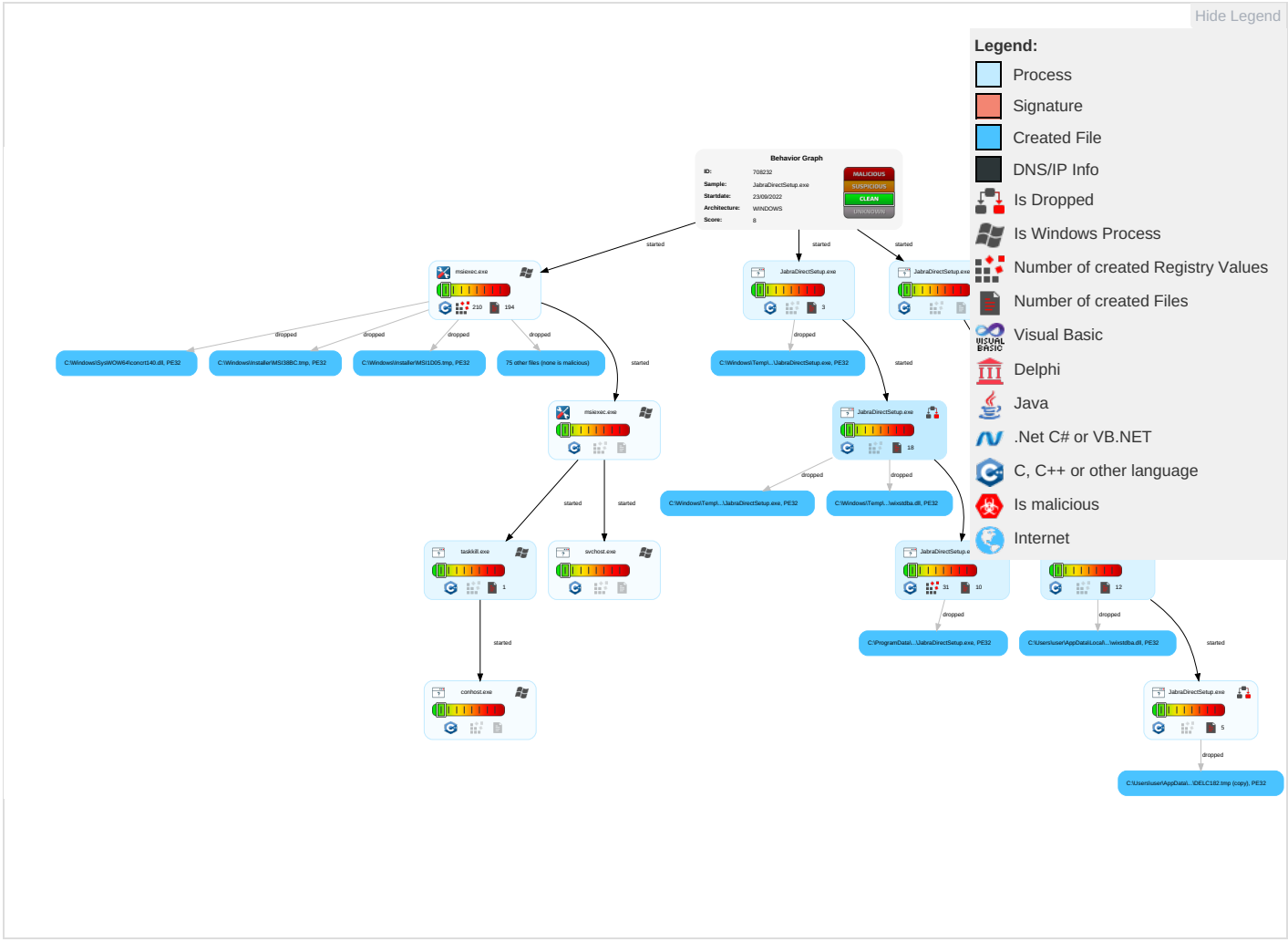
Uses 32bit PE files
Creates a software restore point
Creates license or readme file
Uses new MSVCR Dlls
PE / OLE file has a valid certificate
Contains modern PE file flags such as dynamic base (ASLR) or NX
Binary contains paths to debug symbols

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 Replication Through Removable Media	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	1 2 System Time Discovery	1 Replication Through Removable Media	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	2 Native API	1 Windows Service	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 1 Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 3 Command and Scripting Interpreter	Logon Script (Windows)	1 Windows Service	2 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	1 Service Execution	Logon Script (Mac)	1 2 Process Injection	1 Timestomp	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	3 7 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	1 Query Registry	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	3 1 Masquerading	DCSync	2 Security Software Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Virtualization/Sandbox Evasion	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 Access Token Manipulation	/etc/passwd and /etc/shadow	1 1 Process Discovery	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)	1 2 Process Injection	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

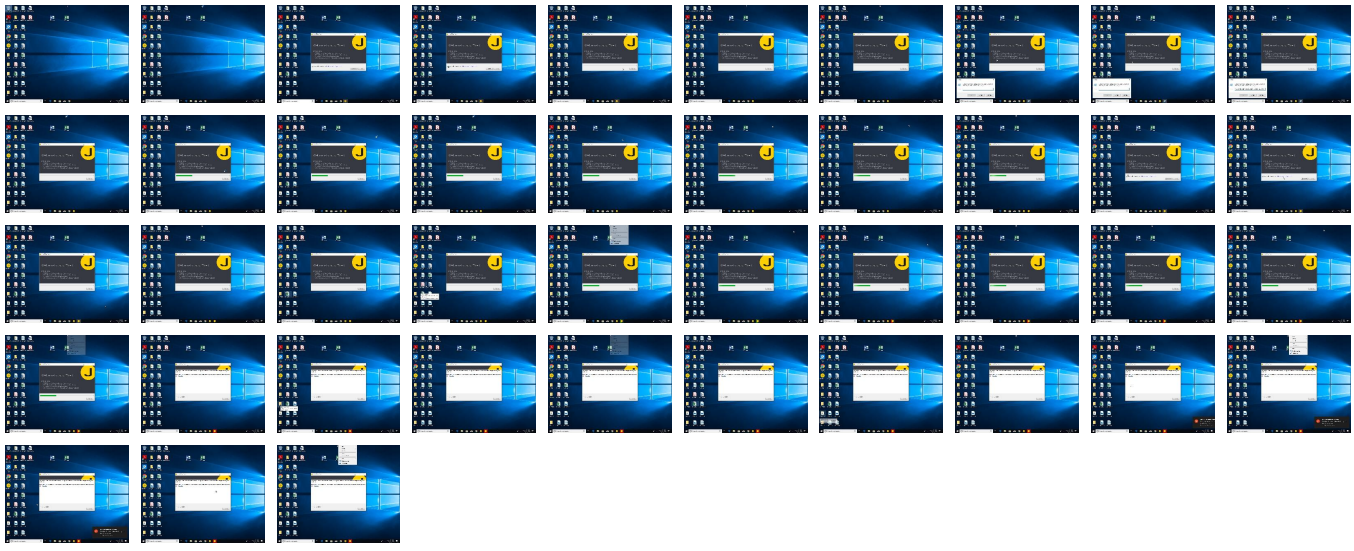
Behavior Graph

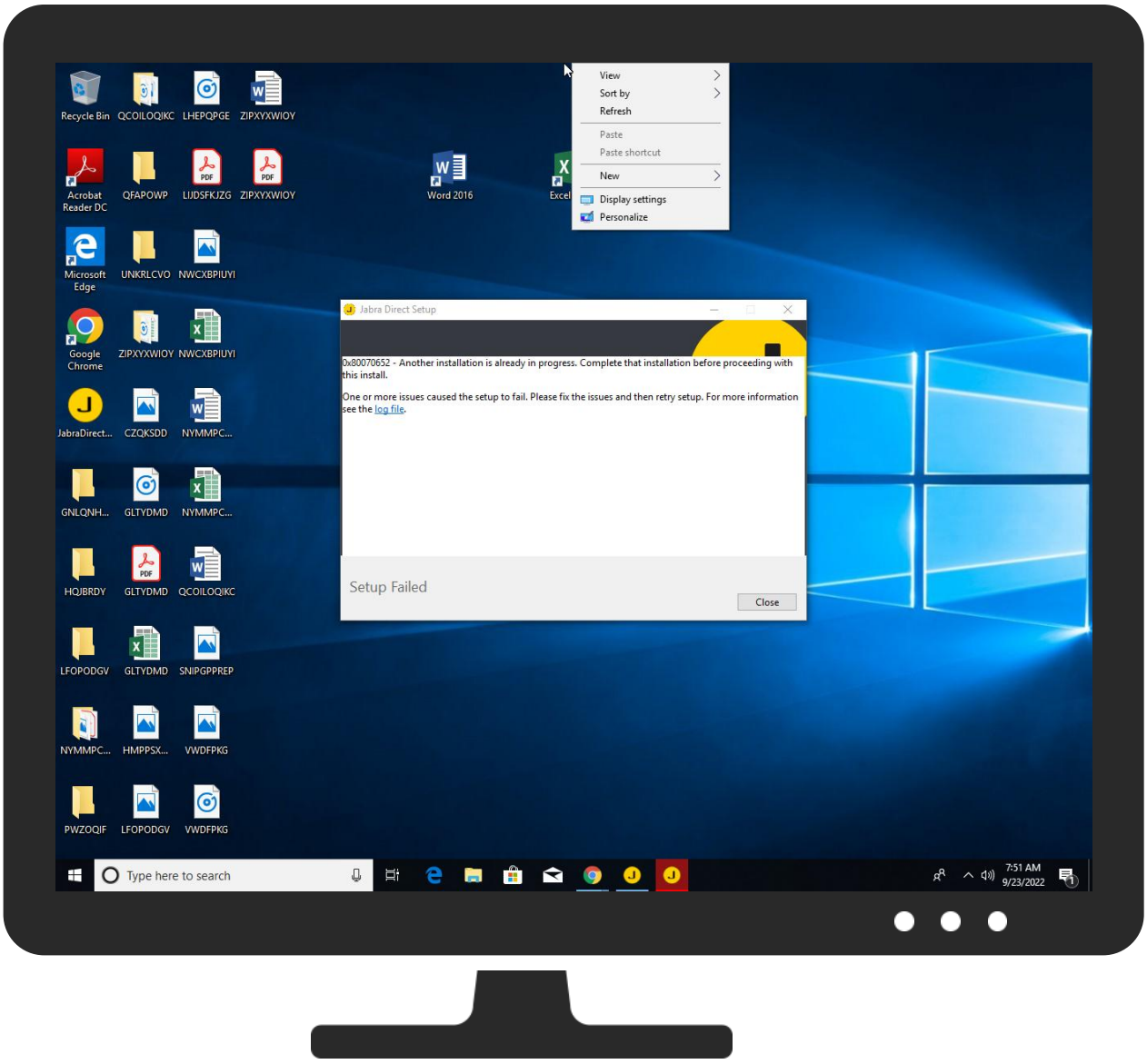


Screenshots

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
JabraDirectSetup.exe	0%	ReversingLabs		
JabraDirectSetup.exe	0%	Metadefender		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://client.device.v2.soap.uc.cisco.comm	0%	Avira URL Cloud	safe	
http://client.config.v2.soap.uc.cisco.comT	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://client.device.v2.soap.uc.cisco.coml	0%	Avira URL Cloud	safe	
http://service.system.v2.soap.uc.cisco.comTU	0%	Avira URL Cloud	safe	
http://client.system.v2.soap.uc.cisco.com9	0%	Avira URL Cloud	safe	
http://client.system.v2.soap.uc.cisco.comf	0%	Avira URL Cloud	safe	
http://client.device.v2.soap.uc.cisco.comj	0%	Avira URL Cloud	safe	
http://client.device.v2.soap.uc.cisco.como	0%	Avira URL Cloud	safe	
http://client.system.v2.soap.uc.cisco.comT	0%	Avira URL Cloud	safe	
http://service.config.v2.soap.uc.cisco.comT	0%	Avira URL Cloud	safe	
http://client.system.v2.soap.uc.cisco.comm	0%	Avira URL Cloud	safe	
http://client.system.v2.soap.uc.cisco.comn	0%	Avira URL Cloud	safe	
http://client.system.v2.soap.uc.cisco.comr	0%	Avira URL Cloud	safe	
http://client.device.v2.soap.uc.cisco.comT	0%	Avira URL Cloud	safe	
http://client.audio.v2.soap.uc.cisco.com(	0%	Avira URL Cloud	safe	
http://client.audio.v2.soap.uc.cisco.comT	0%	Avira URL Cloud	safe	
http://client.audio.v2.soap.uc.cisco.comq	0%	Avira URL Cloud	safe	
http://client.audio.v2.soap.uc.cisco.comx	0%	Avira URL Cloud	safe	
http://client.audio.v2.soap.uc.cisco.comn	0%	Avira URL Cloud	safe	
http://client.audio.v2.soap.uc.cisco.comw	0%	Avira URL Cloud	safe	
http://client.audio.v2.soap.uc.cisco.comp	0%	Avira URL Cloud	safe	
http://client.audio.v2.soap.uc.cisco.comm	0%	Avira URL Cloud	safe	
http://service.conversation.v2.soap.uc.cisco.comT	0%	Avira URL Cloud	safe	
http://autofac.org8	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://service.conversation.v2.soap.uc.cisco.com/startConversation	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.system.v2.soap.uc.cisco.comT	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.phone.v2.soap.uc.cisco.com/unsubscribe	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.system.v2.soap.uc.cisco.com/getCredentials	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.system.v2.soap.uc.cisco.com/registerClient	CiscoUCIntegration_Part.dll.8.dr	false		high
http://https://support.google.com/chrome/answer/6098869	ar.pak.8.dr, en-US.pak.8.dr, id.pak.8.dr, bg.pak.8.dr, ko.pak.8.dr, ru.pak.8.dr, fa.pak.8.dr, et.pak.8.dr, zh-TW.pak.8.dr	false		high
http://client.audio.v2.soap.uc.cisco.com/onAudioSnapshot	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.audio.v2.soap.uc.cisco.com/setCurrentOutputVolume	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.system.v2.soap.uc.cisco.comf	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://client.config.v2.soap.uc.cisco.comT	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.phone.v2.soap.uc.cisco.com/subscribe	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.conversation.v2.soap.uc.cisco.com/unsubscribe	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.conversation.v2.soap.uc.cisco.com/addMediaToConversation	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.system.v2.soap.uc.cisco.comTU	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.device.v1.soap.uc.cisco.com/setDefaultLine	CiscoUCIntegration_Part.dll.8.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://client.audio.v2.soap.uc.cisco.com/onDefaultInputVolumeUpdated_	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.system.v2.soap.uc.cisco.com9	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.phone.v2.soap.uc.cisco.com/resume	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.config.v2.soap.uc.cisco.com/onConfigDataDeletedW	CiscoUCIntegration_Part.dll.8.dr	false		high
http://wixtoolset.org	MSI3570.tmp.8.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/entry?template=Safety	et.pak.8.dr, zh-TW.pak.8.dr	false		high
http://service.audio.v2.soap.uc.cisco.com/setVoiceActivityDetectionParameters	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.phone.v2.soap.uc.cisco.com/sendDtmfTone	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.audio.v2.soap.uc.cisco.com/setRingerDevice	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.phone.v2.soap.uc.cisco.com/setDoNotDisturb	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.device.v2.soap.uc.cisco.com/setDeviceAlias	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.phone.v2.soap.uc.cisco.com/onErrorU	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.system.v2.soap.uc.cisco.com/unregisterClient	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.device.v2.soap.uc.cisco.com/onErrorT	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.system.v2.soap.uc.cisco.com/setServerAddressTypes	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.audio.v2.soap.uc.cisco.com/getDefaultInputVolume	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.conversation.v2.soap.uc.cisco.com/onRemoteMediaOffered_	CiscoUCIntegration_Part.dll.8.dr	false		high
http://config.v2.soap.uc.cisco.com/types	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.audio.v2.soap.uc.cisco.com/onCurrentInputVolumeUpdated	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.phone.v2.soap.uc.cisco.com/onPhoneParticipantUpdatedU	CiscoUCIntegration_Part.dll.8.dr	false		high
http://https://www.jabra.com/direct	JabraDirectSetup.exe, 00000011.00000002.589444911.0000000002E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://client.device.v2.soap.uc.cisco.como	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://client.device.v2.soap.uc.cisco.coml	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://client.device.v2.soap.uc.cisco.comm	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.audio.v2.soap.uc.cisco.com/setEchoCancellationParameters	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.phone.v2.soap.uc.cisco.com/completeAttendedTransfer	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.device.v2.soap.uc.cisco.comj	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	JabraDirectSetup.exe	false		high
http://client.presence.v2.soap.uc.cisco.com/onSubscriptionRequest	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.presence.v2.soap.uc.cisco.com/setPrivacyListT	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.config.v2.soap.uc.cisco.comT	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://wixtoolset.org/schemas/thmutil/2010(	JabraDirectSetup.exe, 00000001.00000002.590709679.0000000003190000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.opensource.org/licenses/cpl1.0.txt	JabraDirectSetup.exe, 00000001.00000002.577714200.0000000000DE9000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://service.audio.v2.soap.uc.cisco.com/getAutomaticGainControlParameters	CiscoUCIntegration_Part.dll.8.dr	false		high
http://device.v2.soap.uc.cisco.com/types	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.system.v2.soap.uc.cisco.comm	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.conversation.v2.soap.uc.cisco.com/merge	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.system.v2.soap.uc.cisco.comn	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/rpa00	JabraDirectSetup.exe	false		high
http://client.system.v2.soap.uc.cisco.comr	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.audio.v2.soap.uc.cisco.com/getEchoCancellationParameters	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.device.v2.soap.uc.cisco.comT	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.audio.v2.soap.uc.cisco.com/setAutomaticGainControlParameters	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.audio.v2.soap.uc.cisco.com/onDeviceUnpluggedW	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.device.v2.soap.uc.cisco.com/unsubscribe	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.conversation.v2.soap.uc.cisco.com/onCapabilitiesUpdatedk	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.conversation.v2.soap.uc.cisco.com/onParticipantChanged	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.audio.v2.soap.uc.cisco.com/getAudioOutputDevice	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.audio.v2.soap.uc.cisco.com(	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	low
http://service.device.v2.soap.uc.cisco.com/disableDeviceSelectionEvents	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.audio.v2.soap.uc.cisco.com/setOutputLowFreqRolloff	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.presence.v2.soap.uc.cisco.com/unsubscribeT	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.presence.v2.soap.uc.cisco.com/onDerivedPresenceUpdatedZ	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.config.v2.soap.uc.cisco.com/subscribe	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.presence.v2.soap.uc.cisco.com/subscribeT	CiscoUCIntegration_Part.dll.8.dr	false		high
http://www.unicode.org/copyright.html	icudtl.dat.8.dr	false		high
http://service.phone.v2.soap.uc.cisco.com/getVoicemailPilotNumber	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.presence.v2.soap.uc.cisco.com/initializeT	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.audio.v2.soap.uc.cisco.comT	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://client.conversation.v2.soap.uc.cisco.com/onConversationEnded	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.conversation.v2.soap.uc.cisco.com/onParticipantAdded	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.phone.v2.soap.uc.cisco.com/enableMobility	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.config.v2.soap.uc.cisco.com/onConfigDataCreatedW	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.conversation.v2.soap.uc.cisco.com/unmute	CiscoUCIntegration_Part.dll.8.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.jabra.com	JabraDirectSetup.exe, 00000002.00000002.580259743.0000000002D30000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000005.00000003.360875933.000000000089C000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000005.00000003.360748648.0000000000872000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000005.00000003.360935166.0000000000872000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000005.00000003.360771640.000000000089C000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000005.00000002.361457273.0000000000858000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000005.00000003.360482891.0000000002920000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000005.00000003.358928931.000000000089B000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000005.00000003.360706416.000000000089C000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000005.00000003.360148579.0000000002C9A000.00000004.00000800.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000006.00000002.579977537.0000000003570000.00000004.00000020.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000011.00000002.589444911.000000002E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://service.phone.v2.soap.uc.cisco.com/getCallStatistics	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.audio.v2.soap.uc.cisco.com/getNoiseSuppressionParameters	CiscoUCIntegration_Part.dll.8.dr	false		high
http://https://www.jabra.com/directd=am	JabraDirectSetup.exe, 00000000.00000002.581565705.0000000002CB0000.00000004.00000800.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000001.00000002.590709679.000000003190000.00000004.00000800.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000002.00000002.581734533.00000000030E0000.00000004.00000800.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000006.00000002.580218071.0000000003750000.00000004.00000800.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000007.00000002.592749628.0000000003A90000.00000004.00000800.00020000.00000000.sdmp, JabraDirectSetup.exe, 00000011.00000002.590934046.00000000033A0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://client.audio.v2.soap.uc.cisco.comw	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://client.audio.v2.soap.uc.cisco.com/onInputDeviceRemovedX	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.audio.v2.soap.uc.cisco.comx	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://client.audio.v2.soap.uc.cisco.comn	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://client.audio.v2.soap.uc.cisco.comq	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://client.conversation.v2.soap.uc.cisco.com/onParticipantRemovedg	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.audio.v2.soap.uc.cisco.com/onDevicePluggedInT	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.audio.v2.soap.uc.cisco.comp	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.presence.v2.soap.uc.cisco.com/setPresenceT	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.phone.v2.soap.uc.cisco.com/onCapabilitiesUpdated	CiscoUCIntegration_Part.dll.8.dr	false		high
http://service.device.v2.soap.uc.cisco.com/setPhoneMode	CiscoUCIntegration_Part.dll.8.dr	false		high
http://system.v2.soap.uc.cisco.com/types	CiscoUCIntegration_Part.dll.8.dr	false		high
http://autofac.org8	Autofac.dll0.8.dr	false	• Avira URL Cloud: safe	unknown
http://client.system.v2.soap.uc.cisco.com/onSystemSnapshotY	CiscoUCIntegration_Part.dll.8.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://service.system.v2.soap.uc.cisco.com/setLogLevel	CiscoUCIntegration_Part.dll.8.dr	false		high
http://client.audio.v2.soap.uc.cisco.comm	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown
http://service.conversation.v2.soap.uc.cisco.comT	CiscoUCIntegration_Part.dll.8.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708232
Start date and time:	2022-09-23 07:48:52 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JabraDirectSetup.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean8.evad.winEXE@18/177@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 45.1% (good quality ratio 43.4%) • Quality average: 79.3% • Quality standard deviation: 26.4%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, audiodg.exe, consent.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Created / dropped Files have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing 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 NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: JabraDirectSetup.exe

Simulations

Behavior and APIs

Time	Type	Description
07:50:02	Autostart	Run: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce {50c3bcea-1203-4bf1-9103-09af1bf52966} "C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" /burn.runonce
07:52:00	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Jabra Direct "C:\Program Files (x86)\Jabra\Direct4\jabra-direct.exe" /minimized

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

3cf367.rbf (copy)

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	243576
Entropy (8bit):	6.627118640957731
Encrypted:	false
SSDEEP:	6144:dmvyl/LAZ/A2ZQDI2NxEcr4NTm8lr/Vx778yBZONRQ7Spuv612z/N5N+JGle:eJ46Bx77DcPuv3zsJGle
MD5:	E4EA46EBA9B7CD64636DF7F775802DA0
SHA1:	D6E828D0CE02843188075DB24B14E0F54836E2B6
SHA-256:	05DA55A844DA2B03E714E1E44C0F7A2A99694947E2499108C402B2B1BC8D96F2
SHA-512:	B67726DE6174DD258475798706D8BF8C662D77EB9FAA4AF6E24D7C0F0C28620C07B7B00D076659031E4C4AD3F5D1398C4AFEAD51318A00F243E69F72B3E95F5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V.3...]X..]X..]X..\Y..]X...X..]X@.\Y..]X..\X..]X@.YY..]X@.^Y..]X@.XYA.]X@.]Y..]X@..X..]X@._Y..]XRich..]X.....PE..L.....`......"!.....x.....0.....k.....@A.....K..<r.....x#.....+...;..8.....<..@.....p..8.....text..... ..`.data....4...0...2... .....@....idata..~....p.....R.....@..@.rsrc.....d.....@..@.reloc...+.....,...h.....@..B.....

C:\Program Files (x86)\Jabra\Direct4\AvayaIPIntegration\AvayaIPIntegration_Part.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	91136

Entropy (8bit):	6.881833050432033
Encrypted:	false
SSDEEP:	1536:mzUaaofRwmk3WI0Sbf7PnzIJSB1HPZQIXA9TP6gvveH28g6NPSJvg+I/yz4AJlty:mzUaaofRwmk370SL7zHXXAxfTSm4DSl8
MD5:	1E48BB914D33C3DCE915F9715A9942E2
SHA1:	9D709E8AFB35EF34F77FAD1306944EED2A9F93A6
SHA-256:	912B902603E0087BACCFB1A5E8FC1F2836C4C49FF420A6B9A4147D906704B925
SHA-512:	58D98546A896237FE307683EDBC6162099DB1F2781F9D6EEC35424E20BC3024A2BF9E426BE446D566084EF00D8824812DC3DCE82656EFE0AB1AF6DA1FB4CA69 2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....I.T.....!.....Z..`.....fx... .....@.. ..... .....x..W..... ..... ..H.....text...lX... ...Z..... ..`.reloc.....\.....@..B.rsrc..... .....^.....@..@.....Hx.....H.....0...G.....a.....0.....~....}.....(.....}.....(....}.....s....}.....s.....s.....s.....s.....s... .....s....s....}..... .]w.(b....o ...(!...("....*.....#.`...8.....{.... .]w.(b...oH.....}.....(....*.0..T.....{.....,..{....o#....{.... .]w.(b...oH....{.....o/..... .]w.(b....o ...(!...("....*.....66..8....0..... A]w.(b....{...... 2]w.(b...+. 9]w.(b....{.....($...

C:\Program Files (x86)\Jabra\Direct4\AvayaIPIntegration\AvayaIP_InterfaceApi.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	49664
Entropy (8bit):	6.0051504458333405
Encrypted:	false
SSDEEP:	1536:KnbsCBU6TuC5EcankDo/bqSQ5OZ+nuTVH7:6bDU+5Ec5o/b6OZxTVH
MD5:	4C61A11B1174770F77B6ED080AD7A389
SHA1:	E154D13BE400020681AF6BB9FB900A6B537E3AC3
SHA-256:	60A2F2FC28E6D64C9CA16FC5DA848EFF360CE2D111599631CA41B9D6E02513F7
SHA-512:	C445A5A8619FDBB737B871D41E2D5BCD055A711BE3B9904AE59AB185DB0E5FDB891ECAC1CE1F310A3F66ABC29D5816F6814093D7074ADB64D714E511FCA2F 24
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....X..6...6...6.....6..q....6.....6..q....6..q....6.....6...7...6..q....6..q.. ..6..q....6.Rich..6.....PE..L....I.T.....!.....B...|.....O.....`.....@.....$.....a.....8g.. @.....`..t.....a..H.....text....@.....B..... ..`.rdata...l...`...n...F.....@..@.data.....@....rsrc...$.....@..@.reloc..... .....@..B.....

C:\Program Files (x86)\Jabra\Direct4\AvayaOneXIntegration\AvayaOneXIntegration_Part.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	102912
Entropy (8bit):	6.534659099561742
Encrypted:	false
SSDEEP:	1536:4DyUJsiYQpNwpWYof7PnzIJSB1HPZQIXA9TP6gvveH28g6N1:iNI07zHXXAxfTS1
MD5:	1B90ECDA321B84BC19C73E75D180423A
SHA1:	A818C75EAE6752A6145F1E2C6F34ED816B06455E
SHA-256:	37E09714C00960932D352B094EA61B658DA23428C7F1A8A1A94C5F7819A09B40
SHA-512:	47837C7389FD50C21486B7245DC4CDDD86975864E91032FF0A7681066F8CFCD4EEE310CDDAB626A54871D5DD3D87292139C464528F4AFA8DEDD17D718B4378
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....t.`....." ..0..... ..... ..... ..@.....O.....D.....I..... ..... ..H.....text..... ..... ..`.rsrc...D.....@..@.reloc..... .....@..B.....H.....W..X.....D...(.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*....0..C..... (.....~....}.....r...pr_..p(....s....(.....r...p('....("...(!...*..(.....o.....,*..(.....r...p('...*...0..'.....{.....o.....r...p.o....(....(.....*.....0..'.....{.....o.....r...p.o....(....(.....*.....{.. ..*"..}....*B(...o!...o"...*..*..*.~..

C:\Program Files (x86)\Jabra\Direct4\AvayaOneXV3Integration\Autofac.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	190976
Entropy (8bit):	6.011014830652571
Encrypted:	false
SSDEEP:	3072:Ug5OK8PAVhSWTiIg/PHqD6Ug7Hiz44Wrbge7ILsf4qzTZ78srAnqdzYR4:UvehS5cWrVaYvp8srAqdzY
MD5:	67E05AE28D1017FBA80C237CE715BD3A

SHA1:	0EF18AEE4FD25144E8B754D2E907D81A8269061E
SHA-256:	8AAEC6C836BFE934799E1F28588E6426BE5D5158EBCFD4B9E0A17B5293764F46
SHA-512:	EB4ACD675A998AD6DF5469F880AB222DFFB0CEE526F43EE7851D45E6C6CBACB01F83E822D651110A7BCCF944E1A5883A846ADFF21E6659D28B8EFFDFF8442 2A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....6.O.....!.....>.... .. ....@.. .....`.....d.. ..@.....O.... .....@.....h..... ..... ..H.....text...D.... ..... .. .`.rsrc..... .....@..@.rel oc.....@.....@..B..... .....H.....D...$.....8..P .....J...D?._.h.XB$..`...q..".Jv$`f.o.sV?.n..;S6..p."1i6..[{..y...UN..\.....vh..jbzy...$..c ?t.T.2_.....d....e.=....l..i....<....(....*.0.."....{?.....{@.....o....*...0.....sR.....}@....{@...u!.....,..o....F...(....(/...-.(...+*.o....o.....o.....~.....o....}?.....o.....S...s ...(...+(...+*..*.(k...*..(....*..(....*..{#....{$...{%....{&...oD.....*....0..2...

C:\Program Files (x86)\Jabra\Direct4\AvayaOneXV3Integration\AvayaOneXV3Integration_Part.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	96768
Entropy (8bit):	5.6072246012901745
Encrypted:	false
SSDEEP:	1536:ac1Q9P4ZUBfjAJWlNMy61BPhvLA5lXO59scydZG0cdc9lu+6B48Yzu:a1J4ZUblYdjGE59sPfQ5
MD5:	37018B063B50F3323ACA973CBB093DE0
SHA1:	0E0A91C8142A1F94D5BC5F718C1670BD9E122F68
SHA-256:	23CB0007932BFD990F4C5C7265E2F7B36C85402BE4B9762DDEF736D15959ABC3
SHA-512:	C8EB43E706E746C736B93C51CC0819083BA99511C4AD631AE2B8883F9E9E718B4DA60D92A328E8F165EA253880B128AEEE43ECF8C9347C892D6B14A0A164FF9 A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o..`....." ..0..p..... ..... ..... ..@.....O.....P..... ..... ..H.....text...4o... ...p..... ..`.rsrc...P.....r.....@..@.relo c.....x.....@..B.....H.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*...0..V.....r.. .p.....%..(.....%..(.....%..(.....%..(.....%..(.....%..(.....E....(....*..(....*..{....*..{....*2.{....o....*..0..s.....s.....~....}.....(.....s....o.....{....(....-...{.....{....o.....Yo ...}.....{.....r.. .p.o!...("....."*.....]]..... 0..*.....s.....}...

C:\Program Files (x86)\Jabra\Direct4\BroadSoftIntegration\BroadSoftIntegration_Part.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	72704
Entropy (8bit):	5.404997646896727
Encrypted:	false
SSDEEP:	1536:kYb7NB9aQZMMVDamJGjRW6sQY/2hPUUWRWNPyD:kYb7NBA32amwRm/
MD5:	157520B9A4BF4753EDB6F762E0BB17B0
SHA1:	5868432D53B6215A49ACDF91025C3CB6406101F9
SHA-256:	968FE0EEE8F2169DD06B4312B67B6E9675A770987DEF525A9E71E499422EF7BC
SHA-512:	5257D7C2AC966EC8A0F9B6AD9458CFDC40F76BA2BAF8533F0E2BEE6A0A1E097D084E092EB0DFB06EC4F430E7782D2A4B008CC7A589CC1C456A107A8508FD3 0E0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....9^....." ..0.....1... ...@..... ....@.....1..O....@..D.....`.....\0..... ..... ..H.....text..... ..... .. .`.rsrc...D....@.....@..@.rel oc.....`.....@..B.....1.....H.....i.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*...0..V.....r. ..p.....%..(.....%..(.....%..(.....%..(.....%..(.....K....(....*..(....*..{....*..{....*2.{....o....*..0..|.....s.....~....}h....(.....s....o.....{h...(....-...{h.....{h...o.....Yo ...}h....{h...%- .&~.....r...p.o!...("....."*.....ff.....0..*.....s...

C:\Program Files (x86)\Jabra\Direct4\CiscoIPCommunicatorIntegration\CiscoIPCommunicator_Part.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	19968
Entropy (8bit):	5.780180647115956
Encrypted:	false
SSDEEP:	384:+BjKfZzhfP/fBPNRbYDMoryrOyuex8DdtSV66I:nB1R0Sb0SVzI
MD5:	D9B0A1A592F24FCE832FDB1F723E91F9
SHA1:	BE7007D71E830F4CFDA7F9D024115724D9ED0CA3
SHA-256:	4D7146AB173726B0988821CAAE3E9A675E5C411ACD1EFD4C1AD45D60C8BA775F
SHA-512:	92151734B38F2D7F0013E6C22106B811254267DFAFF3BE698AAAF54B57533392413DF30E18930E6F87F811E7712C6DDBDBBD1F5234348AEB614F477D434D9B0F

Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R$.U.....!.....D...J.....c... .....@.. ....b..W.....H..... ....H.....text....C... ...D..... ..`.reloc.....F.....@..B.rsr c...H.....H.....@..@.....b.....H.....>...#.....|;..T.....0..a..... B.r..... 1t..X....s.....s.....Y...o..... >d%...Y..Yfefefeffe />T ...a..affeeffefefea....,...o....+....,... .T...Y..Xfeffeefefa...,..o....+....8...(....3#.. Xw....X..Y.Xa...~....`.....8.....-'.... ...a..Xfefefeffea...~....`.....+_.o.....(....o.....~....`..... X..X ..aa..+*~.....`..... .@...Y..Yfefeffeefef.Ya....~....X.....*....0..... .....i.8x.....b%. ...

C:\Program Files (x86)\Jabra\Direct4\CiscoJabberIntegration\CiscoJabberIntegration_Part.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	21504
Entropy (8bit):	5.9307434600748685
Encrypted:	false
SSDEEP:	384:i1NEWJlf+wLZA0i+Y0uwRrvmaZrWy/XW845t/VwgH:INEgYRnAlM/VwgH
MD5:	2E85DC954382E97A852AF3A72DD755B9
SHA1:	82CC69BD002D84AC4CEB829F9848BA0D5DF3CC30
SHA-256:	513A82C81CC960CCB0022ED4DE495D6EBCA13C1679C6117B92C29589379A8A46
SHA-512:	F57F04886E4FA1B94A8F2E3027C531D3216ACF9D1A2836CC49356E1DC218B1F9C0EF20581DB6771FC204634469571736D43F2E4BD1B9DF16870B1CC867396802
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....U.....!.....J...P....."i... .....@.. ....h..W..... ....H.....text...(I... ...J..... ..`.reloc.....L.....@..B.rsrc..... .....N.....@..@.....i.....H.....D...$.....8=.....0..c..... .6..... ....X....s.....s.....Y...o..... .C6..Y..Yfefeffeef .%~...X..afeffe effeefa...,...o....+....,... J7b>..a..Xfefeffefefea...,..o....+.....=...(....3#.... m...X..a.Xa...~....`....8.....-'.. .....Y..Yffeeffefea...~....`.....+_.o.....(....o.....~....`..... [...a..aa..+ *~.....`..... .i..X..Yffeefefeffe.Ya..~.....X.....*..0..... .....i.8x.....b%. ...

C:\Program Files (x86)\Jabra\Direct4\CiscoUCIntegration\CiscoUCIntegration_Part.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	392704
Entropy (8bit):	6.1246015784497985
Encrypted:	false
SSDEEP:	3072:9lxS5IA2IYFMGsVXEccg3MMbdmEDBgqcp7BYNQN/ry8yedgP3yviX7sf+pV0nJWv:g5IKNPcmdmEDBgqcfT4ec3yvw7sdJ8
MD5:	B0A4A6AB14B8E4EACDA52B411D7D4FF0
SHA1:	BEC8E714435B51C0AC11D31925BDDFCEA010C516
SHA-256:	B28FB39C3BE9A076E4F7D5D7D2337188A8AA9DE72129B8C9A45C129998426AA2
SHA-512:	729C5EAA62FE8473F22183E848E478A75B54356E4F4E5B58847E3C2DEBC026718BEBA16C2732EEB867D165567362A5DC93A723274D54C791927F16D685145691
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...nJ.T.....!..... ... .@.. .....`..... .....t...W....@..D..... ..... ..... ..H.....text..... ..... ..`.reloc..... .....@..B.rsr c...D....@.....@..@.....H.....:.....x..$_.....((...*.s.....*.~....*.''..}....*....0..9.....{....,0.{.....{....oj..... h\..(.....o)...(*...(+..... *.....C...*...*...*...*...*...*...*...*...*...*...*...*...*...*...*....((.....}.....}.....}....*....{...*..{...*..{....*''..}....*....{....*''..}....*....0..F..... wX..(.....Y.....{.....{.....#.....{.... .$.....{.....(,...*...0.._.....~~...}.....(.....}....

C:\Program Files (x86)\Jabra\Direct4\CiscoWebExConnectIntegration\CiscoWebExConnectIntegration_Part.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	86016
Entropy (8bit):	6.908531011766634
Encrypted:	false
SSDEEP:	1536:+VTr6LtFf7PnzIJSB1HPZQIXA9TP6gvveH28g6NpLAiKPvXws5t+72czy0SKD:+VTr6Lth7zHXXAxfTSp9KPvXws5t+zyc
MD5:	906F5C83859D20FCF38910D8ABEBFF83
SHA1:	0F69AA284E7D140BA45CF4136F51A73511C11059
SHA-256:	1C4C1079E891E19B90B8A576C4A4D5235A562675084B6F9246D8D76546BA5AE7
SHA-512:	E59079A0C4537F853AE490805AD64EA3490DCCC9FF27CA6AFC376608BC8DAFF93763D73666DAA0F40F7F830A0ABFF67D7A38E888E882B9084DBC51F7739D7C 6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J.T.....!....F...L.....d.. .....@.. ....4d..W..... ....H.....text....D... ...F..... ..`.reloc.....H.....@..B.rsrc..... .....J.....@..@.....pd.....H.....$...@.....W.....V.(.....(.....(....*....{...*''..}....*....{...*''..}....*.... ..sC(N....(.....(.....(....*...0..M.....(.... ..}.....s...}.....s.....s...}.....s.....s...}....*...s.....*.~....*..0..a.....}.....-V.{...o....{....,C.{...o....,6..}.....{....o....{.....o....{.....o....{....o...*....0..L.....}.....,A.(.....,o.. ..,1..o....{....,"..o...*..(.....,..o....,..o.

C:\Program Files (x86)\Jabra\Direct4\CiscoWebExConnectIntegration\GNDeviceInterface.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	97792
Entropy (8bit):	6.346077105798904
Encrypted:	false
SSDEEP:	1536:us/cxHaYqit+6hklnAHYOFoQKKYsvqF1ETFzm81W1wIbCMH5ZOZKexIK:usRYqQRkleYcoQKKYsSFsFlW1wlbTH5e
MD5:	AB4941F936ED58F8FF1FD398BAD4F5C1
SHA1:	939DF0AB35349BF91805765F3AB5086A2138BB21
SHA-256:	4B7AA3AC680CD4CE9F924ADF1ABA34E241A62B3F5E579DFE18349BC36410ED3A
SHA-512:	35DC5D3C5445DE278D02C184F55653F72D31EAC5963A3F82E2024BFC903DF75D31B01912FCFC1A1E139F933EAB2444CCE814CB0E9686FE4C535DA0B91A54FA9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....X.J...$...$...$.....$..C....$.....$..C....$..C....$...y...$.....$...%.t.$..C....$..C....$....$..C....$.Rich..$.....PE..L....6.T.....!.....)....@.....X|.....`.....X..... .....@.....H.....text..... ..`.rdata.....@..@.data.....p.....@....rsrc...`.....r.....@..@.reloc..... ....x.....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\CounterpathBriaIntegration\CounterpathBriaIntegration_Part.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	145408
Entropy (8bit):	6.438271041574778
Encrypted:	false
SSDEEP:	3072:oHqqtTZSXl8jS6cdVGNHzcYhvgL7zHXXAxfTSK:oSTlKivQjULS
MD5:	F6468A96A971F2456EF68D2C0B3D27EB
SHA1:	406CAE69C95383FCB99192126F94A3DA2557F5AF
SHA-256:	F5C42BFE2CF7912E3A2B304BC26BF49356F196C446901D1FB67C0BE10AB29518
SHA-512:	1357350FB83D633CC75712C505EC58A8C8D1C92042273135877187AB907101B53F05C4FFBD5649AD73E391280E25514157844BBA1A54A33982082E8CE268785D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Q\.....!..0.....vM... ...`..... ..... ..@.....$M..O...`.....K..... ....H.....text...|-... ....`.rsrc.....`.....0.....@..@.rel oc.....6.....@..B.....XM.....H.....t.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.* ....0..R.....(.....~....}....(P.....(.....(&....(%.....(.....r...p.(....(....s....($...*..-..(#....o....,*..($....rs..p(....*.r...p.(....(....(.....rf..p(....*.r...p.(....(.....(.....rl..p(....*N..(.....rk..p(....*n.{....,.. {.....s!...o"...*.0..G.....,...s#.....{....,1.{.....

C:\Program Files (x86)\Jabra\Direct4\FWU\BluecorePsKeyApi.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	56832
Entropy (8bit):	6.035560378582815
Encrypted:	false
SSDEEP:	768:XCVI1ld6KmugiX/oVz3LyF/lP6CoveNPz5lyQN0dp:N1UqX/oBydPjovmPzPOp
MD5:	1818F334FA49A2AA43496FBA2DA336DF
SHA1:	4455032081AC25F568FDBB7D5D13C0D05F15F4A7
SHA-256:	D93A2315AA65F2DD6AFDB3385807BCC5611FC0766D4D8FD81DAA766EF57BADCC
SHA-512:	87C15CBB0CA0B9CA55E7F10FAFDB5526E97504C9A3309011F396FBE88852365FA8B4436570A0F302799AFF96F24955D22A63AA3BA9652362DC9A9BA2C2B31701
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K`.....yj.....]t.....j.....Sj.....]t.....]t.....]t.....(.....&...Zt... ...Zt.....n.....Zt.....Rich.....PE..L.....`.....!.....=.....@.....@.....d...x.....(.....A..T..... ....B..@.....@.....A..H.....text....-..... ..`.rdata.....@.....2.....@..@.data.....@....rsrc...(.....@..@.reloc..... .....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\FWU\DeviceInfo.xml

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators

Category:	dropped
Size (bytes):	148684
Entropy (8bit):	5.207366738730948
Encrypted:	false
SSDEEP:	768:OMjMGMXzmzVzizSzvzqz6zpzjzczEzszYz7zEzhzvzlzGzEzHMHMlMqMhM+MSMpx:17i
MD5:	5D76AE415D07D6BB230B4109133251FE
SHA1:	193F0E4659A12A8FB07D6D53860DA069291CD915
SHA-256:	933FF1742C1AA4AC89EDC3855553D4764BC775F69FAAAF9BF93A9B4E69013D8A
SHA-512:	CD509CAAFEA9382159AB538A486FFD47C38B53F8AAB4F5A2FC53EE7FDF9D15826B7AE512E061B8F9C80461B85C232F49A57730CE15A3DA11F02CD73D82D4FD31
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<JabraDeviceFirmwareUpdateInfo Version="1.3.50462" platform="Windows" minFWUAppVersion="1.12">.. <device name="AudioCodes HRS 457 UC" usbVendorId="0x0B0E" usbProductId="0x2480" usbDfuVendorId="0x0B0E" usbDfuProductId="0x0984">.. <primaryGnpAddress>8</primaryGnpAddress>.. <fwUpdateProtocolId>1</fwUpdateProtocolId>.. <fwUpdateModeCommandType>gnp_event</fwUpdateModeCommandType>.. <requiresLanguagePackRegion>False</requiresLanguagePackRegion>.. <requiresLanguageSelection>False</requiresLanguageSelection>.. <hasGnpAddress2>False</hasGnpAddress2>.. <hasDockableHeadset>False</hasDockableHeadset>.. <isSelfPowered>False</isSelfPowered>.. <mustBePowerCycledAfterFwUpdate>False</mustBePowerCycledAfterFwUpdate>.. </device>.. <device name="AudioCodes HRS 457 MS" usbVendorId="0x0B0E" usbProductId="0x2481" usbDfuVendorId="0x0B0E" usbDfuProductId="0x0984">.. <primaryGnpAddress>8</primaryGnpAddress>.. <fwUpdateProtocolId>1</f

C:\Program Files (x86)\Jabra\Direct4\FWU\DfuEngine.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	341504
Entropy (8bit):	5.81359535572336
Encrypted:	false
SSDEEP:	6144:7+Az6xVQ1t18y4DtpGXQtCC0MNpn8F29qwWUKOQA3Mb3+OZQY0V:7+Az6xaKy4ReQIC39qweA3qY
MD5:	818485F015AB3D14923E930323F5481B
SHA1:	2AA316A97B8D018470F4FA9343AEBADEB804BAA8
SHA-256:	8E853B2D19BC156DB28F5FC185AFE35D6C8630FD3D4A5B8AE3AF10975D0EC71D
SHA-512:	AF335A433359A82C5B9D862C8FAFDF2B4B19D05CF7BB220A4DFF51E3AFD54618FEE94F9B6214C6AD4EF33F31BF18F478755B49F4710A6B73AB252D9878572D17
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M.z%...v...v...v..v...v.>.v...v..v...v.>.v...v..v...v...v...v.>.v...v.>. vB..v.>.v...v.>.v...v.>.v...vRich...v.....PE..L.....^.....!.....*..... .....s.....R...<.....p*..... .....K..@..... ..@.....text..... ..`.rdata..... .....@..@.data...T!.....@....rsrc.....@..@.reloc.....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\FWU\DfuEngineWrapper.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	71680
Entropy (8bit):	6.093396482057674
Encrypted:	false
SSDEEP:	768:CneMrXTzi4RSFRolYNtg5M9PiKsuN7SXnkNAGb5Vh6oVS76fEIlyQlqWkAuEmg:CeMri/RoCbg5wPVV/PSqEzWTm
MD5:	C24D6B5107085A6D360DDBC1333FE3F2
SHA1:	95E4F719A8C071B0A39E7BF16A1A535F76A3232B
SHA-256:	AF8E73B79ED550594301880A628A63881F0C6829A30A700122AE438FCA707B43
SHA-512:	FD1202A64796418EC9936269DA6FEAF777DB770229E0B5BBA9BB3BA8738FBA23A6FD5F6B04AA23402C4649C2CA93A1359EBC2A8237CBEBF0F154624F8B81BBC3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I.;.'.;.'.;.'.2...?.'.i.&.9.'.T.&.8.'.%...9.'.i."..-.'.i.#.1.'.i.$.:.'. L..9.';. &.~.'...".?.'.....:.';..:'...%.:.'.Rich;.'.....PE..L....e.`.....!.....:.....I.....P.....P.....@.....0..8.....@.....R..p..... .....S..@.....P.,.....PR..H.....text....9.....`..... ..`.rdata.....P.....>.....@..@.data...T.... .....@....rsrc...8....0.....@.. @.reloc.....@.....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\FWU\FwVersionConstraints.xml

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	9811

Entropy (8bit):	4.8628239195360745
Encrypted:	false
SSDEEP:	96:ijdbbnGvw0YUw07qmw078qhmOqEzfmGAxgPwgTmgT/ItAxgPwgTmgT/jAxgPwgTa:PvSUh0qQOqEqlIiIclO
MD5:	53794CC00E5D004910532FF44628B70D
SHA1:	F2AD86A7B459559368A8A2DED0D58207410374EB
SHA-256:	3477FB5D50EDAC14923C6EBF8122B992731594F8E4699FBAD4466509E904D2C9
SHA-512:	18A0FBFB6D6C2D9DE6D91C621C98E6EE7124E753BFDCFF316C4D63CD765E01B41A69B3515AE1BD5C914D5ED9A983E438BFA168D2C24BDC0A6DDEC666000CB249
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.. ========== -->.. This XML file is used by Jabra Updater Agent to determine which firmware -->.. version ranges a device can accept. -->.. -->.. Given this input: -->.. USB Vendor ID -->.. USB Product ID -->.. Product ID (variant), optional -->.. Hardware ID (read from device, 0 if not available) -->.. Configuration ID (read from device, 0 if not specified) -->.. -->.. The output is:

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.CommandLineParser.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	44544
Entropy (8bit):	5.761335027669499
Encrypted:	false
SSDEEP:	768:DpsQQJSsrOPRfN9ykYGzF2/XHGlcxidjdululltlIlRPrGjGAOG2zCM4BHT9fzU:DMJByPH9yk3FDcxidjgo3SjrkGAVMyT+
MD5:	3E51A6737E26DBD38FAD8EB87BD984B7
SHA1:	ACCA16FD2D1FB52B2947F8C5629AFC19A8ED21E8
SHA-256:	54580513F0F04E7DB77F37D6589471D68D0EB44472025C395F87196F3F393614
SHA-512:	A42C4E7C273FA03CB5240D1B2ED5B99965206DE849F26483DD6E9B1F82991F54F77AFDCAA978E0B98222E293B6FBC9D89354A20B938982488B04560C88289993
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`......" ..0.....n.... ..... ..... ..... ..`.....O.....4...T..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....N.....H.....lJ...v.....(...*V.(.....}.....}....*..{....*..{....*6..s.....*.0.....*"..o....*..(....*J..u.....o ...* N..u.....o!...*...0.....*"..o ...*..("...*"..(#...*.0.:.....{$...o%....+...(&...o.....('..-.....o.....o(...*.....%.....*6.{$....o)...*r.....(*....o+...u.....*....0..=.....(,...%u.... ..,...(-...t.....&r...p.o....r=..p(/...s....z.*.....

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.BluecorePsKeyApi.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.4148097970420075
Encrypted:	false
SSDEEP:	96:umKlvzZJlDTuGreizuYtlc/c0cctIg+ct6c9y:2LfTuGrei6Yte/cvcKg+coc
MD5:	C094EE4D593778373EF17212B7E2D4B8
SHA1:	3168B280015B9F527164DB71976FBF6E8E24F2B5
SHA-256:	696FB26DE1749E0877642D354015DB572401F3FA454701121173E4206DC6931B
SHA-512:	C14009B689ABDDEE5EE0DB5DB300CE434CA7363AC61884691F0B1832F40FC3171A2FC0451859788F48ACB397ADFF76AAEB81B61E5871EF0D33ABD154FFE9558A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....V.....!..0.....Z&.. ...@..... ....`.....&..O....@.....`.....%..T..... ....H.....text...`.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....9&.....H.....P .....BSJB.....v4.0.30319.....l...D...#~.....#Strings.....#US.....#GUI D.....#Blob.....3.....l.....*.....>....[.....'.....)....1....9....A....I....Q....Y.....a.....'.... F...#.O...+.a...3.n...;.....C.....K.....S.....[.....G.....H.

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.Conexant.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	20992
Entropy (8bit):	5.5452272480277385
Encrypted:	false
SSDEEP:	384:AJ7MVDfjDMNWLS5ORRo4l11X9zdxmslYFegqiS:AJAdfjSWO54Y1XHx9
MD5:	D78D1CD0CFB11DBCAAE1559A3C3F58FC

SHA1:	CC1667FE2CFEF906F426F34D8950CA5FA4189015
SHA-256:	6D2932BE926858C70F51259A223FEE69DCABD0D99CA01B7ED39BB6A5882B3080
SHA-512:	544A7B9121746A6CF4F44B9D771F22A08F58372ACE49C8F52E5FA0DAF51F4EBEAA7E2E4EBBBFA62662879D621688DB4CB257CA87615C97C9E6DF22B9BDCF4C 63
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....!..0..H.....g... ....`.....g..O.....f..T..... ..... ..H.....text....G... ...H..... ..`.rsrc.....J.....@..@.rel oc.....P.....@..B.....g.....H.....6.../.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.**....(... .*..(.....-.r...ps....z.-.r...ps....z..}.....}.....}.....(...*..0..A.....(.....-.r...ps....z.-.r...ps....z..}.....o....o....}.....(...*B...(.....}....*~.{.....3..(....-...}.....{....*..{....*"..}....*..{....*"..}....*..{....*"..}.. ..*..{....*"..}....*..{....*"..}....*..{....*..0..

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.CphAdvance.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41472
Entropy (8bit):	5.408487705464132
Encrypted:	false
SSDEEP:	768:6GztGm/E81t+hXUXXGXHk9aVU77CyAEcolq9GPuM+1Ups6JV:tJ9TP9vfCyAEcy8GZsU
MD5:	F22F7B99F77823445602DFAFD838E425
SHA1:	C98A3B01E7E5CD92F595025D2B74B99E74496572
SHA-256:	917C3A69ACE7B97D2B976E7276C49918FC09657687776AFE23FCB67F0EFD54E9
SHA-512:	2E2D3B6E452728C48F926610053E5D2AA0962116142AC814326D2F4942450D5DED405DFAF9989C1597AEFAA9F72FA821A55242076AA53032F5E4545E9E701413
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...S_}.....!..0..... ....`.....\_...O.....\...T..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....S...b.....0..).....{?.....(....t.....|?....(...+...3.*....0..).....{?.....(....t.....|?.....(...+...3.**....(... .*.0..W.....s....}.....s....}.....(.....-.r...ps....z.-.r...ps....z..}.....o....o....}$....(....*..0..T.....s....}.....s....}.....(.....-.r...ps....z.-.r...ps....z..}.....}.....}.....(....*.0.....{....3..(....-...}.....{.... 9.....{....,..{.....3-..{.....o....&.{.....3...

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.Csr.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	16896
Entropy (8bit):	5.166115080434496
Encrypted:	false
SSDEEP:	384:wBjuLZLLouZWA333xVyW2t0yPr1IOzRKzWDJnhW:eSZd333PyW2aypR8zW9nI
MD5:	CBD6BA4654E8C09CA10DBF0FE3186C00
SHA1:	E8300B7E34D33B9C4642A5835BDA327EC2DFCDE2
SHA-256:	B00368716E7E6F49A2CA33533925DF77562FF9BAC36AEC345C1E73D170F32C76
SHA-512:	98C7CEE9928E513CBA30F1653381A570256EF550EFE345ED8F1FCA2BE054997D4D10703A5A056CBC0E82BE9104D27F43B2ADCEBECFF3CE3A65C0404E1DD35 0C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....@.....!..0..8.....W... ..`..... ..... ..`.....W..O....`.....V..T..... ..... ..H.....text....7... ...8..... ..`.rsrc.....`.....:.....@..@.rel oc.....@.....@..B.....W.....H.....D0..H&.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3. **....(....*.0..A.....(.....-.r...ps....z.-.r...ps....z..}.....o....o....}.....(....*..(.....-.r...ps....z.-.r...ps....z..}.....}.....}.....(....*~.{.....3..(....-...}.....{....*..{....*"..}....*..{....*"..}....*..{....*...0..n..... ..}.....{.....39.{....,T.{....o.....&...s....(...+,6..(..

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.CsrOta.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	29696
Entropy (8bit):	5.417514604294173
Encrypted:	false
SSDEEP:	768:F5JNIGMSzGKmo+iFndQq8DzX/ppuFVTrQtr56RUtVC6LeOMdxd:jJkifF+jDzSaCK6r
MD5:	1A800819A3F517A61DEDCBCC002B24C2
SHA1:	0E35557EC8BA9E293E2C9CE03E09E48D2DD3D081
SHA-256:	E0D510DD88D9E521007A43B917DE5D7FD656E7DAA38771D17B8CCFE33698EC35
SHA-512:	783CF10FE9EE1F5205CD3E449101B4DE849FA8A6EFCB6D681F6470DCCDF966E07D75EF786A582A01F09C9E7A87C73DB8CFF4745BF688BCD331C4D577A84C5 A1

Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....!..0..j..... ....`.....O.....T..... ..... ..H.....text....h... ...j..... ..`.rsrc.....l.....@..@.reloc..... .....r.....@..B.....H.....>...A.....0..!.....c ....j_i...b~.....a.a....n_*....0.....j...i.X.0..... ....%...%...%.....o.....i.+0..1... ..Y.n ....j_(.....Y.n ....j_(.....Y...0.. ....j_..b. ....n_..c`..*n .....2...%.;...(.....*.0..).....{/.....(....t.....|/.....(...+...3.*....0..).....{/.....(....t.....|/.....(...+...3.*....0.....(.....%- .&r...ps....z}.....%-.&r...ps....z}.....}.....o....

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.CsrUsbOta.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	29184
Entropy (8bit):	5.4060557021184525
Encrypted:	false
SSDEEP:	768:9DNSBswliwK6gM0cMmZeUjg2OFVzcPphD/frQtp5oRUtEMBvfOMdhw:D4OFVl9s9y
MD5:	CDC0F7EC8AF467028D86234CE0B30C98
SHA1:	B332CD08FB77B73065802AEF0364C42A9B9E47C0
SHA-256:	FF7E83E39B953FEDAFCE1CDAC465E9F3EF2289B9F72A804C9BCD066988D81C05
SHA-512:	B8AF089AC833B98DB7198F44A6F1A527FAE2A2F57FFCFB2B907472DD64F09DD91F186E31C9B0F6DEEF818BD19FF94708A40590BDF7E5EE6B03C4B50967A553(6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....!..0..h..... ....`.....~..O.....}..T..... ..... ..H.....text....g... ...h..... ..`.rsrc.....j.....@..@.reloc..... .....p.....@..B.....~.....H.....p=..P@.....0..!.....c ....j_i...b~.....a.a....n_*....0.....j...i.X./..... ....%...%...%.....o.... ..i.+0..1.....Y.n ....j_(.....Y.n ....j_(.....Y...0.. ....j_..b. ....n_..c`..*n .....1...%.9...(.....*.0..).....{-.....(....t.....|-.....(...+...3.*....0..).....{-.....(....t.....|-.....(...+...3.*....0..... (.....-.r...ps....z.-.r...ps....z..}.....}.....}.....}.....

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.DeviceAdapter.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	18944
Entropy (8bit):	5.401014609454434
Encrypted:	false
SSDEEP:	384:zYbKLArTjgf+8R905Jyukt9sqhY+PWsitv5iCa7CinoZQKSk:zYb3rgG8Ry5WsqtAMC/JP
MD5:	8CBFDADB36E90C752580727C49771586
SHA1:	9B10EBF9C56C237A413F845F54ABEA3DE983F3A5
SHA-256:	5B94D96C75EC3A5730C5C67BA2696E0ED4CD10953B90A727A0A0088EFCA6E199
SHA-512:	B24DC98F484F5A2C64B29FCF5E8982F00CF11816CE13F9128C1B645B48B0177299D4D41D0239543CAE37E81B63CA8FE58C792197A05862B8EB6D6A961146F045
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...r.....!..0..@.....2_... ...`..... ..... ..`.....^..O....`.....].T..... ..... ..H.....text...8?... ...@..... ..`.rsrc.....`.....B.....@..@.rel oc.....H.....@..B.....H.....1..X,.....{....*"..}....*..{....*"..}....*..{....*..{....*..{....*..{....*..{....*..{....*..{....*..{....*..{....*..{....*.. {....*"..}....*..{....*..{....*..{....*..{....*..{....*..{....*..{....*..{....*..{....*..0.....(.....s....(.....(....o....}.....(....o....}.....(....o....}.....(....o....}.....(....o....}.....(....o....}.....}.....(....o....}.....(....,:.(....s....(.....(..... .0...s....o.....(....(....}....*...0..

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.DfuEngine.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.2472428389641945
Encrypted:	false
SSDEEP:	48:6cvqF4xlbWLE4JMwYX1rxUl2HotXs7ihpDl94P1w:5TxloqI57i934
MD5:	BB1CB24BC2D1A1162051A9FB4767D5EC
SHA1:	D464563D4C26AE114CDE24A3FA4EF47BECF0FC72
SHA-256:	DFF802D1F4B73EE46A0AE68C989AE9BF994ED8435FAF50CE5236197EFEC15ADB
SHA-512:	F5706ECF95F682DEE8881319E87801FDD800811BED549856BE60FA7D5DF56EE53E501AD131ACAF8EE5A9724828E28F661A5642E49FF8FA8C447D5FA03A99641
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..:.....!..0.....&... ...@..... ..... .`.....%..O....@..p.....`.....$..T..... ....H.....text..... ....`.rsrc...p....@.....@..@.relo c.....`.....@..B.....%.....H.....P ..x.....BSJB.....v4.0.30319.....l...4...#~.....#Strings.....#US.....#GUID .....#Blob.....3.....W.....9.....?..... .....j.....S.....).....1.....9.....A.....I.....Q.....Y.....'.....F.. .#.O...+.a...3.n...;.....C.....K.....S.....

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.Factories.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	5.04767547407641
Encrypted:	false
SSDEEP:	96:FQuZmJTiTcGOU8ZNBMZKQ/kUtjqv5RQXDUuaRhcWgfXd6zpaKx80FX+Ldr4wa:FQuZy9GX6DK7XAuaYfdGwVeOLdr4wa
MD5:	F50650FFA657CCAD791A36FD0FADD4B0
SHA1:	60F64B1766D3AC4BD9C5761931BDB14A45D51AB3
SHA-256:	66DC7DD70ACA30B422DFCB462E5E86AB4AA2AB44A19CDC04F11A7BF946F69163
SHA-512:	AFAA17D7EAFD15FDAA90D236B66AA964D188727FB80AE2663D6162D06A0A302D9AB7FD625BDC2105FDFC486BE889B51E5DE6A7214EF9594880BF32E8ED7BF872
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....\|:.....!..0.....=... ...@..... ....`.....q=..O....@.....`.....t<..T..... ....H.....text..... ....`.rsrc.....@..... .....@..@.rel oc.....`.....&.....@..B.....=.....H.....&.....0.....-.r...ps....z.-.r...ps....z..o.....YE.....%...%...%...%...8 .....s.....8.....o....o.....(....8.....s.....o.....o.....o.....o.....,...@....o....o.....(....9.....o....o....o....(....9.....o....o....~....%-.&~.....s....%.....(...+,o.o....o....~....%-.&~.....s.... %.....(...+,>.o .....s!....+...s"....+$..s#....+...s$....+...s%....+.s&...z....r

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.MassStorage.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	4.899926023323808
Encrypted:	false
SSDEEP:	192:8hU70R7j22nQLGuNxwLeVj39uVMupOQosQ5Xq:8hSg7C2cT4L+zYVMupOHQ
MD5:	C9807A7C6DAF03732363BE760EB303E3
SHA1:	F8FF5FCDF7014798F745E1ECF482CD6A8319C57F
SHA-256:	1651F9F60B33DA7C6F58572D47B7F5AD60634DD4F9D73715805614E43717851A
SHA-512:	9531FC70BC66715F21799D80D5BEB6804EE10D906FBB9F42D8258E196F96A30CFAB1C7AFFA1D55BD5B8861E0B7D1AD62D079E86E399C0CF7345944FB6418A456
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....\" ..0.....=... ...@..... ....`.....=..O....@.....`.....<..T..... ....H.....text..... ....`.rsrc.....@..... .....@..@.rel oc.....`.....&.....@..B.....=.....H.....%.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3. *....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*..{....*..{....*\"..}....*:.(.....}....*....0..".....(....(.....~....(.....(...*.*...0.....(.....(.....(.....(...,..(... .....s.....o.....s.....j.....+@.

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.MxUvc.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	17920
Entropy (8bit):	5.2099989599079874
Encrypted:	false
SSDEEP:	192:ebdrt3dVVUckTfbP+9E5Va7KM6YnJFd3sFM8VFiholglFzSkgEKGFlazmzAU5OUi:aNXYXenHt2MyFi2lglFzSkggX3Vj
MD5:	BC614688F10C9BDE314BB0EA69947687
SHA1:	7104DF08B78E997C9A4385FB5685A737C7980CF6
SHA-256:	52E8ACBA9808FDF3CB4229D541EA90CF4EE51F2BF13EC0CFBB11AF7C79F67171
SHA-512:	BF0CA4DCE07BC92BD41CFC343A86D57D04890499501FA6F637045F0F67DBA547F13FBC0F3F10A42508AA9D1C9AD612DD996B0ACAB1F790106F4F826E32BBB388
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.....!..0..<.....Z... ...`..... ..... .`.....>Z..O....`.....DY..T..... ..... ..H.....text....:... ...<..... ..`.rsrc.....`.....>.....@..@.relo c.....D.....@..B.....rZ.....H.....-..H+.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*..{....*\". .}....*..{....*\"..}....*..{....*\"..}....*..{....*\"..}....*..{....*\"..}....*..{....*\"..}....*r.(.....(....(.....,.(....*.*..{....*\"..}....*..{....*\"..}....*..*.*..*..{....*\"..}....*..*.*..{....*\"..}....*~.{.....3..(....-...}.....{....*....0..a..... (.....%-.&r...ps....z}.....%-.&r...ps....

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.QualcommHid.dll

Process:	C:\Windows\System32\msiexec.exe

File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	19968
Entropy (8bit):	5.269212664509271
Encrypted:	false
SSDEEP:	384:LgS7Nn92HVR4qwDQthJsz8c0Bt32ELjoi4:LgS/21Rbz3dv4
MD5:	06933A19BF98EC71DF2CDBC1C61633C6
SHA1:	FD39E6FB7CD829DA51B2644FA5D286827430756A
SHA-256:	802D6D5A2B0E1CF187D2B387C0DA013146709269CD50E78AF2B0C28DBB6BA2C3
SHA-512:	89B1F80800EA1E4ADD7FDB697E550A227DB3B02F54DCCEFF34F7723B3409F65FEEBA16D92498AE7BBA3D497C9911DE8BFFC04979B421247AD49974E39566871 6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....!..0..D.....b... ....`.....fb..O.....da..T..... ..... ..H.....text....B... ...D..... ..`.rsrc.....F.....@..@.relo c.....L.....@..B.....b.....H..... ..}/...*..{0...*"..}0...*r.(.....(....(.....,..(....*.*..{1...*"..}1...*..{2...*"..}2...*..*..*..{3...*"..}3...*..*..*...0..).....{4.....(....t.....|4.....(...+...3.*....0..).....{4.....(....t.....|4.....(...+...3.*.. ..0.....(.....%-.&r...ps....z}....%-.&r...ps....z...o....o...

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.Sitel.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	63488
Entropy (8bit):	5.506722184044913
Encrypted:	false
SSDEEP:	1536:fGTn7dx2GG/vIKxWsCPr3n2mrxmVO+Jo:+Q/vMxUwVxJo
MD5:	7ACB5A8BBE402320E760593995CACB9D
SHA1:	E47CE2F1762C27CC5AC1760752928ECE92CD5464
SHA-256:	276AA876A9A193FEBCD30BA12408713F60656640B1D50F7371934C669160E419
SHA-512:	92576E86E051D3D7B5AA0C994F062BDED34D82963A3DE7DC98EEBA31B371CD80ED5A7283A26BCDBA9B234A96B4BC0D24EB252459BA36DA27AFD4BCD8ADF9 72FA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{.....!..0..... ... .`..... ..`.....O.... .....@.....T..... ....H.....text..... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....x.....".(....*....0.....o.....4...%..5.o.....-.*.....(....,r...ps....z.....(....- .....(....,re..ps....zr...p....4...(....s....z. ....(.....o.....4...%..i.o.....rb..ps....z*.0..!..... .'.....o.....4...%..j..o....*"..(....*..o....~....%-.&~.....s....%.....(...+*...0.....s.....o.. ..o.....8.....o.....o.....(....,".o .....(....,..o!.....(....-

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FirmwareUpdate.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	18944
Entropy (8bit):	5.245052639891975
Encrypted:	false
SSDEEP:	384:JjI+qJRn61dbLc+FW7s10KowXKmjtbS7:lI+MRsKs105wXKmjtbq
MD5:	1EAF2BC09FC01F94B7CA444A5A025CEC
SHA1:	AC02E54302E7DAB0F249485A399E50874B30E156
SHA-256:	5DFB55A40925E2A7F0008D20AB12C63D1B5038317DD45F712188B1CE3F8059BF
SHA-512:	9EF80CB2F59AC97DAEAEB0FE459AF224FC0877ADF4C89092D80C9620FF9709D34CD2937ED9B1101A31E8C94ABC5EE0E563CA52CAFC2F8F0A595D994ECD6A8 048
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...O.....!..0..@.....^... ...`..... ..... ..`.....]..O....`.....\..T..... ..... ..H.....text....>... ...@..... ..`.rsrc.....`.....B.....@..@.rel oc.....H.....@..B.....]....H.....($...8.....0.....(.....,.....(.....&..*.....0..H.....(....,?.(.....+....(.....X....i2..(. .....+.... ....(.....X....i2.*..{....*"..}....*..{....*"..}....*..(....*..(....*...0.....r...p..&.....&...(.....r9..p(.....~....~.....(Q.....(.....3..*...8.....(...+}\....~.....(T.....^.....(...+}X. .....~....X}`..... .....(V.....{a...

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.FwBuildVectorReader.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	30720

Entropy (8bit):	5.495832207010457
Encrypted:	false
SSDEEP:	384:TpcmV0iK/ptT/F0/KB/Fbl9Ydlz+4405EvtPCKoOLpWrgugHWQABkqwj0p09MTZe:TpX09/bl9Y2vPCPOh2Q2xwjoDSdpyyX
MD5:	D0875BA0C376536CC6F19A1D9DA0AB90
SHA1:	ED7745AF6BE2F114E0F9CE05783953D4C900B188
SHA-256:	4321C1E1270151DB806C52E16392BBA9EBCD3236E1681DA44E73C9A240A443FC
SHA-512:	E277B1218F3060EE586E0A6F3AC8A2B5C493C9C379D6C41D007F8F9EC4FB04DA87E814E47EFDAA03971A62C4D0E049EBDAA03486C6EAB7053865CD81B952074C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...I}....." ..0..n.....6.... ....`.....O.....T..... ..... ..H.....text...<l... ...n..... ..`.rsrc.....p.....@..@.reloc..... .....v.....@..B.....H.....>...L.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..(....~]...%-.&~\.....s....%.]...(...+*..(....~^...%-.&~\.....s....%.^...(...+*..(.....s....(.....s....(.....sl...(.....~....(....*6.(.....(...+*..0..%.....s.....}_....(.....s....(...+

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.GnProtocol.UsbHid.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	13824
Entropy (8bit):	5.148057644575424
Encrypted:	false
SSDEEP:	384:GRze5zQghyDc1c/t5gpsDFDwf5d4nRAJ2CV3aFq+V2E/uMN+VXQ:wzqzNqbxW4nRAJ9aFbj/97
MD5:	8257B567887B4DE030B1A8F7F1D56C8B
SHA1:	14B1FFCBA2B9A124AA646CC1E1C9702CFC970A91
SHA-256:	B89AD4B0911A9060452E6BC2DC783E9E9788A87A40166C9191BEECAF6398CCDC
SHA-512:	673DD376B07C533615F86DF46D063E2521313BCBA68218B94EB160E1996D1A5115308B196F294E7FA270C68EAC2A9B9E46859192606A61274F2FB57460C07A3C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....." ..0..,.....J... ...`..... .....[.. ..`.....I..O....`..<.....H..T..... ..... ..H.....text... *... ...,..... ..`.rsrc...<....`.....@..@.reloc..... .....4.....@..B.....I.....H.....+..T.....TH.....0..m.....o.....&.....,M..s.....r...p(.....r...p(.....(....r3..pr7..po....(....o.....,..o..... ...,..o.....*....(.....;V.....`b.....0..b.....o.....(.....o.....o.....o.....o.....o.....b`....o.....o....,..o.....o.....(....*...0..).....{.....(...t.....|.....(...+...3.*....0..).....{..... ("...t.....|.....(...+...3.*....0..).....{.....

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.GnProtocol.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	5.114313213647495
Encrypted:	false
SSDEEP:	192:in567rLtfId0EX1AAB7L+y+huD6y7mNnsJc5S4Osj/a7NF2O0QmgOu/6:d7/oDCuWy7asJc5S4Osj/a7fl0QmgO1
MD5:	CBF2ECB3CC7E8C2590F0DD142E6037F5
SHA1:	FDDE4DC6D0B49C13DE9A85D86FE65E00FA61E990
SHA-256:	CB9C0FC6E39ED4DC1376A0E90892DE702998B302D8C0802F3130FB6B1A85322C
SHA-512:	869FF7A005092DAA2FE7C78D7C94E91737B9E343E365A145452599FC18D2AC0F06C8BF5CBA9FA45F41ADD2CCC00EC31959C2C5880050F045F7894BAF034F84B7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....+t....." ..0.....B=... ...@..... .....l... ..`.....<..O....@.....`.....<..T..... ....H.....text...H.... ....`.rsrc.....@..... .....@..@.rel oc.....`.....&.....@..B.....#=.....H.....%..|.....;.....0.....s.....o.....o.....%...%...o.....s.....o.....o.....%...%...o.. .....s.....o.....o.....o.....s.....o.....o.....%...o.....s.....o.....o.....%...o.....s.....o.....o.....%...o.....s.....o.....o.....%...o.....s.....o.....o.....%...o.....*...0..d..... ~.....,Y..i.1S.,.....+.....+....,...X...X....i2...1-...i.Y0%.....,...X.....

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.ModelBase.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	4.847945261493644
Encrypted:	false
SSDEEP:	192:8GIRwdXXUgKHFw5sMVZQLS3UJG/CMUvvrx:WRw5XU7lw5sMVtU8KM2
MD5:	430F5BAF6506E6A15B45D3F21B3A1BD0

SHA1:	C83D9F2DCF082CBE172E8B4B5BA031289560703B
SHA-256:	46C668098F9D18E62E8710C44E01E7C5637AE3B9553CB17F70222A02C36DDACD
SHA-512:	172CF14B8C366AF97124331E6B77BF50319D4C6889A0F6708864B4B803A3119C2019BFFADA2C71CAB9D79167731F32DC58D4C98961F53B98AD8306BA51960D71
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rk......" ..0.. .....&>... ...@..... .....*.. ..`.....=..O....@.....`.....<..T..... ....H.....text...,.... ... .`.rsrc.....@....."..... @..@.rel oc.....`.....(.....@..B.....>.....H.....%..|.....p<.....{....*..{....*V.(.....}.....}....*Z.....(.....(.....*....0..D.....s+.....}.....,...s....(....%- !r...p.{.....o....(....s....z*.0..8.....s.....}.....(.....s....(....u.....(...+*.0..%.....s/.....}.....0...s....(....(...+*....0..8.....s.....}.....(.....s....(....u.....(...+*.0..%. .....s3.....}.....4...s....(....(...+*6.(.....(...+*..(....*V....

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.PanaCast.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	12800
Entropy (8bit):	5.151444169850381
Encrypted:	false
SSDEEP:	192:RwTbAMO7QMlxYaCs+mpbivj5SkS5jCi82f2uQxMx9BctpS6PXpI:+WmY2i7DOjj8s2rMx9BcjNPy
MD5:	80B0B0D2003DB5253C41550C2F487144
SHA1:	DDC4BA679870B6E75FBE02E8D8010C9201B503A7
SHA-256:	31E1CB285BA762E4890FA8DD74C5311C0BDAB1D839D15CA141BF838E2B835C9E
SHA-512:	D6E5ACE5123B0F9EDE967D4C88BBD226A4C80D09C24D9218E89B160FFD9EB319FCDFC27768194D5EDAD7F7D1DE6716780775F949670C5D138E01CA7B110F94 6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....!..0..(.....G... ...`..... ..... ..`.....G..O....`..|.....F..T..... ..... ..H.....text....'... ...(..... ..`.rsrc...|....`.....*.....@..@.reloc..... .....0.....@..B.....G.....H.....(.....b.r...p..*....(....(....*....0..%.....(....s@.....s....%.....s....o....*....0..A.....~.....(....~....-.s.. .....~.....X.....~.....,..(.....*.....-5.....0..@.....~.....(....~.....Y.....~....-.~....o.....,..(.....*.....-5.....0..9.....~.....(....~....%-.&+.(.....,..(.....*.....&..... (....*.s.....*..{....*.0..).....{.....(

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.UsbDeviceInformation.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	25088
Entropy (8bit):	5.377092609572361
Encrypted:	false
SSDEEP:	768:rxCJEEp1xn0aUXXam8pnAUh7QBEKHE6KC:FCJRzl0a2XaNh7QvHE6KC
MD5:	FB6C6A101DDEBA7F8AEAED0625775026
SHA1:	A0860EB00F4E898A18A80989F21F0BB17CEA8205
SHA-256:	DE18186EADABC6C821CC27AEDF621E80E2787081091A5CDF9021EE6E7BF9D4D9
SHA-512:	1A4074CC063F93B72B3C9DC258CF71A2F8EDE4BE60099B8DC226CD9B59E6417673F56F0A024584A57997E8C0DE315B64103A20ACB084499E2859C9DFD9FD55B E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...* 5....." ..0..X.....6v... ....`.....u..O.....h.....t..T..... ..... ..H.....text...<V... ...X..... ..`.rsrc...h.....Z.....@..@.rel oc.....`.....@..B.....v.....H.....,<..48.....`t.....:.(.....}....*..{....*..(....*Br...ps.....*:.(.....}....*..0..B.....-.r...ps....z.(.....,r...ps.... z.~....o.....o.....,.(d...*.s....*..{....*V.-..,...o....*.*.*...(.....*6..u....(....*b.,..o.....o.....(....*.*2.o....o....*B.o....%-.&r...p*2.s.....*>....s....(....*:.(.....}....*...(....,.~....*.o.....o.....o.....(....s ....*..0.....(....-.~....*.s....*2.(....o....*2.(....o....*2.(

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.UsbDeviceScanning.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	35328
Entropy (8bit):	5.534248228094931
Encrypted:	false
SSDEEP:	768:wE8Z0vegZtPTwUFFYL1O+1LI9v5Yr2YraeyCWL:w5Zceg5FS1OpvWZmBL
MD5:	3B318C2A671D24D8FCD8B9C2C80B2CD1
SHA1:	327465B531ADF77C039C577970094D5E44AEE6BA
SHA-256:	3EBD682BE3F402C47D180F931EC61149D7819CE972CC64B90C4C0D16E341B680
SHA-512:	84BC7484BB233E79D93C043F66611BE512984C725A20BA6EA02DBFED66471E4E5A8A402C481C6414B64EDD72B63E6FC5ADC37592BD0B629AE5ABF45FA68EEA D5

Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...:....." ..0.....v.... ....`.....$...O.....4...T..... ..... ..H.....text..... ..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....X.....H.....@..(}.....0..)..... {.....(....t.....|.....(...+...3.*....0..)..... {.....(....t.....|.....(...+...3.*....0..)..... {.....(....t.....|.....(...+...3.*....0..)..... {.....(....t.....|.....(...+...3.*....0..B..... (.....s.....o....~J...%-.&~I....o...s....%.J... ....o....&*..{....&.{....('...&.{....%-.&*o....*j.{.....{.....s... .o....*Z.{.....{.....o....*..(....*....0..a...

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.DeviceApis.UsbHidDevices.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	35840
Entropy (8bit):	5.7447981517839235
Encrypted:	false
SSDEEP:	384:+0JKe+JzvcOp0LMDU9oJi6zNkYMGVW8Hv8H/d5qZ91yORQSO4wT3K5I4ZxY2VSu2:Ye+hpcqaec6Z91yORW6Tp7uU/hc3
MD5:	F09F6BABAC74033C1BC664BB3CFBC001
SHA1:	D4B60D3879F505AC7B5B5B501954ABC2925343A8
SHA-256:	48DF286638BB2E42C23DD5616BCF981AE2FE81250B1B54888AB3B8C3AF1DFC75
SHA-512:	DB9DB98E34A6363D4B63CE7BCD860B589A6BE7EB62984B18A4FA23172EEEDFE296597986C6193AD6AC236640B11D994C5CEC92F922239F37686C234C190FADCF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....." ..0..... ....P.. ..`.....H...O.....L...T..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....|.....H.....dF..hX.....(.....}.....s...}.....s...}.....s...}....*f(.....s.....o....&*..{....o.....}.....{....o....+..{....o....&. {....o....-.*z.{.....o.....{.....{....o....*.0..>.....+3..{....{....o....o....%-.&+.o....{....o....&..&...{.....,*......./2.....r.(.....}.....}.....}....*~..{.....{.....(.....{....(....{....*..{....*..{....*..{....*..(.....3,.(....o ...o!....{....3..(....o''....{.....*.*..(#...*..{

C:\Program Files (x86)\Jabra\Direct4\FWU\GNAudio.FirmwareUpdate.DeviceFirmwareUpdateInfo.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14848
Entropy (8bit):	5.074625291254333
Encrypted:	false
SSDEEP:	192:N/ZuFV0widjqadMOzTe4DESf10MlytDkAAL5P2iCl:sywiVfeJSfOMlytDLAL5P2H
MD5:	29019EB61D41A6B776F4A9FE8C2865AB
SHA1:	BF012563109BE34DC40965169908E81D006ADC80
SHA-256:	C827CE4694676F754C27F44DE74AA415485673D2C406B0F542326D2001BA3512
SHA-512:	4202B6475D9FF78B14E938FABA34FE8F17B9BDE8A0A498091A98EF6F1EB0AC12EBFFF0D815F47B7F39E9F9065470695BB54FC4FB401C0B993BBDA4F72157686A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ....." ..0..0.....N... ...`..... ..... ..`.....N..O....`.....M..T..... ..... ..H.....text..../... ...0..... ..`.rsrc.....`.....2.....@..@.rel oc.....8.....@..B.....N.....H.....(...$.....0..L.....(.....}.....}.....}.....}.....}.....}.....}.....}.....}....*..{....*..{....*..{....*..{... .*..{....*..{....*..{....*..{....*..{....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..(....*N.(.....(...+}....*.0..,.....sE.....}'.....}(....{ .....F...s....(...+*.0..,.....sG.....})..... }

C:\Program Files (x86)\Jabra\Direct4\FWU\JabraCmdlineFwUpdater.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	106416
Entropy (8bit):	5.9897447475317405
Encrypted:	false
SSDEEP:	1536:Dlf2f+5aBfW2J9WrZ3pqQLV6PP/RprOSj9bi7Clx/AElxd0VbWsC7/19sWG1KNDK:9j5dy9lBCw4/eT8GSdh
MD5:	71D2773D0A4E101EC30C1F31CA686EB4
SHA1:	DA3DD0550A5D583516453B19C686F09D4656E804
SHA-256:	7D50CE7398646DF86E1D4DC7B5FEFE6A7051FEA9D84E5CA1F4696743ED6B12F8
SHA-512:	55D7C4D9FE5BE396EDED194BFEAB93959580EAADC4AF03C869131B2A0DD99D6F97D0D5C802652DC248D93AE0233F9BF39075E6EE6AF5CBC562256007ECFD5B12
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.....0..z..... .....@.. .....J.... .`.....7...O.....L.....X...T..... ..... ..H.....text....x... ...z..... ..`.rsrc...L.....\|.....@..@.relo c.....@..B.....k.....H.....*.....0.....E.....C...-...Y...*r...p..j...()...(*...*r#..p..j...()...(*...*rE..p..j...()...(*...*rc.. p..j...()...(*...*r}..p..j...()...(*...*.~....s+...*Z(.....o,...o-...o....*.0.....s/...%]$..o0...% ^$..o0...% .$..o0...% .$..o0...% .$..o0...% .$..o0...% .$..o0...% .$..o0...% .$..o0...% 1...o0. ..% 2...o0...% 3...o0...% 4...o0.....*..{,...*"..},...*..{-...*"..}-...*..{....*"..}....*..{/...

C:\Program Files (x86)\Jabra\Direct4\FWU\JabraCmdlineFwUpdater.exe.config

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	912
Entropy (8bit):	5.113183340992605
Encrypted:	false
SSDEEP:	12:TMHdG3VOcrO9LNFF7ap+5lgzM8p0f/2/lFiclFF7ap+5iplp7qf/2/vLjFicYo4p:2dErkPF7NyzP0H2/f9XF7NQ7uH2/F9y
MD5:	1FD5277FF900A25949E0470652DFFCFD
SHA1:	78A07CF6505209894E700B3C6B4B1E3BBA68A800
SHA-256:	14A72D59D5C0FBB5ADE76938E47CD4516DAFE65F467EBD777DFC09F8DDA071C3
SHA-512:	DF2BC1C6632E172D61F073A84C135D4B91935D398C7B21F3F1A05957778B2810C45E4608EFE78CC663D4BAF37AC2208D043F97AB1CE859702CE081BD57EB297
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <startup>.. <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.2" />.. </startup>.. <runtime>.. <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">.. <dependentAssembly>.. <assemblyIdentity name="GNAudio.DeviceApis.UsbDeviceInformation" publicKeyToken="ddd537774a768802" culture="neutral" />.. <bindingRedirect oldVersion="0.0.0.0-5.0.1.64088" newVersion="5.0.1.64088" />.. </dependentAssembly>.. </assemblyBinding>.. <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">.. <dependentAssembly>.. <assemblyIdentity name="System.Runtime.CompilerServices.Unsafe" publicKeyToken="b03f5f7f11d50a3a" culture="neutral" />.. <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="5.0.0.0" />.. </dependentAssembly>.. </assemblyBinding>.. </runtime>..</configuration>

C:\Program Files (x86)\Jabra\Direct4\FWU\Microsoft.Bcl.AsyncInterfaces.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	20872
Entropy (8bit):	6.448532891103289
Encrypted:	false
SSDEEP:	384:69P2wZOXm7YJVHTe+0VJl0vrdaVemxO/f7vWeq/WIdHRN7bg30uw7lGsV9W+:u2zmYrHCV9cIL6TbtCSW
MD5:	1EE251645B8A54A116D6D06C83A2BD85
SHA1:	5DBF1534FFBFF016CC45559EB5EFF3DC4252A522
SHA-256:	075CE79E84041137C78885B3738C1B5A03547D0AE2A79916E844196A9D0EC1DB
SHA-512:	9F67FD0566EAC2DA4253D08697DAAB427E4E85780615D940F086A88424DCBB0563ABAE7E4824088E64EF7024C1BB3BBF324F2D07BC7BA55F79E4AF3C9EA88E97
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....\" ..0..$.....C... ...`..... ..... ..`.....oC..O...`.....#.....|B..T..... ..... ..H.....text....#... ...$..... ..`.rsrc.....`.....&.....@..@.reloc.....,.....@..B.....C.....H.....4&.....A.....(....*..(....*.0.....(....}.....*6.\|.....(...+*:.\|.....(...+*:.\|.....(...+*2.\|....(....*..{....%-.&.\|....s.....(....%-.&.{....*"..(....*>..}.....}....*..0.....{....o.....{....(....*Z..}.....}.....}....*N.{.....{....s....*N.{.....{.....s....*v.{.....{....o ....{....s!...*..(....*"..s....*.0..... .....s"...*&...s"...*..{#...*"..}#...*.0..F.....{$....Xh}$.....}%.

C:\Program Files (x86)\Jabra\Direct4\FWU\Microsoft.VC80.CRT.manifest

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1870
Entropy (8bit):	5.392327712070946
Encrypted:	false
SSDEEP:	48:3SIK+hig4FB09kkK0hpzWU09kkKqYhzVC09kkK0FFzY:ClthaTXkHnCUXk8hgXkFj8
MD5:	D34B3DA03C59F38A510EAA8CCC151EC7
SHA1:	41B978588A9902F5E14B2B693973CB210ED900B2
SHA-256:	A50941352CB9D8F7BA6FBF7DB5C8AF95FB5AB76FC5D60CFD0984E558678908CC
SHA-512:	231A97761D652A0FC133B930ABBA07D456BA6CD70703A632FD7292F6EE00E50EF28562159E54ACC3FC6CC118F766EA3F2F8392579AE31CC9C0C1C0DD761D367
Malicious:	false

Preview:	.<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">.. <noInheritable></noInheritable>.. <assemblyIdentity type="win32" name="Microsoft.VC80.CRT" version="8.0.50727.4053" processorArchitecture="x86" publicKeyToken="1fc8b3b9a1e18e3b"></assemblyIdentity>.. <file name="msvcr80.dll" hash="0a38b652c9d03caab803c6b2505fa301e345bab2" hashalg="SHA1"><asmv2:hash xmlns:asmv2="urn:schemas-microsoft-com:asm.v2" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><dsig:Transforms><dsig:Transform Algorithm="urn:schemas-microsoft-com:HashTransforms.Identity"></dsig:Transform></dsig:Transforms><dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></dsig:DigestMethod><dsig:DigestValue>TM0VvywbHVQayIOw9CSX6M7WpaM=</dsig:DigestValue></asmv2:hash></file>.. <file name="msvcp80.dll" hash="678bf3da5d1987bb88fd47c4801ecb41f51366ef" hashalg="SHA1"><asmv2:hash xmlns:asmv2="urn:schemas-microsoft-com:asm.v2" xm

C:\Program Files (x86)\Jabra\Direct4\FWU\MxUvcFwu.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	78336
Entropy (8bit):	6.442308094031745
Encrypted:	false
SSDEEP:	1536:4PXEwIU2IJEAXZ/EO1tgDGyZ4qMJV3aaVaIZrRt7bwaF3t+CAHX:4PXkU2IJ3WzZ4HPas93t+CAHX
MD5:	DF74CA9CA8F872846A89F1F3D95C8FC7
SHA1:	6116A69AE92676A6802010AAA7C868E06851DABF
SHA-256:	EB462D421078E3D9DE594B1B253AF88A4B04AE6C3E207F95DFF7965D85E5E9E4
SHA-512:	1BA15006292E06AF5169BD16CA82EAB7F6A4A2270400666EF9B2983362C4D1D4212628EF653F6BE4767AA743CD39DF23DF7AB5B0E7617604B3F3CE537BA8EAFC
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Qv.?%.?%.?%...%.?%..;$.?%..<$.?%..:$.?%..>$.?%..>$.?%.>%b.?%h.6$.?%h.?$.?%h..%.?%h.=$.?%Rich.?%.....PE..L.....a.....!.....`.....p.....@..... .....#..,....P.....`..|.....p.....@.....h...@.....text..... ..`.rdata..8G.....H.....@..@.data.....@.....@....rsrc.....P.....".....@..@.reloc..|....`.....$.....@..B.....

C:\Program Files (x86)\Jabra\Direct4\FWU\MxUvcFwuWrapper.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	6.00342310392546
Encrypted:	false
SSDEEP:	768:vOJeXWpXs8I3212Xi4oGgqek8S11o2hSPCCBU8JilyQU8/EJFn:vDXcR6FoGvek2PnBU8JTFJx
MD5:	9A8BC11F2985484CD4D97C29CB585E39
SHA1:	DD99BDEABD4CD3C57ABE7B7E04191E680A1FB2E4
SHA-256:	F71E74538587711E7C19ACD0AB6AA33896CF559B82A15CCB21B5CB498407798D
SHA-512:	49ECC96E178690CC5BC55B8F4D30EC9715F4C3BF93FE31B05A122905E189D5D086D32B183DE8E22EFF64F587AE5CEED9DE9B72D55BFC41432E8795D30476B3B3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-...i...i...i...`...m...;...m...w...k...;...p...;...c...;...h.....j...}.k...i...T.....l.....h.....q.h.....h...Richi.....PE..L.....a.....!.....2.....]A.....P.....@.....(.....DR..p.....R..@.....P.....Q..H.....text...c1.....2..... ..`.rdata.....P.....6.....@..@.data...$.....@....rsrc.....@..@.reloc.....@..B.....

C:\Program Files (x86)\Jabra\Direct4\FWU\PanaCastAPI.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	184320
Entropy (8bit):	6.460255903476623
Encrypted:	false
SSDEEP:	3072:m3ec49NG4rmwp8vNVeVM5+LFwArbdwHUiiYQXccVklknJJasFXK:mOcErn8vTWk+Lueb6riYmJasU
MD5:	E7960D4B15529F2DC586A6D81E3B4141
SHA1:	C4D8078B5EEA9241EFF89E589B2C9366A1CA961A
SHA-256:	8A07DF6BB412BC884E1C791F1EC34397ABBD6CCD55ADCC70D93FC89745AE1456
SHA-512:	68E7DA3DFB4F3A17D4972BB3A92B98FA5EE01FEBF4E982A72EDCE8B114406BE485C46D295867862C5D798665A5937E98B52FFAE8DC9266A3D52C9BCC7F1DC19C
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I..'...'...'.....'..#...'..$...'..''...'..&...'...&...'...&...'.....'...'...'.....'...% ...'.Rich..'.....PE..L.....a.....!.....H.....#.....`.....@.....@.....(v..p.....w.....v..@..... .....`.....text....F.....H..... ..`.rdata..va...`...b...L.....@..@.data.....@....rsrc.....@..@.reloc..... ..@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\FWU\PanaCastAPIWrapper.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	69120
Entropy (8bit):	5.988726028042358
Encrypted:	false
SSDEEP:	1536:6sdnBjBOSqNGDsxAKfT0spDMfRMFvXR8PliG4QhYglhkSsJPnniyjWAPF+0n:xdnBjBOSqNGDsxAgTfBMQ/R8PliG4QhC
MD5:	DA1DDAEE5E4D54B2242DD1E01B20C82F
SHA1:	1B39FFF8B5937E96EB0731917C3122900A2B2B33
SHA-256:	516CD83AC427C6CEDDB01EC355E656AA91E2A846DD2165A4D8E1FF45BC13ADB7
SHA-512:	9B8F4B4868673EC41EF3F901C14868988546FB3584AB9AE3DF97B411746D91A0597A54A683CC6F740027213A4EE1DDEEE35F6AD550D1B6A6BB9FBFB51007F408
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w.....w.....w...%...w.....w.....w.....w.....w..N....w...w ...w..N....w..N.B..w...w*..w..N....w..Rich.w.....PE..L...#.a.....!.....P.....`.....@.....@..... ..@..... 0.....|b..p.....b..@.....`.....4b..H.....text....O.....P..... ..`.rdata.....`.....T.....@..@.data...l.....@....rsrc...@.... ....@..@.reloc.....0.....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\FWU\SitelHidFwu.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	198144
Entropy (8bit):	6.781790426307126
Encrypted:	false
SSDEEP:	6144:qPy2C0t6qKAdjgeKKFEIt5o0Sg+D3gG4q06T8S2ICgVb:72/6edNz54g+D1z3Vb
MD5:	B6CFBB84207EBDA65718579D869BA268
SHA1:	AB0C0D7D5B69624FDB2027CA0EAA0F08D3B1A1C6
SHA-256:	33C3C77CFB9D10D43309C0DABA273324D41E6EA9D42C9BC15B36B57A35506D12
SHA-512:	01FE9345EF27204E5A830A9144D2D33D5C19BED2E832B2AFE6D2C2E6DA8794A8B09C86B82C3792FE0BE4447B1489B47F8D1BD244E5F539CF8C2A2781A66A27A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....fM.k...k...k.....k.....k.....k.....k.....k.....k...cU..k.....k...k ...k..'....k..'....k..'....k...k...k..'....k..Rich.k.....PE..L.....a.....!.....X.....`.....@.....8.....=..@.... .....0...$...''..p..... .....H#.....x''..@.....text...Q..... ..`.rdata...m.....n.....@..@.data...h....P.....>.....@....rsrc..... .....@..@. reloc...$...0...&.....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\FWU\SitelHidFwuWrapper.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	75264
Entropy (8bit):	6.1427489834912485
Encrypted:	false
SSDEEP:	1536:MEFAaiDJGKAc+WbrHuGEC/G+hAQYCrP0mq3Ly69aV:MMiDJbAZW+GECgQlPkLy69
MD5:	0F19A1B367D5954D3562BF1DFF50A37F
SHA1:	15AAA039CE4E7C8BE8DDC858862B2ACBA4558A80
SHA-256:	0286652894A3CE99E45B0BCA70DFB592963A38FD7606D1E55574A1822053242B
SHA-512:	33138963A433E4010731CC2DAB4CC60A88DA13EB0F7C53069E064EDE75D5C9DEDDFD5CD7CFC5DB85D4332A0EFDF3EA933B92CE71097AB07C3766EA95BACFD68
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.!.}.O.}.O.}.O.t..{.O./.N...O.i.N.~.O.c....O./.J.j.O./.K.w.O./.L.|.O..N ...O.}.N.C.O..J.x.O..O.|.O....|.O.}..|.O..M.|.O.Rich}.O.....PE..L.....a.....!.....8.....G.....P.....`.....@.....#.....$.....@..... .....P..$...tR..p.....R..@.....P.....,R..H.....text....7.....8..... ..`.rdata.....P.....<.....@..@.data...|....0.....@....rsrc..... ..@.....@..@.reloc..$....P..... .....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\FWU\System.Buffers.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	20856
Entropy (8bit):	6.425485073687783
Encrypted:	false
SSDEEP:	384:/rMdp9yXOfPfAxR5zwWvYW8a2cyHRN7vCvlbLg:/rMcXP6N6e
MD5:	ECDFE8EDE869D2CCC6BF99981EA96400
SHA1:	2F410A0396BC148ED533AD49B6415FB58DD4D641
SHA-256:	ACCCCFBE45D9F08FFEED9916E37B33E98C65BE012CFFF6E7FA7B67210CE1FEFB
SHA-512:	5FC7FEE5C25CB2EEE19737068968E00A00961C257271B420F594E5A0DA0559502D04EE6BA2D8D2AAD77F3769622F6743A5EE8DAE23F8F993F33FB09ED8DB2741
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....jM^......" ..0..$.....BC... ...`..... ..... ..@.....B..O....`..@.....x#.....A..... ....H.....text...H#... ...$..... ..`.rsrc...@....`.....&..... ..@..@.reloc.....,.....@..B.....$C.....H.....'.....?..X...8A.....j~....%-.&(....s....%.....*..*...0..$.....(.....o.....&...,...o....,..*.*..... .....,!(.....,.r...p.(....(....*..(....*.*.(.....,r...p.....%...%...(....*..(....*.(.....,r...p.....%...%...%...(....*...(....*.~....*2r...p.(....*B.....(.....*R.....(. ..+%-.&(!...*^.....("....(...+&~....*.s$...*"..s%...*..(&...*.*....0.....

C:\Program Files (x86)\Jabra\Direct4\FWU\System.Memory.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	141184
Entropy (8bit):	6.115495759785268
Encrypted:	false
SSDEEP:	3072:IUGrszKKLBFa9DvrJGeesIf3afNs2AldfI:jBFd3/aFs2
MD5:	6FB95A357A3F7E88ADE5C1629E2801F8
SHA1:	19BF79600B716523B5317B9A7B68760AE5D55741
SHA-256:	8E76318E8B06692ABF7DAB1169D27D15557F7F0A34D36AF6463EFF0FE21213C7
SHA-512:	293D8C709BC68D2C980A0DF423741CE06D05FF757077E63986D34CB6459F9623A024D12EF35A280F50D3D516D98ABE193213B9CA71BFDE2A9FE8753B1A6DE2F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....jM^......" ..0..... ... .`..... ..@.....X...O.... ..0.....#...@..... ..... ..... ..H.....text..... ..... ..`.rsrc...0.... .....@..@.rel oc.....@.....@..B.....H.....,.....('...*>..}.....}....*..{....*..{....*..{....{....3..{....{....((...*.*..0.....%.u...,.....(....*.*z. {....%-.&.+.o)....{....(a...*..(....zN.....o*...s+...*.(....z.s,...*..(....zF(U....(O...s-...*.(....z.(V...s-...*.(....z.s....*.(....z.s/...*..(....zN.....o*...s0...*.(....zrr...p(\....c.K...(O...s1...*.(. ...zBr...p(Y...s1...*.(....z.s2...*.(....z.(X...s3...*.(!...z.(_...s3...*.(#...z

C:\Program Files (x86)\Jabra\Direct4\FWU\System.Numerics.Vectors.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	115856
Entropy (8bit):	5.631610124521223
Encrypted:	false
SSDEEP:	1536:nPOw0SUUKw+GbgjMV+fCY1UiiGZ6qetMXIAMZ2zstK/hV+sUwS:nWw0SUUKBM8aOUiiGw7qa9tK/bJS
MD5:	AAA2CBF14E06E9D3586D8A4ED455DB33
SHA1:	3D216458740AD5CB05BC5F7C3491CDE44A1E5DF0
SHA-256:	1D3EF8698281E7CF7371D1554AFEF5872B39F96C26DA772210A33DA041BA1183
SHA-512:	0B14A039CA67982794A2BB69974EF04A7FBEE3686D7364F8F4DB70EA6259D29640CBB83D5B544D92FA1D3676C7619CD580FF45671A2BB4753ED8B383597C6DA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?.Z....." ..0..v..... ....DF.. ..@.....f...O.....>..... ....H.....text....u... ...v..... ..`.rsrc.....x.....@..@.relo c.....@..B.....H.....Q..|?.....$... ...D.....(....*&.l(....k*&.l(....k*..l.l(....k*..l.l(....k*&.l(....k*&.l(....k*&.l(....k*j~....%-.&(....s. ...%.....*..*.0..$.....(.....o.....&...,....o.....,..*.*.....,!(.....,.r...p.(....(....*..(....*.*.(.....,r...p.....%...%...(....*..(....*.(.....,r...p.....%...%...%...(....*...(....*.(....,!r...p.....%...%... %...%...(....*....(....*.~....*2r...p.(....*2rG..p.(....*2r...p.(....*2r...p.(.

C:\Program Files (x86)\Jabra\Direct4\FWU\System.Runtime.CompilerServices.Unsafe.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

Size (bytes):	16768
Entropy (8bit):	6.378509219645678
Encrypted:	false
SSDEEP:	192:erLXx0hyLsbb3rxVj7WU2WLTYoW4GD5dHnhWgN7acWlbAkWD7DiqnajKs3WoHpZ:Ih06sbbVVPWU2WPY7dHRN77RGlGs3jJZ
MD5:	9A341540899DCC5630886F2D921BE78F
SHA1:	BAB44612721C3DC91AC3D9DFCA7C961A3A511508
SHA-256:	3CADCB6B8A7335141C7C357A1D77AF1FF49B59B872DF494F5025580191D1C0D5
SHA-512:	066984C83DE975DF03EEE1C2B5150C6B9B2E852D9CAF90CFD956E9F0F7BD5A956B96EA961B26F7CD14C089BC8A27F868B225167020C5EB6318F66E58113EFA37
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._.....!.....3... ...@....@.. .....t@... .@.....@3..K....@.....#..`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....p3.....H.....$..0.....P ....._.%c.....=.n')...(v..}.d...3...B...).. .:Q(....L.jt....}Xv.b7y0r.[..$....q..c.6.....p..2..qHv/. pb.=..9.o"z.. 0P.t%H....U...0.....q....*..0.....q....*...0.....q....*...0.....*.0.....*..0.....*..0.....q.....*....0.....q.....*....0..... ...*..0.....*....0.....*..0.....*...0.....

C:\Program Files (x86)\Jabra\Direct4\FWU\System.Text.Encodings.Web.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	68472
Entropy (8bit):	5.977153039222987
Encrypted:	false
SSDEEP:	1536:czy/zOmekrEZa8frFpd3hQi/+sBzFLknqPO:TzOmekwZa8zdR+sBpSYO
MD5:	E8CDACFD2EF2F4B3D1A8E6D59B6E3027
SHA1:	9A85D938D8430A73255A65EA002A7709C81A4CF3
SHA-256:	EDF13EBF2D45152E26A16B947CD953AEB7A42602FA48E53FD7673934E5ACEA30
SHA-512:	EE1005270305B614236D68E427263B4B4528AD3842057670FAD061867286815577EC7D3ED8176E6683D723F9F592ABCBF28D24935CE8A34571AB7F1720E2FFC5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&gY....." ..0.....2.... ....@..... ..`.....O.....x#.. .....T..... ..... ..H.....text...8.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....`..,t.....t.....(%...\*..(%...\*..(%...\*^.(%.....4...%...}....\*:.(%.....}....\*:.(%.....}....\*:.(%.....}....\*....0..E..... ...\_.b..._X ....Y..e pp.._.d.X ....X.`.....X(&.....R...(&.....d.R*....0..K..... ..._.b..._X ....Y..e pp.._.d.X ....X.`.....X('.... ..._.S...('.....d.S*..0..&.....+....((...G...Z.(.....X....()...2.* ...0.....().....1...()....Z.6.....(...+.+...()....Z.....s+.....

C:\Program Files (x86)\Jabra\Direct4\FWU\System.Text.Json.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	355720
Entropy (8bit):	6.089400920308145
Encrypted:	false
SSDEEP:	3072:USOCU3QYmd1QhS1h2pCUoUJeXq7YAAEP1VIGm/0aW/49rZbpQ2M6R:Q7MQMh2pCUreatAJhrZlh
MD5:	38470CA21414A8827C24D8FE0438E84B
SHA1:	1C394A150C5693C69F85403F201CAA501594B7AB
SHA-256:	2C7435257690AC95DC03B45A236005124097F08519ADF3134B1D1ECE4190E64C
SHA-512:	079F7320CC2F3B97A5733725D3B13DFF17B595465159DAABCA5A166D39777100E5A2D9AF2A75989DFABDB2F29EAC0710E16C3BB2660621344B7A63C5DBB87EF8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....." ..0..@.....\... ..`..... .....84.. ..`.....Y\..O....`..d.....J...#.....[..T..... ..... ..H.....text....?... ...@..... ..`.rsrc...d....`.....B.....@..@.rel oc.....H.....@..B.....\.....H.....t.....@....Y...[.....(%...\*..(%...\*..(%...\*^.(%.....%...}....\*:.(%.....}....\*:.(%.....}....\*:.(%.....}....\*....0. .E..... ...\_.b..._X ....Y..e pp.._.d.X ....X.`.....X(&.....R...(&.....d.R*....0..K..... ..._.b..._X ....Y..e pp.._.d.X ....X.`.....X('.... ..._.S...('.....d.S*..0..&.....+....((...G...Z.(.....X.... ()...2.*...0.....?.....().....1...()....Z.....(...+.+...()....Z.....s+.....

C:\Program Files (x86)\Jabra\Direct4\FWU\System.Threading.Tasks.Extensions.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	25984
Entropy (8bit):	6.291520154015514
Encrypted:	false
SSDEEP:	384:1R973o62/KqcAnb05J3w0I5eUGef8s72XBWdvVW2JW8aJcyHRN7WEimpplex:1RZ4nNxnYTb6Blha

MD5:	E1E9D7D46E5CD9525C5927DC98D9ECC7
SHA1:	2242627282F9E07E37B274EA36FAC2D3CD9C9110
SHA-256:	4F81FFD0DC7204DB75AFC35EA4291769B07C440592F28894260EEA76626A23C6
SHA-512:	DA7AB8C0100E7D074F0E680B28D241940733860DFBDC5B8C78428B76E807F27E44D1C5EC95EE80C0B5098E8C5D5DA4D48BCE86800164F9734A05035220C3FF1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....jM^....." ..0..8.....V... ...`..... ..... ..@.....V..O....`.....B...#.....PU..... ....H.....text....6... ...8..... ..`.rsrc.....`.....:.....@..@.rel oc.....@.....@..B.....V.....H.....0...$.....T.....(....*..(....z..(....z2.(....s....*2.(....s....*:.....o....*.~....*~.-..(.....}.....}.....}....*~.-.. (.....}.....}.....}....*Z..}.....}.....}....*J.{....%-.&.*o....*^.u....,.....(....*.*~.{.....{....3..{.....{.....*.*&...(....*2...(.....*....0..'.....{.....,..u....%-.&..(...+(....*(....*n.{....,..(....s....*.q.... *..0..a.....{....o0.....,;..{....o2...(.....;...3.~.....s.....

C:\Program Files (x86)\Jabra\Direct4\FWU\System.ValueTuple.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	25232
Entropy (8bit):	6.672539084038871
Encrypted:	false
SSDEEP:	384:VyPa16oAL4D+wW9lWmDlW4lWYDMFm0GftpBjMIraQHRN7VlmTpF0:VWs6oqDjADKeDYViG+LN
MD5:	23EE4302E85013A1EB4324C414D561D5
SHA1:	D1664731719E85AAD7A2273685D77FEB0204EC98
SHA-256:	E905D102585B22C6DF04F219AF5CBDBFA7BC165979E9788B62DF6DCC165E10F4
SHA-512:	6B223CE7F580A40A8864A762E3D5CCCF1D34A554847787551E8A5D4D05D7F7A5F116F2DE8A1C793F327A64D23570228C6E3648A541DD52F93D58F8F243591E32
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?.Z....." ..0.....b2.. ...@..... .....H.. ..@.....2..O....@.....$...>..`.....x1..... ..... ..H.....text...h.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....".....@..B.....B2.....H.....!..T.....0.....j~....%-.&(....s....%.....*..*...0..$.....(.....o.....&...,....o....,..*.*.....!(....,.. r...p.(....(....*..(....*.*.(....,r...p.....%...%...(....*..(....*.(....,r...p.....%...%...%...(....*...(....*.(....,lr...p.....%...%...%...%...(....*....(....*.~....*2r...p.(....*2r[..p.(....*B.....(.....*.BSJB .....v4.0.30319.....l...4...#~.....#Strings....t.....#US.@.....

C:\Program Files (x86)\Jabra\Direct4\FWU\TestEngine.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	446464
Entropy (8bit):	5.891951310393716
Encrypted:	false
SSDEEP:	12288:OhGvF1mFCQ6V+ACcgKvJG8fy3mioVuESBl:giE8Jhy3uud
MD5:	262505DBE54EEE0C3E3851D201BC286F
SHA1:	C9A59DA1AE45258EF88F3EC797B03436D0355D9C
SHA-256:	6908CFB3F32C00E369B4BA76AB9A8AD7796929100BD4B050201E4EEE04CCF42A
SHA-512:	E421C3E6E5AC267C588E2CEEFD3188845EDDD0C9B8E027DD69E3F6EC8E1FF1F6DF164C61F405ADFB2CBB0243D4462CF51FD2FC81AA6AD1E7FF0ACB37B751 8DAB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.Q.....R..... ....Rich.....PE..L....=.K.....!.....0.....!.....@.....YZ..... W..<...$8.....;.....M.....{.. @.....@..P.....text...z'.....0..... ..`.rdata..V...@...0...@.....@..@.data....N...p...@...p.....@....rsrc....;.....@.....@..@.reloc.. ....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\FWU\msvcp80.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	554832
Entropy (8bit):	6.428533960834858
Encrypted:	false
SSDEEP:	12288:UZY4lOHMwLwXBt+ia3htSUa/hUgiW6QR7t5j3Ooc8NHkC2eSQ:UZY4lOHMM8wiShtSj3Ooc8NHkC2eT
MD5:	8C53CCD787C381CD535D8DCCA12584D8
SHA1:	BC7CE60270A58450596AA3E3E5D0A99F731333D9
SHA-256:	384AAEE2A103F7ED5C3BA59D4FB2BA22313AAA1FBC5D232C29DBC14D38E0B528
SHA-512:	E86C1426F1AD62D8F9BB1196DEE647477F71B9AACAFABB181F35E639C105779F95F1576B72C0A9216E876430383B8D44F27748B13C25E0548C254A0F641E4755
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y..y..y..fv..y..y..#y.....y..2...y.....y.....y.....y.....y.....y.....y..Rich .y.....PE..L....LYJ.....!.....@... .....P....B|.....p.....0....@.....L...T...<.....`..P.... ..H2...S.....Pe..@.....P.. .....text...V>.....@..... ..`.rdata.....P.....P.....@..@.data...l&..... .....@....rsrc.....@..@.reloc..NA... ...P.....@..B. .....

C:\Program Files (x86)\Jabra\Direct4\FWU\msvcr80.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	632656
Entropy (8bit):	6.854474744694894
Encrypted:	false
SSDEEP:	12288:bxzh9hH5RVKTp0G+vjhr46CIw+0yZmGyYCj:bph9hHzVKOpXwymGyYo
MD5:	1169436EE42F860C7DB37A4692B38F0E
SHA1:	4CCD15BF2C1B1D541AC883B0F42497E8CED6A5A3
SHA-256:	9382AAED2DB19CD75A70E38964F06C63F19F63C9DFB5A33B0C2D445BB41B6E46
SHA-512:	E06064EB95A2AB9C3343672072F5B3F5983FC8EA9E5C92F79E50BA2E259D6D5FA8ED97170DEA6D0D032EA6C01E074EEFAAB850D28965C7522FB7E03D9C65EA E0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L.....@.....!.....;.....d.....Rich..... .....PE..L...yLYJ.....!.....0...p.....+#.....@.....x.....@.....q...~..Pc..<....`.....P....p..P3...B.....F..@.....@..... .....text...'.....0..... ..`.rdata.....@.....@.....@..@.data...Li.....P.....@....rsrc.....`.....@.....@..@.reloc...7...p...@...P.....@. .B..... .....

C:\Program Files (x86)\Jabra\Direct4\FWU\pttransport.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	81920
Entropy (8bit):	5.6342110277745405
Encrypted:	false
SSDEEP:	1536:UuJYOHf8awqX8iSU+f063abLpXNkX0zODFeurPpn:H2SHWZ3abLpd3ODDPpn
MD5:	E17F1923F41162B7708882BBA566E81F
SHA1:	4E5E00A8EBABC38DE2CBACBC25B854390EF0BBA3
SHA-256:	11E80FA0F9AE0F2D3DB07A6DD77865485206FD48068FC6172BC2D85593FCEF7C
SHA-512:	7A0541607F5C9D41C48B464D343D3F395050EBFC92AAA50DD8F85EBC70BF1637F06FB776535517B8B203948DBE3BFA7929D4208D567857567B55DE4875ADD8A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P.c.....ns.....3lp.....3lv.....P.....l...3l`.....3lc.....3lw.....3lq .....3lu.....Rich.....PE..L...;.K.....!.....N.....+.....P.....4...P.....h.....x...@..... .....text..... ..`.rdata..+8.....@.....@..@.data...h.....@....rsrc.....@..@.reloc..... ... .@..B... .....

C:\Program Files (x86)\Jabra\Direct4\LICENSE	
Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1096
Entropy (8bit):	5.13006727705212
Encrypted:	false
SSDEEP:	24:36DiJHxRHuyPP3GtIHw1Gg9QH+sUW8Ok4F+d1o36qjFD:36DiJzfPvGt7ICQH+sfIte36AFD
MD5:	4D42118D35941E0F664DDDBD83F633C5
SHA1:	2B21EC5F20FE961D15F2B58EFB1368E66D202E5C
SHA-256:	5154E165BD6C2CC0CFBCD8916498C7ABAB0497923BAFCD5CB07673FE8480087D
SHA-512:	3FFBBA2E4CD689F362378F6B0F6060571F57E228D3755BDD308283BE6CBBEF8C2E84BEB5FCF73E0C3C81CD944D01EE3FCF141733C4D8B3B0162E543E0B9F3E 63
Malicious:	false

Preview:	Copyright (c) Electron contributors.Copyright (c) 2013-2020 GitHub Inc...Permission is hereby granted, free of charge, to any person obtaining.a copy of this software and associated documentation files (the."Software"), to deal in the Software without restriction, including.without limitation the rights to use, copy, modify, merge, publis h,.distribute, sublicense, and/or sell copies of the Software, and to.permit persons to whom the Software is furnished to do so, subject to.the following conditions:..The above copyright notice and this permission notice shall be.included in all copies or substantial portions of the Software...THE SOFTWARE IS PROVIDED "AS IS", W ITHOUT WARRANTY OF ANY KIND,.EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF.MERCHANTABILITY, FITNESS FOR A PAR TICULAR PURPOSE AND.NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE.LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION.OF CONTRACT, TORT OR OTHERWISE, ARISIN

C:\Program Files (x86)\Jabra\Direct4\LICENSES.chromium.html

Process:	C:\Windows\System32\msiexec.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	5458104
Entropy (8bit):	4.829207944779583
Encrypted:	false
SSDEEP:	12288:/7etnqnVnMnBnunQ9RBvjYJEi400/Q599b769B9UOE6MwMGucMEbHDuX0YnpWQZG:sPMM5FaWStHvmUKItmfDTeHiVQZp4
MD5:	4247AFA6679602DA138E41886BCF27DA
SHA1:	3BB8C83DC9D5592119675E67595B294211DDBF6E
SHA-256:	BF59A74B4404AA0C893CA8BBE636498629B6A3ACDFF4ACB84DE692462FD626E4
SHA-512:	AD3103F7FD32F0EC652BC7FCB8C303796367292A366037ACAD8E1312775CDD92C2F36ED8C34A809251AD044508E1E7579B79847DE61025BAF8BDA5AD578A033 0
Malicious:	false
Preview:	Generated by licenses.py; do not edit. --><!doctype html>.<html>.<head>.<meta charset="utf-8">.<meta name="viewport" content="width=device-width">.<meta name ="color-scheme" content="light dark">.<title>Credits</title>.<link rel="stylesheet" href="chrome://resources/css/text_defaults.css">.<style>.html {. --google-blue-50: rg b(232, 240, 254);. --google-blue-300: rgb(138, 180, 248);. --google-blue-600: rgb(26, 115, 232);. --google-blue-900: rgb(23, 78, 166);. --google-grey-200: rgb(232, 234, 237);. --google-grey-800: rgb(60, 64, 67);. --google-grey-900: rgb(32, 33, 36);.. --interactive-color: var(--google-blue-600);. --primary-color: var(--google-grey-900);.. -- product-background: var(--google-blue-50);. --product-text-color: var(--google-blue-900);.. background: white;.}..@media (prefers-color-scheme: dark) {. html {. -- interactive-color: var(--google-blue-300);. --primary-color: var(--google-grey-200);.. --product-background: var(--google-grey-800);. --pro

C:\Program Files (x86)\Jabra\Direct4\LyncIntegration\default.xml

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	124
Entropy (8bit):	4.820507904693396
Encrypted:	false
SSDEEP:	3:JLWMNHU8LdgCfSYuwA48JCDLhRSUfqYJW9YVb:JiMVBd/pz8J2VRS6qYdb
MD5:	7D2B0C0D6C342CAB811D2AF4848B9F5C
SHA1:	B956EB87F6AB1505C36857C99639E76EC79276D3
SHA-256:	FE75BFCC96F9F79892C16EEBAD9B5382C9ACB95C35AC5727C0C0DF66DD516A20
SHA-512:	EF353DACB825BB3919E9EFC53BAAE8DCFF63544EE88DA8DD0F4D6D4F8B80E761F53D30E1AE79D8D05162C7B3314FE0EBD01DCA3FFBF07A0073E9E0B8D889 4CBB
Malicious:	false
Preview:	.<?xml version="1.0" encoding="UTF-8"?>..<settings>.. <setting id="IntelligentCallTransfer" value="false" />..</settings>

C:\Program Files (x86)\Jabra\Direct4\NEC SP 350 Integration\GNDeviceInterface.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	97792
Entropy (8bit):	6.346077105798904
Encrypted:	false
SSDEEP:	1536:us/cxHaYqit+6hklnAHYOFoQKKYsvqF1ETFzm81W1wIbCMH5ZOZKexIK:usRYqQRkleYcoQKKYsSFsFlW1wIbTH5e
MD5:	AB4941F936ED58F8FF1FD398BAD4F5C1
SHA1:	939DF0AB35349BF91805765F3AB5086A2138BB21
SHA-256:	4B7AA3AC680CD4CE9F924ADF1ABA34E241A62B3F5E579DFE18349BC36410ED3A
SHA-512:	35DC5D3C5445DE278D02C184F55653F72D31EAC5963A3F82E2024BFC903DF75D31B01912FCFC1A1E139F933EAB2444CCE814CB0E9686FE4C535DA0B91A54FA 9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....X.J...$...$...$.....$..C....$.....$..C....$..C....$...y...$.....$...%.t.$..C ....$..C....$.....$..C....$.Rich..$.....PE..L....6.T.....!.....)....@.....X|.....`.....X..... .....@.....H.....text..... ..`.rdata.....@..@.data.....p.....@....rsrc...`.....r.....@..@.reloc..... ....x.....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\ZoomIntegration\Autofac.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	190976
Entropy (8bit):	6.011014830652571
Encrypted:	false
SSDEEP:	3072:Ug5OK8PAVhSWTiIg/PHqD6Ug7Hiz44Wrbge7ILsf4qzTZ78srAnqdzYR4:UvehS5cWrVaYvp8srAqdzY
MD5:	67E05AE28D1017FBA80C237CE715BD3A
SHA1:	0EF18AEE4FD25144E8B754D2E907D81A8269061E
SHA-256:	8AAEC6C836BFE934799E1F28588E6426BE5D5158EBCFD4B9E0A17B5293764F46
SHA-512:	EB4ACD675A998AD6DF5469F880AB222DFFB0CEE526F43EE7851D45E6C6CBACB01F83E822D651110A7BCCF944E1A5883A846ADFF21E6659D28B8EFFDFF8442 2A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....6.O.....!.....>.... .. ....@.. .....`.....d.. ..@.....O.... .....@.....h..... ..... ..H.....text...D.... ..... .. `.rsrc..... .....@..@.rel oc.....@.....@..B..... .....H.....D...$.....8..P .....J...D?._.h.XB$..`...q..".Jv$`f.o.sV?.n..;S6..p."1i6..[{..y...UN..\.....vh..jbzy...$..c ?t.T.2_.....d....e.=.....l..i....<....(....*.0..".....{?.....{@.....o....*...0.....sR.....}@....{@...u!.....,..o.....F...(....(/...-.(...+*.o....o.....o.....~.....o....}?.....o.....S...s ...(...+(...+*..*.(k...*..(....*..(....*..{#....{$...{%....{&...oD.....*....0..2...

C:\Program Files (x86)\Jabra\Direct4\chrome_100_percent.pak	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	142210
Entropy (8bit):	7.920484146948989
Encrypted:	false
SSDEEP:	3072:nKzw9bp66mdgZeMj6g2Z8Gb0+VRLf0ld0GY3cQ3F2DExm/KLQ2I:nKzw986mdgZezgm8Gb0OV8ld0GecQ3m3
MD5:	4F7CF265DB503B21845D2DF4DC903022
SHA1:	970B35882DB6670C81BD745BDEED11F011C609DA
SHA-256:	C48E6D360AEE16159D4BE43F9144F77D3275A87B3F77EAE548E357601C55FC16
SHA-512:	5645D2C226697C7AC69CE73E9124630696516FC18286A5579823588F93A936DA71084A3850F1F9A7B34C624F4C502957107F5957FFBA5E6C1E4DA6D8DA7D3348
Malicious:	false
Preview:	.....#.N...:.....V^....W^....X^....Y^....Z^1...[^....\^....]^....^^...._^....`^/...g^."..h^M$..k^.%..l^:'..s^.'..t^31..u^a9..v^.;..w^)<..Tj.=..Uj8>..Vj.?..Wj.B..Xj.E..Yj.I..Zj.M..[j.P..\j .T...jWX...j.Y...j.[...jp\...jc]...j.^...j.^...j.....jV....z+....z.....zd....za....z.....z.....z*....z.....z.....z.....zI....z.....z.....zE....z.....z.....z=....z]....z.....z."...z9,...zq6...z.:...z?<...z.E...z.M...zpN.. .z.O...z.Q...z.T...z.U...z.X...z.Z...zc\...z:^...z.`...z>a...z.b...zPd...z.g...z.i...zGl...z.m...z:q...z.t...z:v...z.....z.....{.....{.....{.....{x....{Z....{....{T....{....{.....{.....{W....{<....{.....{.....{.....{.....{N... .{<....{.....{....{.....{.....{e....{.....{.....{....{.....{{....{B....{.... {....!{...."{@...${R...%{....&{...'{r...({....){X...*{....+{.....{J...-{.....{..../{....0{F...1{....2{....3{....4{F...5{}...6{s...7{h...:{`...d}:...e}.. ..f}....g}3...h}....i}....j}....k}.....l}f...m}....n}....o}l...p}]...q}G...r}....s}G...t}....u}T...v}....w}m ..x}. ..z}.!..{}.!

C:\Program Files (x86)\Jabra\Direct4\chrome_200_percent.pak	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	207666
Entropy (8bit):	7.946728386126796
Encrypted:	false
SSDEEP:	6144:XDQYaF+9b16mdgZezVk5GMRejnbdZnVE6Yopym74:8fs1FdgEj6edhVELo374
MD5:	6A7A9DEE6B4D47317B4478DBA3B2076C
SHA1:	E9167673A3D25AD37E2D83E04AF92BFDA48F0C86
SHA-256:	B820D19A7A8CE9D12A26837F967F983E45B07550B49E7B9A25E57B417C5F6FD9
SHA-512:	67466E21A13CA449B014B511FB49BFC51DF841EB5776F93B4BDA2E0023DA96D368AC5C65DE051ED9DE1899275B9F33839AF2C387BE903688CDB48BF08993791 E
Malicious:	false
Preview:	.....#.O...:.....V^z...W^....X^m...Y^2...Z^p...[^k...\^)&..]^e+..^^u..._^.5..`^":..g^yB..h^.D..k^_F..l^.I..s^YJ..t^.^..u^.p..v^v..w^.v..Tj#x..Uj.|..Vj8...Wj,...Xj1...Yjp...Zj....[jc...\j .....j.....j.....j.....j.....j.....j<....j.....j.....z.....z]....z.....z.....z.....z(....z.....zM!...z.)...zu0...z.5...zX;...z:B...z.D...z.H...z.L...z V...zLY...z.a...z.e...zLo...z.y...z.}...zv....zM....z....z.....z....z....z....z....z....zZ....z1....z....z....z....z....z.....z.....z*....zC....z.....z5....zf....z\....{<....{.....{M....{g....{k....{.....{J ...{.!...{P#...{.$...{T&...{.(...{.*...{T/...{B4...{#<...{.D... {bE...{.F...{.H...{zI...{.J...{7L...{.O...{.S...{.W...{.X...{TZ...{.[...{.....{"....{q... {....!{w..."{0...${B...%{....&{....'{A...({....){....*{....+{.....{....-{.....{..../{....0{....1{....2{'...3{H...4{<...5{....6{... .7{n...:{2...d},...e}....f}....g}I...h}....i}*...j}....k}Y...l}....m}....n}k...o}....p}....q}....r}`...s}....t}{...u}....v}....w}C.

C:\Program Files (x86)\Jabra\Direct4\d3dcompiler_47.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	3714200
Entropy (8bit):	6.570736584573205
Encrypted:	false
SSDEEP:	49152:sXMoHAsisjBFjJMLhHELxJm8ZU8W/GBj5Z535TMpinAizxkl/cD11bqCG7jHbOkD:srZOb8W/G5hnAizxz7NZy9AG
MD5:	2F2E363C9A9BAA0A9626DB374CC4E8A4
SHA1:	17F405E81E5FCE4C5A02CA049F7BD48B31674C8F
SHA-256:	2630F4188BD2EA5451CA61D83869BF7068A4F0440401C949A9FEB9FB476E15DF
SHA-512:	E668A5D1F5E6F821EBFA0913E201F0DFD8DA2F96605701F8DB18D14EA4FDEAC73AEB9B4FE1F22EAEFFCDD1C0F73A6701763727D5B09775666F82B678404E49 4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s.....s.....G...../.....)....+..... Rich.....PE..L.....!.....*6.....P.*.....@6.....@9.....9...@A.....46.u...X37.....P7.@.....8..''...`7.,.....T.....l.....@.. .....07.T.....text...e(6.....*6..... ..`.data...h....@6..d....6.....@....idata.....07.....6.....@..@.rsrc...@....P7.....6.....@..@.reloc..,...`7.... ...6.....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\ffmpeg.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2579968
Entropy (8bit):	6.889668352280003
Encrypted:	false
SSDEEP:	49152:GtGX4mOrucp9DHNj8CvJhAbEfvWyZOjp2:sGobp9DHNVvJhAAfCd2
MD5:	BE54EA68B64E4E48BFC511C431E722A0
SHA1:	808FBFA63E6C72264E4EE24F236A92EC6734CC81
SHA-256:	9F494FAE70E0D178A5FFCC7DD8B1821853862B35A39FE8EE1D9963F631841E1C
SHA-512:	B02DA4A3EABDFD190C19E4BAD3913BA097F2EEB3D20B868D68539737932F4C637880F76DA22ED37C2DFC2D92A7D4FC96D33511F7F24776B2279DA853425D00 6
Malicious:	false
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....a.....''!....$ ..4.....`9.....@A.... .....8S&.....0Y&.(.....8.....''&..... !&.....a .....Z&.....text...5# .....$ ..... ..`.rdata...E...@ ..F...(.....@..@.d ata.....&.....n&.....@....00cfg.....`8.....&.....@..@.tls.....p8.....&.....@....voltbl.....8.....&.....reloc.....8.....&.....@..B..... ....

C:\Program Files (x86)\Jabra\Direct4\icudtl.dat

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	10217376
Entropy (8bit):	6.2876877711974375
Encrypted:	false
SSDEEP:	196608:GEGwSv9AAQTgyTliXUxR0rHa93WhlU6tgLQH:G4KlQTlliXUxR0rHa93WhlU6tgL4
MD5:	2E7D2F6C3EED51F5ECA878A466A1AB4E
SHA1:	759BD98D218D7E392819107FAB2A8FD1CFC63DDF
SHA-256:	B62B7240837172959299DC3BE44FFFA83DC374353154ECA1612E1BDE330AA8FA
SHA-512:	0F1465E8EFE32B0EABA628A30BBB21254A05D80F4407A1434120A55FB928CF575B3879E1B7CF754CD19B23C262AE715FA84A8049073563CB38F1855BE7DB1124
Malicious:	false
Preview:	...'.....CmnD..... Copyright (C) 2016 and later: Unicode, Inc. and others. License & terms of use: http://www.unicode.org/copyright.html .1....A.....A.....A..`....A..... .A.....A..P....A...%...B...&...B..p&..(B...m..<B...n..OB...n..bB..Po..uB...o...B..`q...B...q...B.. r...B...r...B...s...B..pt...B...u...C..@v.. C...v..3C...x..FC...x..YC...z..lC..P|...C...| ...C...}...C..P~...C..0....C.....C.....C..`....D.....D.....*D.....=D.....ND..`...bD.....rD.....D..p....D..p....D.....D.....D..`....D.....E.....E..P...'E.....7E.....JE.....aE..0...qE..P... .E.....E.....E..@....E.....E.....E.../...F....&.'F..@.&.>F....&.UF....&.oF.. .&..F....&..F..P.&..F....&..F..0.&..F..PW(..G..."). G....).?G....).aG...A*..G....*..G....*..G....+..G.... +..G..0.+..H....+."H...V+.>H....+.\H..p.-.uH..p.-..H....-..H....-..H...P.-..H..P....H.....I.....%I..@...5I..@8..HI...8..[I...8..nI..09...I...9...I...9...I..0:...I...;...I..P]...I..@_...I.....J..... 'J.....<J..../.QJ..

C:\Program Files (x86)\Jabra\Direct4\jabra-direct.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123449232
Entropy (8bit):	6.985088222819441

Encrypted:	false
SSDEEP:	1572864:BDn/N3jQvA8zrweOHF/bHmZcAfevAokgrJt1/yY/g0p/3PIfa4RpkN71Z66ZSa9V:rzLXlRhIRpza9dXiR3w
MD5:	9D784E6AB3BC1C6B7FC6ECC956F481B0
SHA1:	98D2AE7AE6251EA4FCEC8E61E65F7BCD5BD8F929
SHA-256:	C18D18BE0FAD808F121B684D51ADBFEE5C6C7383825E72B69AB14B059082BBDF
SHA-512:	9B7C9CAF10D4F29177415006BD3B9978AE20213D47D4CFC60DAB9AECA0144A543FE56ADDE1C339CEEB76C1C59B0C5618E73741E38475F20903BF2DC5C90276D7
Malicious:	false
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....a.....".....(...^d.....@.....a \..@.....^.....`/.!.h....p_.....[..... a..2.....0.....].....!.....i..`.....text....'.....(..... ..`.rdata....+..@....+..,.....@..@.data.....<..P".....4".....@....00cfg..... _.....R'.....@..@.rodata.`....0_.....T'..... ..`.tls....E....@_.....^'.....@....voltbl.{....P_.....`'.....CPADinfo(....`_.....b'.....@....rsrc.....p_.....d'.....@..@.reloc...2.. a...2...).....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\libEGL.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	357888
Entropy (8bit):	6.5691137577215635
Encrypted:	false
SSDEEP:	6144:JEYlqgyp/a1fn9F3bsyy/0oTv1eqMuQ/4RQpV5+eMHm+liv:JEYlryp/M3bsyyb7SuQ/WQJWW
MD5:	D355712649261F04E35313F428784892
SHA1:	C9675CADF5D48AD933E4666538E60BBCFB817645
SHA-256:	7A2711D25A80633849CD8403A8B067C1D31D4A9670071BF9B9BE93A5E5B9D20F
SHA-512:	E533A0E8726CD495FCB6B273B6368B5FB9FEABF26660C9D2B4EDC22EE3B3EE8896FD00CEB33ABAFFBE886DBE9411036D1A9CF2C6C2A560C9210C871EF81428EA
Malicious:	false
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....a.....".....!.....X.....V.....@A.... .....[...(.....x.....5..$.....(.....P@.....l.....text...n..... ..`.rdata.....0.....@..@.data....3.. .0.....@....00cfg.....p.....4.....@..@.tls.....6.....@....voltbl.....8.....rsrc...x.....:.....@..@.reloc...5.....6...@..... ....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\libGLESv2.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6882304
Entropy (8bit):	6.77549184376196
Encrypted:	false
SSDEEP:	98304:5YIGfy80+u5gmtWsCfrpcYMADDxym5roFpCbo1rNRyOf47:5NopuPZ6pcSD1ym5dbyLnfY
MD5:	6B82B51B147D20E6DE09E499A7F24C95
SHA1:	FA4A2B3FFE11480B5FAEEDA07516B0292DF2FA4B
SHA-256:	1A201BB5C32F0A3FBB44E065386D733B12C918B1DD3456048C3FFED883DDF4E9
SHA-512:	388199E8A1432D473327501804E5F25A3540EB1EC84628501504C120EE88849010CEE656B7E66817008FD1B312A00C3DC5E29F52C158BE7B63456A69B317F409
Malicious:	false
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....a.....".....N..... QF.....`..... ....@A.....a.....b.d.....a.....a..... O.....l.b.T...$.a.@.....text.....N.....N..... ..`.rdata.....O.....N..... ...@..@.data...XY3.. c..f....b.....@....00cfg.....`e.....@..@.tls.....be.....@....voltbl.....de.....rsrc.....fe.....@..@.reloc..... .....le.....@..B..... .....

C:\Program Files (x86)\Jabra\Direct4\locales\am.pak	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	178779
Entropy (8bit):	4.97446111738704
Encrypted:	false
SSDEEP:	3072:AIyAPv4Oj0/92t7Rh4rgEkDvuhE8oeLt/ki7xVGMqyZJjhE+2WACT5x0kek97GY0:3yT51ueQRUHx30jH8+X
MD5:	522E5A1097344781CA089A14FF4E76C1
SHA1:	264A6A05D7F1D7D38BCEAFAF20337DC402233BCB

SHA-256:	68C1862F7859ABB1114E2BA352E95843C1B72436870BDE98BFF79A7B976E7FDD
SHA-512:	39F600A0D6B30D8D450A747BE69A886A2FC0E68CEBB74C9133D5DEB8032F0316F0343B07F844C5534275DFF5DEBB3AD2D0388295F87AB356D37290A03A1D85E1
Malicious:	false
Preview:	........-./.j..;..k..;..l..;..n..;..o..<..p..<..q..<..r.%<..s.6<..t.?<..v.T<..w.a<..y.g<..z.v<..|.|<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....=....(=....W=....v=....x=....|=.. ...=.....=.....=.....>....8>....X>....._>....b>....c>....o>....x>....>.....>.....>.....>.....>.....>.....>..*..?..+..?...,'?../.8?..0.R?..1..?..2..?..3..?..4..@..5.F@..6..@..7..@..>..A..?..A..N. 3A..g.@A..i.CA..j.GA..k.LA..l.TA..:RYA..;R.A..<R.A..=R.B..>R.B..?R.B..@R"C..ARKC..BR.C..CR.C..DRvE..ER.E..FR.E..GR.E..HR.E..IR.E..JR.F..KRRF..LR+G..MR nG..ORwG..PR.G..QR.G..RR.H..SR!H..TR:H..URpH..VR.H..\R.H..eR.I..gR3I..mRBI..nRYI..oRrI..qR.I..rR.J..sR7J..tRVJ..uRhJ..vR.J..wR.J..xR.K..zR\L..{RvL..|R.L..}R.L.. .R.L...R.M...R.N...R.N...R(O...R.O...RUP...RGQ...R^Q...RxQ...R.Q...R.S...R.T...R.U...RBV...RxV...R.V...R.V...R.V...R.V...R.W...R.W...R.W...R.X...R.X...R.X...R+Y...R.Y...R .Z...R.Z...R.Z...R|[...R.[...R.[...R.[...R.[...R.[...R%\...R&\...R<\...R?\...Rh\...R.\...R.\...RI]...Rf]...R.]

C:\Program Files (x86)\Jabra\Direct4\locales\ar.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	184455
Entropy (8bit):	5.056082907290393
Encrypted:	false
SSDEEP:	3072:9OUzH2KNRpqhXUJXFxnw+7zF+hFBM2S2xHMuZtE9T6N9/fpK1P/X21MgSENKKSIP:QUtNR8+7IrLMgSENuiTI1Zk
MD5:	65E3D23DE6D268D068B0CF3C88EB4F61
SHA1:	E78E7F1A3AB4ABC6BAC7E793E9AD8EDC6C71C485
SHA-256:	3B54952D90F37BD1D76E63464A9A5499FE1B8B0DB6E0F30CA029E0768B9C7B74
SHA-512:	91CD3B0924F11B3529B8371BF40329B574FCA43D3894A6D4015E68052BFC8C12D8595D15EB52B0D4D20FF91722808E0B48EF4C038759ED8D71FB8035621B4E52
Malicious:	false
Preview:	........&.6.j..;..k..;..l..;..n..;..o..;..p..<..q..<..r..<..s.(<..t.1<..v.F<..w.S<..y.Y<..z.h<..|.n<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....<....=....2=....i=.....=.....=.....=.....=.. ...=.....=.....>....&>....<>....R>....Y>....\>....f>....p>....~>.....>.....>.....>.....>.....>.....>..*..>..+..>...,..?../.+?..0.6?..1.v?..2..?..3..?..4..?..5..?..6.Y@..7.z@..>..@..?..@..N..@ ..g..@..i..@..j..@..k..@..l..@..:R.@..;R@A..<RtA..=RwB..>R.B..?R.B..@R.B..AR.C..BR^C..CR~C..DRmG..ER.G..FR.G..GR.G..HR.G..IR.G..JR.H..KRSH..LR,I..MRmI ..ORqI..PR.I..QR.I..RR.I..SR.J..TR,J..URGJ..VR\J..\R.J..eR.J..gR.J..mR.J..nR.K..oR*K..qR.K..rR.K..sR.K..uR.L..vR&L..wRPL..xR.L..yR.M..zRXN..{RvN..|R.N..}R.N...R .N...R.O...R.P...R.P...R.P...R.Q...R.Q...R8S...ReS...R.S...R.S...R.W...R.Y...RM[...R.[...R.[...R.\...R.\...R-\...RF\...R.\...RL]...R.]...R.^...RO^...Rm^...R.^...Rj_...R._...Re`...R .`...R.a...R.a...R.a...R.a...R.a...R.b...R6b...R\b...R]b...Rvb...R.b...R.b...R?c...Ric...R.c...R.c...RAd...RPd

C:\Program Files (x86)\Jabra\Direct4\locales\bg.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	198452
Entropy (8bit):	4.784894388458354
Encrypted:	false
SSDEEP:	6144:Vh7NaTBDnvbFnyZzrmLy8A/dW72vyPsUVwo:VjaTBDnv5nPLy8A/dW72vy2o
MD5:	D84F4C3C323B503FF927F2FBD3A5B078
SHA1:	BCD9457455C40252AA46FE4413E677F2037F6493
SHA-256:	19BA7F27E7950DF34CFECC8E3DFD68E64BD096141E8F54E4C4FB765450040C1A
SHA-512:	AF6F845ACE493AC0E5478F1ADD029A06453757767871E5B308161DDCC37618E6EFA1C26066B4FD1DCA3EEECCB7D61773175B1F4333DD42E4F06DF5B6559C646
Malicious:	false
Preview:	........O...j. <..k./<..l.:<..n.B<..o.G<..p.T<..q.Z<..r.i<..s.z<..t..<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....=.....=.....=.....=....Z=....|=.....=.....=.....=.....=.....=.. ...=.....=.....>....G>....u>.....>.....>.....>.....>.....>.....?....&?....8?....I?....I?....v?.....?.....?..*..?..+..?.,,.?../.<@..0.E@..1..@..2..@..3..@..4.*A..5._A..6..A..7..A..>.-B..?.<B..N.]B..g.kB..i.nB..j.rB..k.yB..l..B..:R.B..;R.B..<R.C..=R4D..>RJD..?R.D..@R.D..AR.D..BRDE..CRnE..DR.F..ER.G..FR!G..GR-G..HRZG..IRlG..JR.G..KR.H..LRXI..MR.I..OR.I.. PR.J..QR0J..SRvJ..TR.J..UR.J..VR.J..\RHK..eR`K..gR.K..mR.K..nR.K..oR.K..qRhL..rR.L..sR.L..tR.L..uR.M..vRBM..wR.M..xRpN..yR&O..zR.O..{R.P..|RMP..}RwP.. .R.P...R.Q...R.R...R.R...R.S...RwS...RTT...R.U...R.U...R%U...RaU...R W...R.W...R.X...R.Y...RBY...RLY...RnY...R.Y...R.Y...R.Y...R.Z...R.Z...R.[...R.[...R.\...Rq\...R#]...R .]...RB^...R.^...R._...R._...R._...R"`...RM`...R.`...R.`...R.`...R.`...R.`...RYa...R.a...R.b...R@b...R.b

C:\Program Files (x86)\Jabra\Direct4\locales\bn.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	255890
Entropy (8bit):	4.403450386880528
Encrypted:	false
SSDEEP:	1536:2rXkIYJj5gnPp2KJjyr98JMgqxpDwuDKOQv+h2mWmc:2rXkbi9mrQ
MD5:	4197C553BFADE7AA1E05FCABB761372A
SHA1:	EEFD8C48A19651B6C2B9D2044B3C36E2CFF9E196
SHA-256:	B375FD830D598819AF858BD17F8F84431725578FC4AE656DD28E95FDA2435585
SHA-512:	32B702A6452202B35A9A69D1A5F6D491EC4F2F47CA503997259F91CE93C5600F22D52CFCD793E1575EBA104ECED26226E98E0EA7B92DAF4010169B6175900486

Malicious:	false
Preview:	........1.+.j..;..k..;..l..;..n..<..o..<..p..<..q..<..r..<..s.?<..t.H<..v.]<..w.j<..y.p<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<....m=.....=.....=.....=.....>....!>.. ..%>....W>....s>.....>.....>.....>.....?....1?....4?....5?....K?....^?.....?.....?.....?.....?.....?....."@..*.@@..,.C@../.z@..0..@..1..A..2.(A..3.DA..4..A..5..A..6.yB..7..B..>..C..?..C ..N.QC..g.jC..i.mC..j.qC..k.vC..l..C..:R.C..;R.C..<R.D..=R.E..>R.E..?R5F..@RtF..AR.F..BR,G..CRXG..DR.J..ERSJ..FR\J..GRtJ..HR.J..IR.J..JR.K..KR.K..LR.L..MR.L..OR .M..PRdM..QR.M..RR.M..SR.M..TR.N..UR<N..VRQN..\R.N..eR.N..gR.O..mR'O..nRQO..oRwO..qR#P..rRvP..sR.P..tR.P..uR.P..vRDQ..wR.Q..xR.R..yR.S..zR.U..{R+U..|R .U..}R.U...R.V...RaW...RkY...R.Y...R.Y...R0Z...R.[...R.\...R.\...R.\...RD]...R.`...RTb...R.c...RLd...R.d...R.d...R.d...R.d...R.e...Rue...R.f...R.f...R.g...R.h...RQh...Ryh...RVi...R .j...R.j...R'k...R.l...R.l...R.l...R.l...R.l...R+m...R.m...R.m...R.m...R.m...R.m...R`n...R.n...R.o...R.o...R.o

C:\Program Files (x86)\Jabra\Direct4\locales\ca.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	124679
Entropy (8bit):	5.418470066988079
Encrypted:	false
SSDEEP:	3072:xrXKs1DaccguH65rqx0hmSBL8l/oT6nm1VhNO54f1fXiUUpYEHGPXf410ozRhqP2:tBbcgco73O56XiUUpY/PXfc0yaYnwAkI
MD5:	25D4E7BBE06A0D105E9AC3489492B066
SHA1:	67A7459AA3FBC1A35F475321DDE84BB2392DEE5F
SHA-256:	152755D4FB86EB089FD59F4124F6F3407A591AD2E735FF0770F22F0E20B4A56A
SHA-512:	6C867C7979F2E9F852F907591EED027C244F313DB71B1A4C7EEC65301E9EE7CA4F8A5F80C5F01300741E95BD94BDD23B624125C2C0BDAC9C67EA40948DAC1F E
Malicious:	false
Preview:	........P...j."<..k.1<..l.<<..n.D<..o.I<..p.V<..q.\<..r.k<..s.|<..t..<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....=.....=.....=.....=.....=....9=....S=....l=.....=.....=.....=.....=.. ...=.....=.....=.....=.....>.....>....,>....3>....6>....7>....@>....I>....Q>....V>....\>....n>....t>....|>.....>..*..>..+..>.,..>../..>..0..>..1.*?..2..:?..3.J?..4.i?..5..?..6..?..7..?..>..?..?..?..N. .@..g..@..i..@..j..@..k..@..l.$@..:R'@..;RT@..<Rv@..=R.A..>R.A..?RFA..@RaA..AR~A..BR.A..CR.A..DR.B..ER.B..FR.B..GR.B..HR.B..IR.B..JR.B..KR0C..LR.C..MR .C..OR.D..PR.D..QRAD..RRgD..SRoD..TR.D..UR.D..VR.D..\R.D..eR.D..gR.E..mR.E..nR$E..oR3E..qR}E..rR.E..sR.E..tR.E..uR.E..vR.E..wR.F..xR.F..yR.G..zR.G..{R .G..|R.G..}R.G...R.H...R.H...RbI...RxI...R.I...R.I...RMJ...R.J...R.J...R.J...R.J...R.L...R.L...R.M...RWM...R.M...R.M...R.M...R.M...R.M...R.M...R-N...R^N...R.N...R.N...R.N ...R4O...R.O...R.O...REP...RwP...R.Q...R.Q...R#Q...R&Q...R)Q...RIQ...RgQ...R|Q...R}Q...R.Q...R.Q...R.Q...R.Q...R.R...RTR

C:\Program Files (x86)\Jabra\Direct4\locales\cs.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	128113
Entropy (8bit):	5.8125338078305155
Encrypted:	false
SSDEEP:	3072:TejzoGFJ+17jN6lD+g+5XZ/VGm8Q+ndbx:TYiN6lDu/Vx8QYdbx
MD5:	B63984C00E9BD3A9B19B0B018D378FE8
SHA1:	2664A3D55A2B55CCE48CB5B95E726EBD68200C5E
SHA-256:	CC6D83368650EF16106B5387817A35543A7FC9978DC848CCC48F62AB1095CFFD
SHA-512:	62771CF5001CDDED38DFBBEB8248DFA82BC944592D6D17D58406227D13784D8A1D7809F8D53A1FD0641603795973F0BA107641F0A395CA5A55D009240090D08
Malicious:	false
Preview:	........D...j..<..k..<..l.$<..n.,<..o.1<..p.><..q.D<..r.S<..s.d<..t.m<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<....2=....B=....T=....f=....{=.... }=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>.....>....(>....4>....9>....?>....\>..*.f>..+.i>..,..>../..>..0..>..1..>..2..>..3..?..4."?..5.C?..6..?..7..?..>..?..?..?..N. .?..g..?..i..?..j..?..k..?..l..?..:R.?..;R.@..<R+@..=R.@..>R.@..?R.@..@R.A..AR.A..BRWA..CReA..DR7C..ERKC..FRRC..GRXC..HRmC..IRwC..JR.C..KR.C..LR9D..MR YD..OR_D..PR.D..QR.D..RR.D..SR.D..TR.D..UR.E..VR.E..\RFE..eRQE..gRdE..mRkE..nRyE..oR.E..qR.E..rR.E..sR.F..uR.F..vR%F..wRHF..xR.F..yR.G..zR.G..{R.G..|R .G..}R.G...R.G...RyH...R/I...R>I...RRI...R.I...R.J...R.J...R.J...R.J...R.K...R.M...R.M...R.N...R.N...R.O...R O...R.O...R7O...RDO...RkO...R.O...R.O...RGP...R`P...RsP...R.P ...R.Q...R>Q...R.Q...R.Q...RER...RMR...RUR...R\R...R_R...RuR...R.R...R.R...R.R...R.R...R.R...R.R...R.R...R.S...R`S...RvS

C:\Program Files (x86)\Jabra\Direct4\locales\da.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	116655
Entropy (8bit):	5.42451803709918
Encrypted:	false
SSDEEP:	1536:aXU2vOESB3QxjxnFg5JmFT/I+5MGA/4v8pOmPEHhIGaH:UU2vyQ9xnKmFTg+5SwPIH
MD5:	B40365DE752513B202F1D781EF37614F
SHA1:	67AAB464F8F9863805E15328BCD60B3BB34EB9A3
SHA-256:	E9A4763DCE8E08FB13EBF28F6D0071529ADFAC6BB71C5AF01BC975EB9A47F01C
SHA-512:	DFFF3795908536034B07E90B33533C0A7313CF1DB6F6080462F808DC782AB44A6A332E00EEEFC6EF7A7B21651D9FB016640E1CF81C89D9CFF33B69D041A3822E
Malicious:	false

Preview:	.....K...j..<..k.'<..l.2<..n.:<..o.?<..p.L<..q.R<..r.a<..s.r<..t.{<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....<.....=.....=.....=..../=....==....M=....a=....z=....|=.....=.. ...=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>.....>....1>..*.;>..+.>>...,\>../.l>..0.v>..1..>..2..>..3..>..4..>..5..>..6..?..7./?..>.B?..?.K?..N.Y?..g.d?.. i.g?..j.k?..k.p?..l.u?..:Rz?..;R.?..<R.?..=R|@..>R.@..?R.@..@R.@..AR.@..BR.@..CR.A..DRRB..ERnB..FRuB..GR{B..HR.B..IR.B..JR.B..KR.B..LRzC..MR.C..OR.C.. PR.C..QR.C..RR.D..SR.D..TR.D..UR.D..VR:D..\RrD..eRyD..gR.D..mR.D..nR.D..oR.D..qR.D..rR.E..sR"E..tR2E..uR8E..vRNE..wRnE..xR.E..yR0F..zR.F..{R.F..|R.F.. }R.F...R.F...RdG...R.H...R.H...R$H...ROH...R.H...R.I...R7I...RFI...R`I...R.J...R.K...R.K...R.K...R.K...R.K...R.L...R.L...R.L...ROL...R.L...R.L...R.M...RGM...RXM...R.M...R .M...R.N...ReN...R.N...R.O...R$O...R*O...R-O...R?O...RUO...RgO...RhO...RvO...RyO...R.O...R.O...R.O...R.O...R&P...R8P

C:\Program Files (x86)\Jabra\Direct4\locales\de.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	125889
Entropy (8bit):	5.481390677133355
Encrypted:	false
SSDEEP:	1536:5EU9mAaoQsqXghFlahUbnLKbF1CfEO5emQUvehSbbXwqPHxQ1NlkGfkhI9Z4C2Dl:5gcQstjhUzLKVnS3w2H8NrCDM/rnCSE
MD5:	3F101E4C28AACC84DCC0693DB76DAA00
SHA1:	C40B4028C0E109DFBBCBBC6B18E9132169736E06
SHA-256:	C47776ECD40FA3CD3C8342A77AC5C841778DE33B82AF05BC22CF426E0D0FC220
SHA-512:	F57CF6F4703B0B9A85F1A6683388756E0827152F2CBA006716F9B87451F4E9CAA124CB33DE0715F3B6564004CBD787006ABA100245BFC397DDD015297DEF902B
Malicious:	false
Preview:	.....@.j..;..k..;..l..;..n..;..o..;..p..;..q..;..r..<..s..<..t..<..v.2<..w.?<..y.E<..z.T<..|.Z<..}.l<....t<....y<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....=.....=....-=..../=....3=.. ..F=....O=....d=....z=....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>....#>....9>..*.B>..+.E>..,c>../.t>..0.|>..1..>..2..>..3..>..4..>..5..?..6.L?..7.`?..>.t?..?.|?..N. .?..g..?..i..?..j..?..k..?..l..?..:R.?..;R.?..<R.@..=R.@..>R.@..?R.@..@R.A..AR!A..BR_A..CRvA..DRwB..ER.B..FR.B..GR.B..HR.B..IR.B..JR.B..KR.C..LR.C..MR.C..OR.C.. PR.D..QR!D..RR@D..SRFD..TR\D..URwD..VR.D..\R.D..eR.D..gR.D..mR.D..nR.E..oR.E..qRbE..rR.E..sR.E..tR.E..uR.E..vR.E..wR.E..xR~F..yR.G..zR.G..{R.G..|R.G.. }R.H...R.H...R.H...R.I...R.I...R.I...R.I...R\J...R.J...R.J...R.J...R.J...R.L...R.L...R%M...R~M...R.M...R.M...R.M...R.M...R.M...R.N...RaN...R.N...R.O...R(O...R9O...R]O...R .O...R.P...RpP...R.P...RBQ...RMQ...RRQ...RVQ...RnQ...R.Q...R.Q...R.Q...R.Q...R.Q...R.Q...R.Q...R.Q...R&R...RgR...R~R

C:\Program Files (x86)\Jabra\Direct4\locales\el.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	218261
Entropy (8bit):	4.866027006419147
Encrypted:	false
SSDEEP:	6144:N73vCi+6FMkDuvmtF5IKRrl3Cp4o3/UzFMeF+f9I2hl361YlXSTzG:9vCi+6FMkDuvmtF5IKRrl3Cp4o3/UzFq
MD5:	BEABB3BB4E26E939809153603932CE6F
SHA1:	9FAF16FE40690FDC1256620967F819E203238801
SHA-256:	F83EB97D6DDD4E6EE38F4B3F3E8BA9ECF5B712E37822162A91D0D8A29C1450F2
SHA-512:	111F1F097CEECA20FF293881DA9FEC2B6E57F26B819A423CC6CC3A53A628622ABCB5EFBFA30B85F7BFC9E9533FC75FC05588FD79333EEF55AE1C7815852E51 D1
Malicious:	false
Preview:	.....D...j..<..k..<..l.$<..n.,<..o.1<..p.><..q.D<..r.S<..s.d<..t.m<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<....Y=.....=.....=.....=.....>.....>.....>.. ...>....C>....f>.....>.....>.....>.....?.....?.....?.....?....-?....G?....Y?....i?....|?.....?.....?.....?.....?..*..?..+..?.,...@../.l@..0..@..1..A..2..A..3.FA..4..A..5..A..6.PB..7.xB..>..B..?..B..N. .B..g..B..i..B..j..C..k..C..l..C..:R.C..;RpC..<R.C..=R.D..>R.D..?R?E..@RfE..AR.E..BR.F..CR,F..DR.G..ER.H..FR.H..GR.H..HRSH..IReH..JR.H..KR.H..LR+J..MR.J..OR.J.. PR.K..QR%K..RRYK..SRiK..TR.K..UR.K..VR.K..\RkL..eR.L..gR.L..mR.L..nR.L..oR.L..qR.M..rR.M..sR.N..tR*N..uRBN..vR.N..wR.N..xR.O..yR.P..zR.Q..{R.Q..|R6R.. }R]R...R.R...R.S...R7U...RRU...RvU...R.U...R.V...RoW...R.W...R.W...R.W...R.Y...R.Z...R.[...RM\...R.\...R.\...R.\...R.\...R.\...R4]...R.]...R.^...R.^...RS_...Rt_...R._...R.`...RHa.. .R.b...Rfb...R}c...R.c...R.c...R.c...R.c...R.c...R.d...R/d...R0d...ROd...RRd...R.d...R.d...R.d...R.e

C:\Program Files (x86)\Jabra\Direct4\locales\en-GB.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	102515
Entropy (8bit):	5.467867231389823
Encrypted:	false
SSDEEP:	1536:6O7p/MB5xbWQWGvjrD0KkK4Rr3qS65iBqgESOiJedMJrVuh5IJVfm3ggl+LXIcn:BqbpvjEK2TBqgL65b3ggl+L9
MD5:	3CA86CAF200C1A33279BCADC352CAA90
SHA1:	9729D8E2824D914778883426B980BC9AFBCA4FB8
SHA-256:	CA42D6CCE0E64FBA4F10F61F393AC74E63364F86A7FA62C0632F29950EE0E5F5
SHA-512:	6F9269BCE8B1B15775ACE3E33888FE64303E43C226044C1ACE002F0AFB6A56B080004AC76D0598151DB18C2932F43A9D9C0516E17EEC71A305D99973864B154(
Malicious:	false

<table>
<tr><td>Preview:</td><td>........P...j."<..k.1<..l.<<..n.D<..o.l<..p.V<..q.\<..r.k<..s.|<..t..<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....=.....=.....=.....=.....=....8=....E=....T=....d=....u=....w=....
{=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>.....>.....>.....>..*.6>..+.9>..,.W>../.h>..0.q>..1..>..2..>..3..>..4..>..5..>..6..?..7.&?..>.;?..?.C?..N.
R?..g.[?..i.^?..j.b?..k.g?..l.n?..:Rs?..;R.?..<R.?..=R.@..>R.@..?R(@..@R6@..ARE@..BRr@..CR.@..DR.A..ER@A..FREA..GRKA..HRTA..IR\A..JRnA..KR.A..LR.A..MR
.B..OR.B..PR#B..QR+B..RRAB..SRIB..TR\B..URxB..VR.B..\R.B..eR.B..gR.B..mR.B..nR.B..oR.B..qR5C..rRQC..sR[C..tRgC..uRkC..vRzC..wR.C..xR.C..yRLD..zR.D..{R
.D..|R.D..}R.D...R.D...RxE...R'F...R6F...REF...RhF...R.F...R+G...R:G...RIG...RbG...RGH...R.H...R4I...ReI...R.I...R.I...R.I...R.I...R.I...R.I...R.I...R%J...R|J...R.J...R.J...R.J...R
.K...R\K...R.K...R.K...RDL...RKL...RQL...RVL...RZL...RlL...R.L...R.L...R.L...R.L...R.L...R.L...R.L...R.L...R2M</td></tr>
</table>

C:\Program Files (x86)\Jabra\Direct4\locales\en-US.pak

<table>
<tr><td>Process:</td><td>C:\Windows\System32\msiexec.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>103364</td></tr>
<tr><td>Entropy (8bit):</td><td>5.460354904891128</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:iJMRBUgPvpWYRt0FASED0FhFL2tr/4Sx5dBqgDSO0JedMVrBnh6NVfD3ggl+sZ4J:dRppJ8ASTheZBqgmT6/3ggl+sxwh</td></tr>
<tr><td>MD5:</td><td>B6A2C492D2BC0278F350201BDB66EA21</td></tr>
<tr><td>SHA1:</td><td>9C2652CF0BF720C41263C675DB5C342C08F66B35</td></tr>
<tr><td>SHA-256:</td><td>A453FE4E06016AAC08B58A1569074F3BE985A730B5CA1E345CB3E286B042ACF5</td></tr>
<tr><td>SHA-512:</td><td>CB39C7E9C58CDF23900014EB589C50E495B80E0CBC6A369110F84E96BF2A47E9057DF1914287990C04D7A5FD3119EABB30642492D0A50D359FF7D2305CB4AE2</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>........]...j.<<..k.K<..l.V<..n.^<..o.c<..p.p<..q.v<..r..<..s..<..t..<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....=.....=.....=.....=....!=....(=....)=....*=....R=...._=....n=....~=.....=.....=.....=..
...=.....=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>.....>.... >....+>..../>....6>....H>..*.P>..+.S>..,.q>../..>..0..>..1..>..2..>..3..>..4..>..5..>..6./?..7.??..>.T?..?.\?..N.
k?..g.t?..i.w?..j.{?..k..?..l..?..:R.?..;R.?..<R.?..=R.@..>R#@..?RA@..@RO@..AR^@..BR.@..CR.@..DRWA..ERiA..FRnA..GRtA..HR}A..IR.A..JR.A..KR.A..LR.B..MR
,B..OR2B..PRLB..QRTB..RRjB..SRrB..TR.B..UR.B..VR.B..\R.B..eR.B..gR.B..mR.C..nR.C..oR.C..qR]C..rRyC..sR.C..tR.C..uR.C..vR.C..wR.C..xR.D..yRkD..zR.D..{R
.D..|R.D..}R.E...R.E...R.E...RIF...RXF...RgF...R.F...R.F...RYG...RhG...RsG...R.G...R.H...R.I...R.I...R.I...R.I...R.I...R.I...R.I...R.I...R.J...RRJ...RwJ...R.J...R.J...R.J...R.K...R
qK...R.K...R.K...R.L...R.L...R.L...R.L...R.L...R.L...R.L...R.L...R.L...R.L...R.L...R.L...R.M...R4M...RNM...R.M</td></tr>
</table>

C:\Program Files (x86)\Jabra\Direct4\locales\es-419.pak

<table>
<tr><td>Process:</td><td>C:\Windows\System32\msiexec.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>123269</td></tr>
<tr><td>Entropy (8bit):</td><td>5.3843207196837675</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:UKIZXoOhjRbKZr4hJzsxaXG0BM4uddPcHYKC2Kb/0PWFsMH5Bth/VZQWrYHh+:fIxokl6khIWu5b0B+</td></tr>
<tr><td>MD5:</td><td>961D4613247A7FFF2CA6EF333CCAE7E3</td></tr>
<tr><td>SHA1:</td><td>4D4F0894966E4FB1DCB648C7E6A341ACFAAEF796</td></tr>
<tr><td>SHA-256:</td><td>AE6D834ADFAAF9B1AE60513C232D98F59496E93436EED2114FE1F322A5AA3DA8</td></tr>
<tr><td>SHA-512:</td><td>9B68031F565336DDE3CE6D13C9AEE89E1091A13CCE318232A6328C9978C556CF59044752EE6A99E0ACCDD8B5C0B46B85CB9C591A40DF6FB4F7061EA3460B7C
BF</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>........M...j..<..k.+<..l.6<..n.><..o.C<..p.P<..q.V<..r.e<..s.v<..t..<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....=.....=.....=.....=....0=....B=....Q=....f=....}=....
.=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>.....>.....>.....>....&>....,>....3>....D>....J>....R>....t>..*..>..+..>..,..>../..>..0..>..1..?..2..?..3.(?..4.F?..5.i?..6..?..7..?..>..?..?..?..N.
.?..g..@..i..@..j..@..k..@..l..@..:R.@..;RK@..<Rr@..=R"A..>R*A..?RNA..@R`A..ARsA..BR.A..CR.A..DR.B..ER.B..FR.B..GR.B..HR.B..IR.B..JR.B..KR/C..LR.C..MR
.C..OR.D..PR-D..QR=D..RReD..SRnD..TR.D..UR.D..VR.D..\R.D..eR.D..gR.D..mR.D..nR.E..oR(E..qRsE..rR.E..sR.E..tR.E..uR.E..vR.E..wR.F..xR.F..yR.G..zR.G..{R
.G..|R.G..}R.G...R.H...R.H...RhI...R.I...R.I...R.I...RGJ...R.J...R.J...R.J...R.J...R.K...RLL...R.L...R0M...RTM...R\M...RhM...RsM...R.M...R.M...R.M...R!N...R.N...R.N...R.N
...R.N...RUO...R.O...R.P...R-P...R.P...R.Q...R.Q...R.Q...R.Q...R,Q...RCQ...RVQ...RWQ...RiQ...RlQ...R.Q...R.Q...R.Q...R,R</td></tr>
</table>

C:\Program Files (x86)\Jabra\Direct4\locales\es.pak

<table>
<tr><td>Process:</td><td>C:\Windows\System32\msiexec.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>124460</td></tr>
<tr><td>Entropy (8bit):</td><td>5.361878868943351</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:AWkJ0NIsQLDdokwF7/ev4dYP/XFKqh3vijTagFW9XlhgoMhSKW9wfQ1weJ:AWrNIsQfekwF72RPMs5ayuoCg</td></tr>
<tr><td>MD5:</td><td>D70507A4B5EDA648D2787C50B08962BD</td></tr>
<tr><td>SHA1:</td><td>43D15A408F3F048A695B8310A934C4B4ACE476DE</td></tr>
<tr><td>SHA-256:</td><td>00C7A1E751599C9FA28C6D61D4F7150D98D22708932173E9D18CA385ED06BA79</td></tr>
<tr><td>SHA-512:</td><td>15A2C63E2EC741F1F3B3308403D2DE467123316C02B143EF883C897B58CB3B8ED5963DC30FF088FD1DD69EE51D5AC559816ECB8314F7BE299091FD8F9385934</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
</table>

Preview:	.....Q...j.$<..k.3<..l.><..n.F<..o.K<..p.X<..q.^<..r.m<..s.~<..t..<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....=.....=.....=.....=.....=....A=....T=....d=....y=.....=.... .=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>.....>....(>....1>....:>....@>....G>....X>....^>....f>.....>..*..>..+..>..,..>../..>..0..>..1..?..2..?..3.-?..4.K?..5.j?..6..?..7..?..>..?..?..?..N. .?..g..@..i..@..j..@..k..@..l..@..:R%@..;RO@..<Rl@..=R.A..>R.A..?R;A..@RMA..AR`A..BR.A..CR.A..DRoB..ER.B..FR.B..GR.B..HR.B..IR.B..JR.B..KR.C..LR.C..MR .C..OR.C..PR.D..QR'D..RRPD..SRYD..TRkD..UR.D..VR.D..\R.D..eR.D..gR.D..mR.D..nR.E..oR'E..qRsE..rR.E..sR.E..tR.E..uR.E..vR.E..wR.F..xR.F..yR.G..zR.G..{R .G..|R.G..}R.G...R.G...R.H...R0I...RGI...R\I...R.I...R.I...RfJ...RnJ...R.J...R.J...R.K...R&L...R.L...R.L...R.M...R.M...R)M...R3M...RCM...RqM...R.M...R.M...R`N...R.N...R.N ...R.N...RZO...R.O...R.P...RCP...R.P...R.P...R.P...R.P...R.Q...R.Q...R4Q...RJQ...RKQ...R]Q...R`Q...R{Q...R.Q...R.Q...R.R

C:\Program Files (x86)\Jabra\Direct4\locales\et.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	112339
Entropy (8bit):	5.457796630510558
Encrypted:	false
SSDEEP:	1536:f2wPznXWSPlv3DyE4x8yoRjsg9jvuLEC8hu6HpsPQ3rJ:frX9PlvGE4x87j2LSu6SPQ39
MD5:	6EEEF27E49CCE6E1E54EC9AFB4400BFC
SHA1:	68F1889306CEE7CF8CBD83AA954FDA1A7C4522FB
SHA-256:	E352F03C09C1B5F396E1580BDD7911EFE525F7CA306A4D04391724F20E8B3A21
SHA-512:	AA6E47844EC346E479C0EBB2F791869A0FE74F3A86AFEB5FBCCECACD1EDF8207FF8075218FD95C9BFC006F22722CD4D5DCD5F36157401F08921C511ADF5845 34
Malicious:	false
Preview:	.....U...j.,<..k.;<..l.F<..n.N<..o.S<..p.`<..q.f<..r.u<..s..<..t..<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....=.....=.....=.....=.....=.....=.....L=....\=....n=.....=.....=.....=.....=.. ...=.....=.....=.....=.....=.....=.....>.....>.....>.....>.....>....&>....>....1>....9>....D>....J>....P>....i>..*.t>..+.w>..,..>../..>..0..>..1..>..2..>..3..>..4..?..5.3?..6.k?..7..?..>..?..?..?..?..N. .?..g..?..i..?..j..?..k..?..l..?..::R.?..;R.@..<R.@..=R.@..>R.@..?R.@..@R.A..AR!A..BRaA..CRmA..DR@B..ERUB..FR\B..GRhB..HRzB..IR.B..JR.B..KR.B..LRDC..MR mC..ORrC..PR.C..QR.C..RR.C..SR.C..TR.C..UR.D..VR.D..\RHD..eRRD..gRaD..mRiD..nR~D..oR.D..qR.D..rR.E..sR.E..tR!E..uR'E..vR?E..wRcE..xR.E..yR*F..zR.F..{R .F..|R.F..}R.F...R.F...RuG...R.H...R&H...R?H...RqH...R.H...RNI...R^I...RlI...R.I...R.J...R.K...RhK...R.K...R.K...R.K...R.K...R.K...R.K...R.L...RUL...RxL...R.L...R.L...R.M ...R3M...R.M...R.M...R.N...R5N...R.N...R.N...R.N...R.N...R.N...R.N...R.O...R.O...R.O...R.O...R6O...RhO...R.O...R.O...R.O

C:\Program Files (x86)\Jabra\Direct4\locales\fa.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	175570
Entropy (8bit):	5.150004308450072
Encrypted:	false
SSDEEP:	3072:P3WGBFHUC+Xv94Rawpa8k+6NS9/W2ESEmbzR2XQmN4o67sbdxv7fhb8YIO/ECuDj:PW+j+XV4Rawpa8k+6NS9/W2ESEmbV2X0
MD5:	567A54A71296CE5B500DED0F18F47722
SHA1:	C11E654D088352AB80B91382A2630D60EDCF5C6A
SHA-256:	73E17A4A96EFF210349B7349E9ECA2CAA3C88A1E28C5A5D45D129791BF47E636
SHA-512:	16DE38F742A5DCE0B9A89A909363CD78E1EF81C66A290596C53E60A5074EF65ECFBCE779863B8F566494250989D07903FAC2D282CC99D4221326980E61372494
Malicious:	false
Preview:	.....H.j..;..k..;..l..;..n..;..o..;..p..;..q..;..r..;..s..<..t..<..v."<..w./<..y.5<..z.D<..|.J<..}.\<....d<....i<....q<....y<.....<.....<.....<.....<.....<.....<.....=....@=....g=....j=....r=....x=.. ...=.....=.....=.....=.....=.....>.....>....%>....(>....9>....J>....X>....`>....g>....{>.....>.....>.....>..*..>..+..>..,..>../. ?..0..?..1.r?..2..?..3..?..4..?..5..?..6.W@..7..@..>..@..?..@..N..@..g..@..i. .@..j..A..k..A..l..A..:R.A..;RnA..<R.A..=R.B..>R.B..?R.B..@R.C..AR8C..BR.C..CR.C..DR.E..ER.E..FR.E..GR.E..HR.E..IR.E..JRMF..KR.F..LRrG..MR.G..OR.G..PR .H..QR3H..RRiH..SRsH..TR.H..UR.H..VR.H..\RCI..eRTI..gRrI..mR|I..nR.I..oR.I..qR.J..rRSJ..sRnJ..tR.J..uR.J..vR.J..wR"K..xR.L..yR.L..zR.M..{R.M..|R.N..}R-N...RTN...R? O...RvP...R.P...R.P...R.Q...R.Q...R.R...R.R...R.S...R.U...R.V...RvW...R.W...R.X...R/X...R=X...RTX...R.X...R.Y...RvY...R.Z...R.Z...RUZ...R.Z...R.[...R.[...R.\...RR\...R.].. .R(]...R.]...R4]...R^]...R|]...R.]...R.]...R.]...R.]...R.]...R$^...RX^...R.^...R._...R=_...RL_...Rt_

C:\Program Files (x86)\Jabra\Direct4\locales\fi.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	114567
Entropy (8bit):	5.4247269157874545
Encrypted:	false
SSDEEP:	3072:tjLtQlWmiTJqWUEvIj+EE/18olzRj/xm0PjNM1z0gZqmnf:hl97EE/18o//J47f
MD5:	C460CA8B7F13C098E77AE10467E75460
SHA1:	21AEA67B989BE5D62EB63A5258CCDDD4FBF745D9
SHA-256:	5FADF7152337659F9EF833FB99D9FC73257409D231BE7D0DEAC95AC6F0DE3C39
SHA-512:	439755820EFDA2F77B4DC9A9911570B040D1DC3B15F6B2E805430A9683F04743B024DFE3024045E5D917C5568360AB14D3760D8D4102C4B22C2668EA212A5A5C
Malicious:	false

Preview:

........A...j..<..k..<..l..<..n.&<..o.+<..p.8<..q.><..r.M<..s.^<..t.g<..v.|<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....=.....=....?=....R=....k=....
m=....q=....v=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>....!>....2>..*.:>..+.=>..,.[>../.}>..0..>..1..>..2..>..3..>..4..>..5..?..6.P?..7.o?..>..?..?..?..N.
.?..g..?..i..?..j..?..k..?..l..?..:R.?..;R.?..<R.@..=R.@..>R.@..?R.@..@R.A..AR A..BRRA..CR_A..DR>B..ERUB..FR\B..GRdB..HRuB..IR~B..JR.B..KR.B..LR,C..MR
YC..ORdC..PR.C..QR.C..RR.C..SR.C..TR.C..UR.C..VR.C..\R D..eR)D..gR7D..mR?D..nRUD..oRdD..qR.D..rR.D..sR.D..tR.D..uR.D..vR.E..wR7E..xR.E..yR.F..zRlF..{R
.F..|R.F..}R.F...R.F...RcG...R.H...R+H...RCH...RvH...R.H...R;I...RNI...R[I...R~I...RjJ...R.J...RVK...R.K...R.K...R.K...R.K...R.K...R.K...R.K...R=L...R`L...R.L...R.L...R.L...R.L...R
SM...R.M...R.M...R.M...RlN...RtN...R|N...R.N...R.N...R.N...R.N...R.N...R.N...R.N...R.N...R.O...R@O...RsO...R.O

C:\Program Files (x86)\Jabra\Direct4\locales\fil.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	128265
Entropy (8bit):	5.192924735393796
Encrypted:	false
SSDEEP:	1536:K/30Y8ticQwdYffV7LelC3czfNvuNpEWnG/9lKgWAM64CzPEhhYkZp36/Q1DGdXK:030YnfwdENmCOKgWAaCzy7/6/6OX25
MD5:	023E1C6DC11700FE55D788305E7340CD
SHA1:	E6494FFE95933D618CAD050F2E363149E8C6D48F
SHA-256:	E318914046B66D1C77E0AAF17547FB757313ADF68F244792DE93EC1C8820BB2B
SHA-512:	9F4A793D05EC3B1E605142C3B2B3269C5E49254E5E903B20A4523D7F9447992CE44707315F9550E7BE6617979CFAF7E84D72C5C12D73E2001C4D4D908DFDACF
Malicious:	false

Preview:

........V...j..<..k.=<..l.H<..n.P<..o.U<..p.b<..q.h<..r.w<..s..<..t..<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....=.....=.....=.....=.....=.....=....C=....P=....e=....{=.....=....
.=.....=.....=.....=.....=.....=.....=.....=.....>.....>.... >....!>....+>....3>....>>....C>....L>....]>....d>....l>.....>..*..>..+..>..,..>../..>..0..>..1..?..2.(?..3.0?..4.N?..5.o?..6..?..7..?..>..?..?..?..N.
.?..g..@..i..@..j..@..k..@..l..@..:R.@..;RS@..<Rj@..=R.@..>R.@..?R&A..@R9A..ARPA..BR.A..CR.A..DR.B..ER.B..FR.B..GR.C..HR.C..IR.C..JR8C..KR`C..LR.C..MR
.D..OR.D..PR:D..QRED..RRcD..SRmD..TR.D..UR.D..VR.D..\R.D..eR.D..gR.E..mR.E..nR.E..oR.E..qR.E..rR.E..sR.E..tR.E..uR.E..vR.E..wR.F..xRxF..yR.F..zRYG..{R
oG..|R.G..}R.G...R.G...RfH...R(I...R:I...RSI...R.I...R.I...R.J...R.J...R.J...R.J...RGL...R.M...R.M...R.M...R.N...R$N...R8N...R@N...RON...RuN...R.N...R.N...RMO...RlO...R.O
...R.O...R.P...RkP...R.P...R.P...R.Q...R.Q...R.Q...R.Q...R.Q...R.Q...R.Q...R.Q...R.Q...R.R...R.R...R0R...RZR...RyR...R.R

C:\Program Files (x86)\Jabra\Direct4\locales\fr.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	133889
Entropy (8bit):	5.388106276450332
Encrypted:	false
SSDEEP:	3072:xhyIhlRCoM5J3cQR5bJK9GR+0dZ85ow1xBMpQzpRHD+IwKByroFDuFcVXQSxwgAE:xhhfRe5RcQR5daGR+0dZ85owvBMpkRHt
MD5:	CD689820DE5F5A12D820EC9B9BFC4738
SHA1:	5CF1B8B255C53849FAE015CF9DE5A30FB80E69E5
SHA-256:	83C7C6D4A6B7076E0FFFFB7932B837ABD0A0D08522A7A061645E10C0B7E51CFB
SHA-512:	5219F12A7A58D7751640217E49C54749EF7849DC016A9029046FD7A5C628B07E220DF92ABDD77CA491A8119E01BDECE968CDB7405442544BA941E70A4E78ECB
Malicious:	false

Preview:

........B...j..<..k..<..l. <..n.(<..o.-<..p.:<..q.@<..r.O<..s.`<..t.i<..v.~<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....=....)=....7=....I=....X=....Z=....^=..
..e=....r=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>....">....(>..../>....P>..*.Z>..+.]>..,.{>../..>..0..>..1..>..2..>..3..>..4..?..5.8?..6..?..7..?..>..?..?..?..N..?..g..?..
i..?..j..?..k..?..l..?..:R.?..;R.@..<R>@..=R.@..>R.@..?R.@..@R.A..AR.A..BRvA..CR.A..DR.B..ER.B..FR.B..GR.B..HR.B..IR.B..JR%C..KRMC..LR.C..MR.D..OR.D..
PR4D..QRED..RRgD..SRpD..TR.D..UR.D..VR.D..\R.E..eR.E..gR,E..mR7E..nRNE..oRbE..qR.E..rR.E..sR.E..uR.F..vR,F..wR_F..xR.F..yRtG..zR.H..{R'H..|RMH..}R]H..
.RxH...R.I...R.I...R.I...R.J...R<J...R.J...R.K...R.K...R.K...R.K...R.M...RfN...R"O...RkO...R.O...R.O...R.O...R.O...R.O...RDP...RtP...R.P...R.Q...R.Q...RPQ...R.Q...R;R...R
.R...R.R...R.S...R.S...R.S...R.S...R.S...R.S...R.S...R.S...R.S...R.S...R.T...R T...RNT...RrT...R.T...R.T...R.T

C:\Program Files (x86)\Jabra\Direct4\locales\gu.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	246383
Entropy (8bit):	4.44286641381821
Encrypted:	false
SSDEEP:	3072:XaalEQx39v+iA1A626irP8n3U8IrU3iYdO3C36zoYimPVOCqgPB/KO4ue5GmdRPQ:qvgWGFX
MD5:	122164EB1C7F38A57CC1E2C694B87F23
SHA1:	B0F02AC486D2DF23418A9342FE2C4159FA0FD041
SHA-256:	FA84E5692AA3F1DA2B7F2C3024279986405C1784D8CAB39D8B2648BC0A178A9B
SHA-512:	EA9E3A97CEBE1A46C5D0FBE3E69E15536E80094F3F0E99F9E04ED6C37F9B00C236E334651FA1EE03FFC12251AF9DBF3064A4013823CBE77751551026166D4E2 4
Malicious:	false

Preview:	.....4.(.j..;..k..;..l..<..n..<..o..<..p..<..q.$<..r.3<..s.D<..t.M<..v.b<..w.o<..y.u<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<....R=....t=.....=.....=.....>.....>.....>.. ..F>....\>....r>.....>.....>.....>.....?.....?.....?.....?....)?....B?....a?....t?.....?.....?.....?.....?.....?..*.$@..+.'@..,.E@../.y@..0..@..1..A..2..A..3.<A..4.pA..5..A..6..B..7.=B..>..B..?..B..N. .B..g..B..i..B..j..B..k..B..l..C..:R.C..;R^C..<R.C..=R.D..>R.D..?R>E..@R.E..AR.E..BRVF..CR|F..DRLI..ERtI..FR}I..GR.I..HR.I..IR.I..JRGJ..KR.J..LR.K..MR.L..OR.L.. PRvL..QR.L..RR.L..SR.L..TR.M..URLM..VRxM..\R.N..eRHN..gRyN..mR.N..nR.N..oR.N..qRtO..rR.O..sR.O..tR.P..uR!P..vR]P..wR.P..xR.Q..yR.R..zR.S..{R.T..|RuT.. }R.T...R.T...R"V...R.W...R.W...R<X...R.X...R.Y...R.[...RC[...Rc[...R.[...Rv_...R.a...R/b...R.b...R.c...R'c...R@c...RRc...R{c...R.c...R.d...R.d...R.e...R.f...RLf...R.f...R.g...R`h.. .R.i...R_i...R.j...R.j...R.j...R.j...R.j...RNk...R.k...R.l...R.l...R0l...R3l...R.l...R.l...R$m...R.m

C:\Program Files (x86)\Jabra\Direct4\locales\he.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	154333
Entropy (8bit):	4.812260538422886
Encrypted:	false
SSDEEP:	1536:n4EkYLcFhLbVk3NspwWHHe1AqEgSQ0HgLggnQUMHWWmXWOnhY57YNwq1oyP5f3Xq:Zn45p1zQWgccMYXC52VL3XTnwVFFaDE3
MD5:	408AECC4684DE0473BF1E3BBC30334CC
SHA1:	6A0DCD49CFCCBEEB41EBBF437412D6FDCCE5A15D
SHA-256:	31ED1AC7D7B392C4C79C223240D97588494892D5DDDFA62FC664CAC39BDB791F
SHA-512:	145A6E2D3B211768C942A85959DD899895C5912B9451C513ECCB4FD9BCB24EE754D761BAB84BA1C2A87B5E348495F2BA8170838A337A430129C5222569254C7[
Malicious:	false
Preview:	.....'.5.j..;..k..;..l..;..n..;..o..;..p..<..q..<..r..<..s.*<..t.3<..v.H<..w.U<..y.[<..z.j<..|.p<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<.....<....=....%=....>=....W=....t=....v=....z=.. ...=.....=.....=.....=.....=.....=.....>.....>.....>.... >....*>....?>....I>....S>....^>....r>....z>.....>.....>..*..>..+..>.,,.>../..>..0..>..1.2?..2.G?..3.Z?..4.~?..5..?..6..?..7..@..>..@..?.0@..N. I@..g.V@..i.Y@..j.]@..k.b@..l.j@..:Ro@..;R.@..<R.@..=R.A..>R.A..?R.A..@R.B..AR.B..BRwB..CR.B..DR.E..ER"E..FR,E..GR6E..HRTE..IR`E..JR.E..KR.E..LR.F..MR .F..OR.F..PR-G..QRFG..RRjG..SRrG..TR.G..UR.G..VR.G..\R.H..eR.H..gR-H..mR7H..nRTH..oRkH..qR.H..rR.H..sR.I..tR+I..uR3I..vR]I..wR.I..xR,J..yR.J..zR_K..{RwK..|R.K.. }R.K...R.K...R.L...R.M...R.M...R.M...R.N...R.N...R.O...R.O...R.O...R.O...R.R...R.S...R.T...R4U...ReU...RoU...R.U...R.U...R.U...R.U...R@V...RqV...R.V...R$W...R;W...R.W...R .X...RUX...R.X...R.X...R.Y...R.Y...R.Y...R.Y...R.Y...R.Z...R.Z...R.Z...R4Z...R7Z...RfZ...R.Z...R.Z...RT[

C:\Program Files (x86)\Jabra\Direct4\locales\hi.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	255098
Entropy (8bit):	4.420191364918154
Encrypted:	false
SSDEEP:	3072:5Mnqz5cwfKSlv8Fj3cvEVhkDNoWSkO/S/+fm9NLFLORvTHIf+onLzBKfzzrz3/Em:5dBnzh
MD5:	A4CF1951E12BF7EF6D30E0FE0E7DEDB3
SHA1:	3200CA510FE4FCC45D162BBDBF89A23769A1A112
SHA-256:	5AA42687E1729624C09F7038722622CD501D5420060182820E6DCCEA71A4647D
SHA-512:	382F43E98946EA23C12787F2F3CE00EA77ED265C23051844E0287509C0279D33FCFC50F3D0739CAC16BDCA7A38344B2E6755D32727A87814EB56D9CBFB74257[
Malicious:	false
Preview:	.....%.7.j..;..k..;..l..;..n..;..o..;..p..<..q..<..r..<..s.&<..t./<..v.D<..w.Q<..y.W<..z.f<..|.l<..}.~<.....<.....<.....<.....<.....<.....<.....<.....<.....<....L=....n=.....=.....=.....=.....=.....=.. ...>.....>....S>....u>.....>.....>.....>.....>.....>.....>.....?....0?....I?...._?.....?.....?.....?.....?.....@..*."@..+.%@..,.C@../..@..0..@..1..A..2.9A..3.YA..4..A..5..A..6.%B..7.oB..>..B ..?..B..N..C..g.*C..i.-C..j.1C..k.6C..l.DC..:RIC..;R.D..<RiD..=R.F..>R.F..?R!G..@R\G..AR.G..BRHH..CRtH..DR.K..ER.K..FR.K..GR.L..HRjL..IR|L..JR.L..KR7M..LR.N..MR NO..ORdO..PR%P..QRPP..RR.P..SR.P..TR4Q..URyQ..VR.Q..\RPR..eRtR..gR.R..mR.R..nR.R..oR.R..qR.S..rR.S..sR(T..tR]T..uRmT..vR.T..wR1U..xR(V..yR.W..zR.X..{R 5X..|RtX..}R.X...R.X...R.Z...R.[...R.[...R.\...R.\...R.]...R._...R:_...Rk_...R._...R.b...R.d...RWe...R.e...R.f...R2f...RQf...Rcf...R.f...R$g...RUh...R.h...R.i...R.i...R.i...RHj...R.k...R.k.. .R.l...RZm...R.n...R.n...R.n...R.n...R.o...RXo...R.o...R.o...R.o...R.o...R9p...R.q...R_q...R.q...R.r

C:\Program Files (x86)\Jabra\Direct4\locales\hr.pak

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	122538
Entropy (8bit):	5.505630347516926
Encrypted:	false
SSDEEP:	3072:Oj/ve1KR0AGCMoleWq7ljdpYbLnoUDEiTMMoksk74uXKpx9s:anewldK6
MD5:	7EFB7C48C535F836F6534FEF4ADAD84C
SHA1:	487038B015BF2998857138F7C4198F203F0B5008
SHA-256:	7876AD2719DD22EC9784AB78651D8114C5196199129596171301148 6DE9EDAD5
SHA-512:	9CD43019D225BD024DC063E210FA2FD4E628DACC56EB2690EBD5E78AAA34D961D0175D7A2E92936669F0CCB52590AF4AE4FED1405252ABC3B8C00962DBEC8 C4
Malicious:	false

Preview:	.....N...j..<..k.-<..l.8<..n.@<..o.E<..p.R<..q.X<..r.g<..s.x<..t..<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....=.....=.....=....5=....A=....M=....[=....l=.... n=....r=....z=.....=.....=.....=.....=.....=.....=.....=.....=.....=.....>.....>.....>....&>....,>....4>....V>..*.a>..+.d>..,..>../..>..0..>..1..>..2..>..3..>..4..?..5.1?..6.s?..7..?..>..?..?..?..N. .?..g..?..i..?..j..?..k..?..l..?..::R.?..;R.@..<R)@..=R.@..>R.@..?R.@..@R.A..AR.A..BREA..CRUA..DR.B..ER.C..FR.C..GR.C..HR,C..IR4C..JR]C..KR.C..LR.D..MRFD..ORND.. PRzD..QR.D..RR.D..SR.D..TR.D..UR.D..VR.E..\R2E..eR;E..gRLE..mRRE..nRnE..oR.E..qR.E..rR.E..sR.F..tR.F..uR$F..vR;F..wRiF..xR.F..yR4G..zR.G..{R.G..|R.G.. }R.G...R.G...RsH...R*I...R=I...RQI...R.I...R.J...R.J...R.J...R.J...R.K...R.M...R.M...R.N...R.O...R(O...R0O...R@O...RMO...R]O...R.O...R.O...R.O...RKP...RdP...R{P...R.P...R .Q...RRQ...R.Q...R.Q...RcR...RjR...RpR...RvR...R.R...R.R...R.R...R.R...R.R...R.R...R.R...R%S...RQS...R.S...R.S

C:\Program Files (x86)\Jabra\Direct4\locales\hu.pak	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	131931
Entropy (8bit):	5.632963569789605
Encrypted:	false
SSDEEP:	3072:Nt0lRS3jViHCwXRkiG5ZqnPgdAaWdpEYLt5R3ICm:WRY+iiGMP6WdpE6r3ICm
MD5:	BF08B678CFE95AE1D1434AD985D713EC
SHA1:	2FBEB8F695872076F2D49B29BA46D274712BE438
SHA-256:	BDF02941626EFF00AEE71EA9C69F8DDEB10B9DACDBFD23B18C462E3ED8992C26
SHA-512:	C056FD90D00C4BE9CF404C83CD023E7AEFA350B77D14CF6EBEE4868E724699B28F113E7E7F02D9E9D0F89B0ECD200BF91CC3E9777C63FE09DE28C80DA20C8 A8C
Malicious:	false
Preview:	.....F...j..<..k..<..l.(<..n.0<..o.5<..p.B<..q.H<..r.W<..s.h<..t.q<..v..<..w..<..y..<..z..<..|..<..}..<.....<.....<.....<.....<.....<.....<.....<.....<.....<....;=....K=....a=....v=.....=.....=.....=.. ...=.....=.....=.....=.....=.....>....,>....3>....6>....7>....A>....N>....^>....g>....q>.....>.....>.....>..*..>..+..>..,..>../..>..0..>..1.2?..2.>?..3.K?..4.h?..5..?..6..?..7..?..>..?..?..?..@..N. .@..g..@..i./@..j.3@..k.8@..l.?@..:RD@..;Ru@..<R.@..=RWA..>ReA..?R.A..@R.A..AR.A..BR.B..CR-B..DR;C..ERKC..FRRC..GR\C..HRnC..IR|C..JR.C..KR.C..LR[D..MR .D..OR.D..PR.D..QR.D..RR.D..SR.D..TR.D..UR.E..VR+E..\RlE..eR|E..gR.E..mR.E..nR.E..oR.E..qR.E..rR.F..sR.F..tRAF..uRFF..vRcF..wR.F..xR.F..yRgG..zR.G..{R .G..|R#H..}R7H...RTH...R.H...R.I...R.I...R.I...R.J...R.J...R.K...R.K...R*K...RGK...R`L...R.L...ROM...R.M...R.M...R.M...R.M...R.M...R.N...R4N...R.N...R.N...R.O...RBO...RWO ...R.O...R.P...RcP...R.P...R.P...R.Q...R.Q...R.Q...R.Q...R.Q...R.Q...R.Q...R.R...R.R...R.R...R.R...R1R...RPR...R.R...R.R...R.S

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.9997414716837945
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	JabraDirectSetup.exe
File size:	85228936
MD5:	df71bfab12e144a002d85d07c0fa0fd8
SHA1:	700b1257e4bdc35bb9d53388e1c4220773827621
SHA256:	98ececd8b2573b79e79b97ebf1034afeac5107e50869422066b438138ae18d14
SHA512:	59a451a7b9af7562c096848bea425d0a1ce9c54a18a51b160c649d1f82e7f2fb7acea9336edc76a784a52e01a941b0944f61a29630dffbf8fb9ca6b9e3f77cb0
SSDEEP:	1572864:K9hKvmziAc4CnPATU3PlBfLZyn9vU/9oJjlreEPm1Hpb2Ok7d1CDW/IIDgoaVH8D:KK5TATU3PlBzgn9veWJPQHpSzTC6flam
TLSH:	A81833335CAC8B36E3901532E818B2771C25A7695351C5AAE3D9FC6C7A032D326B7BC5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.o.}k..}k..}k.....wk.....k.....ek../...nk../...ik../...Vk..t...xk..t...lk..}k.. (j.....6k.....|k..}k...k.....|k..Rich}k.

File Icon

Icon Hash:	70e0da9adac6f071

Static PE Info

General

Entrypoint:	0x42df71
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, REMOVABLE_RUN_FROM_SWAP, NET_RUN_FROM_SWAP
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x5D807032 [Tue Sep 17 05:33:38 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	42d651751c1d75ed4fa8fe71751854ff

Authenticode Signature	
Signature Valid:	**true**
Signature Issuer:	CN=Symantec Class 3 SHA256 Code Signing CA, OU=Symantec Trust Network, O=Symantec Corporation, C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 3/9/2020 1:00:00 AM 3/22/2023 12:59:59 AM
Subject Chain	• CN=GN AUDIO A/S, OU=Jabra, O=GN AUDIO A/S, L=Ballerup, S=Denmark, C=DK
Version:	3
Thumbprint MD5:	A5FC63381B6C41BFDCB078BEFD733D73
Thumbprint SHA-1:	6C01548344A5417E71115135AE426AC77AD268D6
Thumbprint SHA-256:	729A2B1F424C36112E75EFF3A7291F36B155620213C593454198FED07C6AC04B
Serial:	67A5CEB68A3258E8FA98A9234A07F349

Entrypoint Preview
Instruction
call 00007F3EF4A89BDFh
jmp 00007F3EF4A8951Fh
int3
int3
int3
int3
int3
mov eax, dword ptr [esp+08h]
mov ecx, dword ptr [esp+10h]
or ecx, eax
mov ecx, dword ptr [esp+0Ch]
jne 00007F3EF4A896ABh
mov eax, dword ptr [esp+04h]
mul ecx
retn 0010h
push ebx
mul ecx
mov ebx, eax
mov eax, dword ptr [esp+08h]
mul dword ptr [esp+14h]
add ebx, eax
mov eax, dword ptr [esp+08h]
mul ecx
add edx, ebx
pop ebx
retn 0010h
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
cmp cl, 00000040h
jnc 00007F3EF4A896B7h
cmp cl, 00000020h
jnc 00007F3EF4A896A8h
shrd eax, edx, cl
shr edx, cl
ret
mov eax, edx
xor edx, edx
and cl, 0000001Fh
shr eax, cl
ret
xor eax, eax
xor edx, edx
ret
push ebp
mov ebp, esp
jmp 00007F3EF4A896AFh
push dword ptr [ebp+08h]
call 00007F3EF4A8FA88h
pop ecx
test eax, eax
je 00007F3EF4A896B1h
push dword ptr [ebp+08h]
call 00007F3EF4A8FB11h
pop ecx
test eax, eax
je 00007F3EF4A89688h
pop ebp
ret
cmp dword ptr [ebp+08h], FFFFFFFFh
je 00007F3EF4A89FA4h
jmp 00007F3EF4A89F81h
push ebp
mov ebp, esp
push dword ptr [ebp+08h]
call 00007F3EF4A89FBDh
pop ecx
pop ebp
ret
push ebp
mov ebp, esp
test byte ptr [ebp+08h], 00000001h
push esi
mov esi, ecx
mov dword ptr [esi], 0046030Ch
je 00007F3EF4A896ACh
push 0000000Ch
push esi
call 00007F3EF4A8967Dh
pop ecx

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x680b4	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6d000	0x5730	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x51463f8	0x1990	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x73000	0x3dd0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x67030	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x67084	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x66a10	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4a000	0x3e0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x67c34	0x100	.rdata
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	0x48ff7	0x49000	False	0.5367883133561644	data	6.572059575788497	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x4a000	0x1f760	0x1f800	False	0.30963231646825395	data	5.137524712720983	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6a000	0x16fc	0xa00	False	0.27265625	data	3.1551613029957557	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.wixburn	0x6c000	0x38	0x200	False	0.130859375	data	0.7421500244532455	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x6d000	0x5730	0x5800	False	0.23979048295454544	data	4.998531404362636	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x73000	0x3dd0	0x3e00	False	0.8069556451612904	data	6.788270717274864	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6d178	0x25a8	data	English	United States
RT_MESSAGETABLE	0x6f720	0x2840	data	English	United States
RT_GROUP_ICON	0x71f60	0x14	data	English	United States
RT_VERSION	0x71f74	0x2e8	data	English	United States
RT_MANIFEST	0x7225c	0x4d2	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCloseKey, RegOpenKeyExW, OpenProcessToken, AdjustTokenPrivileges, LookupPrivilegeValueW, InitiateSystemShutdownExW, GetUserNameW, RegQueryValueExW, RegDeleteValueW, CloseEventLog, OpenEventLogW, ReportEventW, ConvertStringSecurityDescriptorToSecurityDescriptorW, DecryptFileW, CreateWellKnownSid, InitializeAcl, SetEntriesInAclW, ChangeServiceConfigW, CloseServiceHandle, ControlService, OpenSCManagerW, OpenServiceW, QueryServiceStatus, SetNamedSecurityInfoW, CheckTokenMembership, AllocateAndInitializeSid, SetEntriesInAclA, SetSecurityDescriptorGroup, SetSecurityDescriptorOwner, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, RegSetValueExW, RegQueryInfoKeyW, RegEnumValueW, RegEnumKeyExW, RegDeleteKeyW, RegCreateKeyExW, GetTokenInformation, CryptDestroyHash, CryptHashData, CryptCreateHash, CryptGetHashParam, CryptReleaseContext, CryptAcquireContextW, QueryServiceConfigW

DLL	Import
USER32.dll	PeekMessageW, PostMessageW, IsWindow, WaitForInputIdle, PostQuitMessage, GetMessageW, TranslateMessage, MsgWaitForMultipleObjects, PostThreadMessageW, GetMonitorInfoW, MonitorFromPoint, IsDialogMessageW, LoadCursorW, LoadBitmapW, SetWindowLongW, GetWindowLongW, GetCursorPos, MessageBoxW, CreateWindowExW, UnregisterClassW, RegisterClassW, DefWindowProcW, DispatchMessageW
OLEAUT32.dll	VariantInit, SysAllocString, VariantClear, SysFreeString
GDI32.dll	DeleteDC, DeleteObject, SelectObject, StretchBlt, GetObjectW, CreateCompatibleDC
SHELL32.dll	CommandLineToArgvW, SHGetFolderPathW, ShellExecuteExW
ole32.dll	CoUninitialize, CoInitializeEx, CoInitialize, StringFromGUID2, CoCreateInstance, CoTaskMemFree, CLSIDFromProgID, CoInitializeSecurity
KERNEL32.dll	GetCPInfo, GetOEMCP, IsValidCodePage, CloseHandle, CreateFileW, GetProcAddress, LocalFree, HeapSetInformation, GetLastError, GetModuleHandleW, FormatMessageW, lstrlenA, lstrlenW, MultiByteToWideChar, WideCharToMultiByte, LCMapStringW, Sleep, GetLocalTime, GetModuleFileNameW, ExpandEnvironmentStringsW, GetTempPathW, GetTempFileNameW, CreateDirectoryW, GetFullPathNameW, CompareStringW, GetCurrentProcessId, WriteFile, SetFilePointer, LoadLibraryW, GetSystemDirectoryW, CreateFileA, HeapAlloc, HeapReAlloc, HeapFree, HeapSize, GetProcessHeap, FindClose, GetCommandLineA, GetCurrentDirectoryW, RemoveDirectoryW, SetFileAttributesW, GetFileAttributesW, DeleteFileW, FindFirstFileW, FindNextFileW, MoveFileExW, GetCurrentProcess, GetCurrentThreadId, InitializeCriticalSection, DeleteCriticalSection, ReleaseMutex, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, CreateProcessW, GetVersionExW, VerSetConditionMask, FreeLibrary, EnterCriticalSection, LeaveCriticalSection, GetSystemTime, GetNativeSystemInfo, GetModuleHandleExW, GetWindowsDirectoryW, GetSystemWow64DirectoryW, GetCommandLineW, VerifyVersionInfoW, GetVolumePathNameW, GetDateFormatW, GetUserDefaultUILanguage, GetSystemDefaultLangID, GetUserDefaultLangID, GetStringTypeW, ReadFile, SetFilePointerEx, DuplicateHandle, InterlockedExchange, InterlockedCompareExchange, LoadLibraryExW, CreateEventW, ProcessIdToSessionId, OpenProcess, GetProcessId, WaitForSingleObject, ConnectNamedPipe, SetNamedPipeHandleState, CreateNamedPipeW, CreateThread, GetExitCodeThread, SetEvent, WaitForMultipleObjects, InterlockedIncrement, InterlockedDecrement, ResetEvent, SetEndOfFile, SetFileTime, LocalFileTimeToFileTime, DosDateTimeToFileTime, CompareStringA, GetExitCodeProcess, SetThreadExecutionState, CopyFileExW, MapViewOfFile, UnmapViewOfFile, CreateMutexW, CreateFileMappingW, GetThreadLocale, FindFirstFileExW, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetStdHandle, GetConsoleCP, GetConsoleMode, FlushFileBuffers, DecodePointer, WriteConsoleW, GetModuleHandleA, GlobalAlloc, GlobalFree, GetFileSizeEx, CopyFileW, VirtualAlloc, VirtualFree, SystemTimeToTzSpecificLocalTime, GetTimeZoneInformation, SystemTimeToFileTime, GetSystemInfo, VirtualProtect, VirtualQuery, GetComputerNameW, SetCurrentDirectoryW, GetFileType, GetACP, ExitProcess, GetStdHandle, InitializeCriticalSectionAndSpinCount, SetLastError, RtlUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, RaiseException, LoadLibraryExA
RPCRT4.dll	UuidCreate

Possible Origin

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

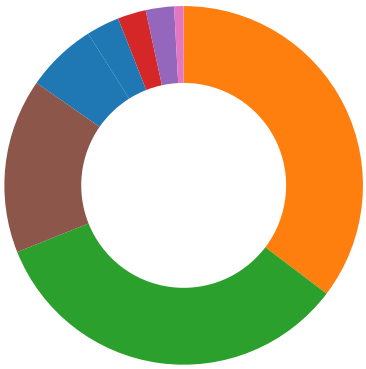
Network Behavior

No network behavior found

Statistics

Behavior

- JabraDirectSetup.exe
- JabraDirectSetup.exe
- JabraDirectSetup.exe
- JabraDirectSetup.exe
- JabraDirectSetup.exe
- JabraDirectSetup.exe
- msiexec.exe
- msiexec.exe
- taskkill.exe
- conhost.exe
- JabraDirectSetup.exe
- svchost.exe



Click to jump to process

System Behavior

Analysis Process: JabraDirectSetup.exe PID: **2040**, Parent PID: **6072**

General

Target ID:	0
Start time:	07:49:49
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\JabraDirectSetup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\JabraDirectSetup.exe"
Imagebase:	0x1220000
File size:	85228936 bytes
MD5 hash:	DF71BFAB12E144A002D85D07C0FA0FD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: JabraDirectSetup.exe PID: **1120**, Parent PID: **2040**

General

Target ID:	1
Start time:	07:49:50
Start date:	23/09/2022
Path:	C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe" -burn.clean.room="C:\Users\user\Desktop\JabraDirectSetup.exe" -burn.filehandle.attached=572 -burn.filehandle.self=568
Imagebase:	0xad0000
File size:	602888 bytes
MD5 hash:	6D9E7D60EE823CDB1AEA3F0C4C5B6C56
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	AD4173	CreateDirectoryW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	AD4173	CreateDirectoryW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	7	AD4173	CreateDirectoryW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\wixstdba.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AF0D6B	CreateFileW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\license.rtf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AF0D6B	CreateFileW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\Background.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AF0D6B	CreateFileW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\thm.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AF0D6B	CreateFileW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\thm.wxl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AF0D6B	CreateFileW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\logo.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AF0D6B	CreateFileW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\BootstrapperApplicationData.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AF0D6B	CreateFileW
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	AD4173	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Jabra_Direct_20220923074951.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AD3099	CreateFileW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	AD4173	CreateDirectoryW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	AD4173	CreateDirectoryW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	AE85FA	CreateFileW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\JabraDirect.msi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AF0D6B	CreateFileW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\DFUDriverSetupX64Setup.msi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AF0D6B	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:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\wixstdba.dll	0	23965	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 3a 76 0d 4f 7e 17 63 1c 7e 17 63 1c 7e 17 63 1c 8b fd 1c 74 17 63 1c 8b fd 1c 06 17 63 1c 8b fd 1c 66 17 63 1c 2c 7f 67 1d 6e 17 63 1c 2c 7f 60 1d 6c 17 63 1c 2c 7f 66 1d 61 17 63 1c 77 6f fd 1c 7a 17 63 1c 77 6f fd 1c 63 17 63 1c 7e 17 62 1c 7c 16 63 1c fd 7e 66 1d 67 17 63 1c fd 7e 63 1d 7f 17 63 1c fd 7e fd 1c 7f 17 63 1c 7e 17 fd 1c 7f 17 63 1c fd 7e 61 1d 7f 17 63	MZ@!L!This program cannot be run in DOS mode.$:vO~c~c~ctccfc ,gnc,`lc,facwozcwocc~b|c ~fgc~cc~c~ac	success or wait	7	AF09AC	WriteFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\license.rtf	0	17648	7b 5c 72 74 66 31 5c 61 6e 73 69 5c 64 65 66 66 30 5c 6e 6f 75 69 63 6f 6d 70 61 74 7b 5c 66 6f 6e 74 74 62 6c 7b 5c 66 30 5c 66 6e 69 6c 5c 66 63 68 61 72 73 65 74 30 20 43 6f 75 72 69 65 72 20 4e 65 77 3b 7d 7d 0d 0a 7b 5c 2a 5c 67 65 6e 65 72 61 74 6f 72 20 52 69 63 68 65 64 32 30 20 31 30 2e 30 2e 31 37 31 33 34 7d 5c 76 69 65 77 6b 69 6e 64 34 5c 75 63 31 20 0d 0a 5c 70 61 72 64 5c 66 30 5c 66 73 32 32 5c 6c 61 6e 67 31 30 33 30 20 4a 61 62 72 61 20 44 69 72 65 63 74 20 45 6e 64 20 55 73 65 72 20 4c 69 63 65 6e 73 65 20 41 67 72 65 65 6d 65 6e 74 5c 70 61 72 0d 0a 5c 70 61 72 0d 0a 49 4d 50 4f 52 54 41 4e 54 20 4e 4f 54 49 43 45 3a 20 50 4c 45 41 53 45 20 52 45 41 44 20 43 41 52 45 46 55 4c 4c 59 20 42 45 46 4f 52 45 20 49 4e 53 54 41 4c 4c 49 4e 47	{\rtf1\ansi\deff0\nouicompat{\ fonttbl{\f0\fnil\fcharset0 Courier New;}} {*\generator Riched20 10.0.17134}\viewkind4\uc 1 \pard\f0\fs22\lang1030 Jabra Direct End User License Agreement\par\parIMPORTANT NOTICE: PLEASE READ CAREFULLY BEFORE INSTALLING	success or wait	1	AF09AC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\Background.png	0	11997	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 45 00 00 01 23 08 03 00 00 01 7c 7f 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 01 fd 50 4c 54 45 36 3a 40 68 60 30 6b 10 fd fd 00 fd fd 18 4f 4d 38 43 44 3c fd fd 1c fd 7c 24 fd fd 04 fd 08 fd 72 28 5b 56 34 fd fd 20 b5 0c fd fd 04 fd fd 1c 5c 57 34 fd 73 28 fd fd 20 fd fd 20 fd fd 0c 2b 28 19 1d 1d 1b 47 3f 16 fd 03 6f 05 64 55 12 fd fd 0a 39 33 18 fd fd 18 fd 7c 24 75 69 2c b4 0c 43 43 3c fd fd 14 fd fd fd fd fd fd fd fd fd 68 6b 70 fd fd 01 e4 06 6f 04 75 77 7c fd fd fd fd fd fd fd fd cd fd fd fd fd fd 68 6b 6f 43 46 4c fd fd fd fd 77 0d fd fd fd 4f 52 58 75 77 7b 74 78 7c 4f 53 57 fd fd 35 fd fd fd fd fd fd	PNGIHDRE#|sRGBgAMAaPLTE6:@h`0OM8CD<|$r([V4 \W4s(+(G?dU93\|$ui,CC<hkpuw|hkoCFLwORXuw{tx|OSW	success or wait	1	AF09AC	WriteFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\thm.xml	0	5245	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 54 68 65 6d 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 69 78 74 6f 6f 6c 73 65 74 2e 6f 72 67 2f 73 63 68 65 6d 61 73 2f 74 68 6d 75 74 69 6c 2f 32 30 31 30 22 3e 0d 0a 20 20 3c 57 69 6e 64 6f 77 20 57 69 64 74 68 3d 22 35 38 31 22 20 48 65 69 67 68 74 3d 22 34 30 30 22 20 48 65 78 53 74 79 6c 65 3d 22 31 30 30 61 30 30 30 30 22 20 46 6f 6e 74 49 64 3d 22 30 22 3e 23 28 6c 6f 63 2e 43 61 70 74 69 6f 6e 29 3c 2f 57 69 6e 64 6f 77 3e 0d 0a 20 20 3c 46 6f 6e 74 20 49 64 3d 22 30 22 20 48 65 69 67 68 74 3d 22 2d 31 32 22 20 57 65 69 67 68 74 3d 22 35 30 30 22 20 46 6f 72 65 67 72 6f 75 6e 64 3d 22 30 30 30 30 30 30 22 20 42 61 63	<?xml version="1.0" encoding="utf-8"?><Theme xmlns="http://wixtoolset.org/schemas/thmutil/2010"> <Window Width="581" Height="400" HexStyle="100a0000" FontId="0">#(loc.Caption)</Window> <Font Id="0" Height="-12" Weight="500" Foreground="000000" Bac	success or wait	1	AF09AC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\thm.wxl	0	3899	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 57 69 78 4c 6f 63 61 6c 69 7a 61 74 69 6f 6e 20 43 75 6c 74 75 72 65 3d 22 65 6e 2d 75 73 22 20 4c 61 6e 67 75 61 67 65 3d 22 31 30 33 33 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 78 2f 32 30 30 36 2f 6c 6f 63 61 6c 69 7a 61 74 69 6f 6e 22 3e 0d 0a 20 20 3c 53 74 72 69 6e 67 20 49 64 3d 22 43 61 70 74 69 6f 6e 22 3e 5b 57 69 78 42 75 6e 64 6c 65 4e 61 6d 65 5d 20 53 65 74 75 70 3c 2f 53 74 72 69 6e 67 3e 0d 0a 20 20 3c 53 74 72 69 6e 67 20 49 64 3d 22 54 69 74 6c 65 22 3e 5b 57 69 78 42 75 6e 64 6c 65 4e 61 6d 65 5d 3c 2f 53 74 72 69 6e 67 3e 0d 0a 20 20 3c	<?xml version="1.0" encoding="utf-8"?> <WixLocalization Culture="en-us" Language="1033" xmlns="http://schemas.microsoft.com/wix/2006/localization"> <String Id="Caption">[WixBundleName] Setup</String> <String Id="Title">[WixBundleName]</String> <	success or wait	1	AF09AC	WriteFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\logo.png	0	11997	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 45 00 00 01 23 08 03 00 00 01 7c 7f 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 01 fd 50 4c 54 45 36 3a 40 68 60 30 6b 10 fd fd 00 fd fd 18 4f 4d 38 43 44 3c fd fd 1c fd 7c 24 fd fd 04 fd 08 fd 72 28 5b 56 34 fd fd 20 b5 0c fd fd 04 fd fd 1c 5c 57 34 fd 73 28 fd fd 20 fd fd 20 fd fd 0c 2b 28 19 1d 1d 1b 47 3f 16 fd 03 6f 05 64 55 12 fd fd 0a 39 33 18 fd fd 18 fd 7c 24 75 69 2c b4 0c 43 43 3c fd fd 14 fd fd fd fd fd fd fd fd fd 68 6b 70 fd fd 01 e4 06 6f 04 75 77 7c fd fd fd fd fd fd fd fd cd fd fd fd fd fd 68 6b 6f 43 46 4c fd fd fd fd 77 0d fd fd fd 4f 52 58 75 77 7b 74 78 7c 4f 53 57 fd fd 35 fd fd fd fd fd fd	PNGIHDRE#|sRGBgAMAaPLTE6:@h`0OM8CD<|$r([V4 \W4s(+(G?dU93\|$ui,CC<hkpuw|hkoCFLwORXuw{tx|OSW	success or wait	1	AF09AC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\BootstrapperApplicationData.xml	0	6856	fd fd 3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 75 00 74 00 66 00 2d 00 31 00 36 00 22 00 3f 00 3e 00 0d 00 0a 00 3c 00 42 00 6f 00 6f 00 74 00 73 00 74 00 72 00 61 00 70 00 70 00 65 00 72 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 20 00 78 00 6d 00 6c 00 6e 00 73 00 3d 00 22 00 68 00 74 00 74 00 70 00 3a 00 2f 00 2f 00 73 00 63 00 68 00 65 00 6d 00 61 00 73 00 2e 00 6d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 63 00 6f 00 6d 00 2f 00 77 00 69 00 78 00 2f 00 32 00 30 00 31 00 30 00 2f 00 42 00 6f 00 6f 00 74 00 73 00 74 00 72 00 61 00 70 00 70 00 65 00 72	<?xml version="1.0" encoding="utf-16"?> <BootstrapperApplicationData xmlns="http://schemas.microsoft.com/wix/2010/Bootstrapper	success or wait	1	AF09AC	WriteFile
unknown	0	985	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	985	155	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	1140	103	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	1243	111	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	1354	99	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	1453	110	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	1563	64	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	1627	98	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	B10082	WriteFile
unknown	1830	93	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	1923	93	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	2016	95	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	2111	99	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	B10082	WriteFile
unknown	2538	112	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	2650	68	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	2718	96	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	2814	79	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	2893	125	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	3018	208	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	B10082	WriteFile
unknown	3226	191	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	B10082	WriteFile
unknown	3417	102	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	B10082	WriteFile
unknown	4065	208	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	B10082	WriteFile
unknown	4952	66	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	5018	51	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe	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 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 39 0a 6f fd 7d 6b 01 fd 7d 6b 01 fd 7d 6b 01 fd fd fd fd 77 6b 01 fd fd fd fd 00 6b 01 fd fd fd fd 65 6b 01 fd 2f 03 05 fd 6e 6b 01 fd 2f 03 02 fd 69 6b 01 fd 2f 03 04 fd 56 6b 01 fd 74 13 fd fd 78 6b 01 fd 74 13 fd fd 6c 6b 01 fd 7d 6b 00 fd 28 6a 01 fd fd 02 04 fd 36 6b 01 fd fd 02 fd fd 7c 6b 01 fd 7d 6b fd fd 7f 6b 01 fd fd 02 03 fd 7c 6b 01 fd 52 69 63 68 7d 6b 01	MZ@!L!This program cannot be run in DOS mode.$9o}k}k}kwkkek/nk/ik/Vktxktlk}k(j6k|k}kk|kRich}k	success or wait	148	B1467A	WriteFile
unknown	5069	74	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	5143	73	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	5216	69	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	5285	66	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	B10082	WriteFile
unknown	5599	197	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	B10082	WriteFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\JabraDirect.msi	0	32768	fd fd 11 71 1a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 04 00 fd fd 0c 00 06 00 00 00 00 00 00 00 00 02 00 00 00 15 00 00 00 01 00 00 00 00 00 00 00 00 10 00 00 02 00 00 00 01 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 04 00 00 00 08 00 00 00 0c 00 00 00 10 00 00 00 14 00 00 00 18 00 00 00 1c 00 00 00 20 00 00 00 24 00 00 00 28 00 00 00 2c 00 00 00 30 00 00 00 34 00 00 00 38 00 00 00 3c 00 00 00 40 00 00 00 44 00 00 00 48 00 00 00 4c 00 00 fd 4f 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	> $(,048<@DHLO	success or wait	2581	AF09AC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\DFUDriverSetupX64Setup.msi	0	12288	fd fd 11 71 1a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 04 00 fd fd 0c 00 06 00 00 00 00 00 00 00 02 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00 10 00 00 02 00 00 00 01 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd	>	success or wait	31	AF09AC	WriteFile
unknown	6398	256	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	B10082	WriteFile
unknown	6944	166	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile
unknown	7110	432	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	B10082	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe	unknown	64	success or wait	1	ADB56F	ReadFile
C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe	unknown	24	success or wait	1	ADB621	ReadFile
C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe	unknown	36	success or wait	1	AF07DA	ReadFile
C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe	unknown	16	success or wait	8	AF07DA	ReadFile
C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe	unknown	8	success or wait	3	AF07DA	ReadFile
C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe	unknown	8	success or wait	3	AF07DA	ReadFile
C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe	unknown	8	success or wait	6	AF07DA	ReadFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\license.rtf	unknown	4092	success or wait	1	6D53B1A5	ReadFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.ba\license.rtf	unknown	4092	success or wait	4	6D53B1A5	ReadFile
C:\Windows\Temp\{E08359EB-BFFA-49B5-8115-528C8789A364}\.cr\JabraDirectSetup.exe	unknown	4096	success or wait	147	B137A5	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	4	success or wait	1	AE55A9	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}.Cache	unknown	4	success or wait	1	AE55A9	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	AE48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	70	success or wait	1	AE49A2	ReadFile
C:\Users\user\Desktop\JabraDirectSetup.exe	unknown	36	success or wait	1	AF07DA	ReadFile
C:\Users\user\Desktop\JabraDirectSetup.exe	unknown	16	success or wait	3	AF07DA	ReadFile
C:\Users\user\Desktop\JabraDirectSetup.exe	unknown	256	success or wait	3	AF07DA	ReadFile
C:\Users\user\Desktop\JabraDirectSetup.exe	unknown	8	success or wait	1	AF07DA	ReadFile
C:\Users\user\Desktop\JabraDirectSetup.exe	unknown	8	success or wait	1	AF07DA	ReadFile
C:\Users\user\Desktop\JabraDirectSetup.exe	unknown	8	success or wait	19	AF07DA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}.Cache	unknown	8	success or wait	1	AE48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}.Cache	unknown	260	success or wait	2	AE49A2	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	AE48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1625	AE48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	unknown	1	AE48EA	ReadFile

Analysis Process: JabraDirectSetup.exe PID: **4216**, Parent PID: **1120**

General

Target ID:	2
Start time:	07:49:58
Start date:	23/09/2022
Path:	C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe" -q -burn.elevated BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8} {D37BA658-0E76-49AC-BEF7-9E23554C8C54} 1120
Imagebase:	0x12e0000
File size:	602888 bytes
MD5 hash:	6D9E7D60EE823CDB1AEA3F0C4C5B6C56
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	12E4173	CreateDirectoryW
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	12E4173	CreateDirectoryW
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	1323863	CopyFileW
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\state.rsm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13245E7	CreateFileW
C:\ProgramData\Package Cache\{316F5FBF-4536-4A14-8D29-C1A9A8D800B6}v5.12.06601\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	12E4173	CreateDirectoryW
C:\ProgramData\Package Cache\.unverified\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	12E4173	CreateDirectoryW
C:\ProgramData\Package Cache\{D662C345-04FD-4F6C-AB68-B9BC6D6A5D2F}v7.0.32822.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	12E4173	CreateDirectoryW
C:\ProgramData\Package Cache\.unverified\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	12E4173	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\JabraDirect.msi	C:\ProgramData\Package Cache\.unverified\JabraDirect.msi	success or wait	1	1323A38	MoveFileExW
C:\ProgramData\Package Cache\.unverified\JabraDirect.msi	C:\ProgramData\Package Cache\{316F5FBF-4536-4A14-8D29-C1A9A8D800B6}v5.12.06601\JabraDirect.msi	success or wait	1	1323A38	MoveFileExW
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\DFUDriverSetupX64Setup.msi	C:\ProgramData\Package Cache\.unverified\DFUDriverSetupX64Setup.msi	success or wait	1	1323A38	MoveFileExW
C:\ProgramData\Package Cache\.unverified\DFUDriverSetupX64Setup.msi	C:\ProgramData\Package Cache\{D662C345-04FD-4F6C-AB68-B9BC6D6A5D2F}v7.0.32822.0\DFUDriverSetupX64Setup.msi	success or wait	1	1323A38	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	0	262144	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 39 0a 6f fd 7d 6b 01 fd 7d 6b 01 fd 7d 6b 01 fd fd fd fd 77 6b 01 fd fd fd fd 00 6b 01 fd fd fd fd 65 6b 01 fd 2f 03 05 fd 6e 6b 01 fd 2f 03 02 fd 69 6b 01 fd 2f 03 04 fd 56 6b 01 fd 74 13 fd fd 78 6b 01 fd 74 13 fd fd 6c 6b 01 fd 7d 6b 00 fd 28 6a 01 fd fd 02 04 fd 36 6b 01 fd fd 02 fd fd 7c 6b 01 fd 7d 6b fd fd 7f 6b 01 fd fd 02 03 fd 7c 6b 01 fd 52 69 63 68 7d 6b 01	MZ@!L!This program cannot be run in DOS mode.$9o}k}k}kwkkek/nk/ik/Vktxktlk}k(j6k|k}kk|k Rich}k	success or wait	3	1323863	CopyFileW
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\state.rsm	0	794	4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	M	success or wait	1	132467A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe	unknown	64	success or wait	1	12EB56F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe	unknown	24	success or wait	1	12EB621	ReadFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe	unknown	36	success or wait	1	13007DA	ReadFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe	unknown	16	success or wait	2	13007DA	ReadFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe	unknown	8	success or wait	1	13007DA	ReadFile
C:\Windows\Temp\{240BAF75-3E5B-4E93-8F26-E04B9DE786C2}\.be\JabraDirectSetup.exe	unknown	8	success or wait	1	13007DA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	4	success or wait	1	12F46A2	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	76	success or wait	1	12F4736	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}.Cache	unknown	4	success or wait	1	12F46A2	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}.Cache	unknown	76	success or wait	1	12F4736	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}.Cache	unknown	8	success or wait	1	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	4	12F48EA	ReadFile
C:\ProgramData\Package Cache\.unverified\JabraDirect.msi	unknown	4096	success or wait	20646	131F467	ReadFile
C:\ProgramData\Package Cache\.unverified\JabraDirect.msi	unknown	4096	end of file	1	131F467	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}.Cache	unknown	8	success or wait	2	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}.Cache	unknown	8	success or wait	2	12F48EA	ReadFile
C:\ProgramData\Package Cache\.unverified\DFUDriverSetupX64Setup.msi	unknown	4096	success or wait	243	131F467	ReadFile
C:\ProgramData\Package Cache\.unverified\DFUDriverSetupX64Setup.msi	unknown	4096	end of file	1	131F467	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	208	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}	unknown	8	success or wait	1344	12F48EA	ReadFile
\pipe\BurnPipe.{D9E1E3E0-161A-4566-8CAE-5A87964B54C8}.Cache	unknown	8	unknown	1	12F48EA	ReadFile

Registry Activities

Analysis Process: JabraDirectSetup.exe PID: **1128**, Parent PID: **3528**

General

Target ID:	5
Start time:	07:50:11
Start date:	23/09/2022
Path:	C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" /burn.runonce
Imagebase:	0xda0000
File size:	602888 bytes
MD5 hash:	6D9E7D60EE823CDB1AEA3F0C4C5B6C56
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	64	success or wait	1	DAB56F	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	24	success or wait	1	DAB621	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	36	success or wait	1	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	16	success or wait	2	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	8	success or wait	1	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	8	success or wait	1	DC07DA	ReadFile

Analysis Process: JabraDirectSetup.exe PID: **5340**, Parent PID: **1128**

General

Target ID:	6
Start time:	07:50:12
Start date:	23/09/2022
Path:	C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" /burn.log.append "C:\Users\user\AppData\Local\Temp\Jabra_Direct_20220923074951.log
Imagebase:	0xda0000
File size:	602888 bytes
MD5 hash:	6D9E7D60EE823CDB1AEA3F0C4C5B6C56
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	64	success or wait	1	DAB56F	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	24	success or wait	1	DAB621	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	36	success or wait	1	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	16	success or wait	2	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	8	success or wait	1	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	8	success or wait	1	DC07DA	ReadFile

Analysis Process: JabraDirectSetup.exe PID: **1240**, Parent PID: **5340**

General

Target ID:	7
Start time:	07:50:13
Start date:	23/09/2022
Path:	C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" -burn.clean.room="C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" -burn.filehandle.attached=560 -burn.filehandle.self=580 /burn.log.append "C:\Users\user\AppData\Local\Temp\Jabra_Direct_20220923074951.log
Imagebase:	0xda0000
File size:	602888 bytes
MD5 hash:	6D9E7D60EE823CDB1AEA3F0C4C5B6C56
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	DA4173	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	DA4173	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	7	DA4173	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\wixstdba.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DC0D6B	CreateFileW
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\license.rtf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DC0D6B	CreateFileW
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\Background.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DC0D6B	CreateFileW
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\thm.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DC0D6B	CreateFileW
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\thm.wxl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DC0D6B	CreateFileW
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\logo.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DC0D6B	CreateFileW
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\BootstrapperApplicationData.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DC0D6B	CreateFileW
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	4	DA4173	CreateDirectoryW

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\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\wixstdba.dll	0	23965	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 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 3a 76 0d 4f 7e 17 63 1c 7e 17 63 1c 7e 17 63 1c 8b fd 1c 74 17 63 1c 8b fd 1c 06 17 63 1c 8b fd 1c 66 17 63 1c 2c 7f 67 1d 6e 17 63 1c 2c 7f 60 1d 6c 17 63 1c 2c 7f 66 1d 61 17 63 1c 77 6f fd 1c 7a 17 63 1c 77 6f fd 1c 63 17 63 1c 7e 17 62 1c 7c 16 63 1c fd 7e 66 1d 67 17 63 1c fd 7e 63 1d 7f 17 63 1c fd 7e fd 1c 7f 17 63 1c 7e 17 fd 1c 7f 17 63 1c fd 7e 61 1d 7f 17 63	MZ@!L!This program cannot be run in DOS mode.$:vO~c~c~ctccfc ,gnc,`lc,facwozcwocc~b|c ~fgc~cc~c~c~ac	success or wait	7	DC09AC	WriteFile
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\license.rtf	0	17648	7b 5c 72 74 66 31 5c 61 6e 73 69 5c 64 65 66 66 30 5c 6e 6f 75 69 63 6f 6d 70 61 74 7b 5c 66 6f 6e 74 74 62 6c 7b 5c 66 30 5c 66 6e 69 6c 5c 66 63 68 61 72 73 65 74 30 20 43 6f 75 72 69 65 72 20 4e 65 77 3b 7d 7d 0d 0a 7b 5c 2a 5c 67 65 6e 65 72 61 74 6f 72 20 52 69 63 68 65 64 32 30 20 31 30 2e 30 2e 31 37 31 33 34 7d 5c 76 69 65 77 6b 69 6e 64 34 5c 75 63 31 20 0d 0a 5c 70 61 72 64 5c 66 30 5c 66 73 32 32 5c 6c 61 6e 67 31 30 33 30 20 4a 61 62 72 61 20 44 69 72 65 63 74 20 45 6e 64 20 55 73 65 72 20 4c 69 63 65 6e 73 65 20 41 67 72 65 65 6d 65 6e 74 5c 70 61 72 0d 0a 5c 70 61 72 0d 0a 49 4d 50 4f 52 54 41 4e 54 20 4e 4f 54 49 43 45 3a 20 50 4c 45 41 53 45 20 52 45 41 44 20 43 41 52 45 46 55 4c 4c 59 20 42 45 46 4f 52 45 20 49 4e 53 54 41 4c 4c 49 4e 47	{\rtf1\ansi\deff0\nouicompat{\fonttbl{\f0\fnil\fcharset0 Courier New;}}{*\generator Riched20 10.0.17134}\viewkind4\uc1 \pard\f0\fs22\lang1030 Jabra Direct End User License Agreement\par\parIMPORTANT NOTICE: PLEASE READ CAREFULLY BEFORE INSTALLING	success or wait	1	DC09AC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\Background.png	0	11997	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 45 00 00 01 23 08 03 00 00 01 7c 7f 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 01 fd 50 4c 54 45 36 3a 40 68 60 30 6b 10 fd fd 00 fd fd 18 4f 4d 38 43 44 3c fd fd 1c fd 7c 24 fd fd 04 fd 08 fd 72 28 5b 56 34 fd fd 20 b5 0c fd fd 04 fd fd 1c 5c 57 34 fd 73 28 fd fd 20 fd fd 20 fd fd 0c 2b 28 19 1d 1d 1b 47 3f 16 fd 03 6f 05 64 55 12 fd fd 0a 39 33 18 fd fd 18 fd 7c 24 75 69 2c b4 0c 43 43 3c fd fd 14 fd fd fd fd fd fd fd fd fd 68 6b 70 fd fd 01 e4 06 6f 04 75 77 7c fd fd fd fd fd fd fd fd cd fd fd fd fd fd 68 6b 6f 43 46 4c fd fd fd fd 77 0d fd fd fd 4f 52 58 75 77 7b 74 78 7c 4f 53 57 fd fd 35 fd fd fd fd fd fd	PNGIHDRE#|sRGBgAMAaPLTE6:@h`0OM8CD<|$r([V4 \W4s(+(G?dU93\|$ui,CC<hkpuw|hkoCFLwORXuw{tx|OSW	success or wait	1	DC09AC	WriteFile
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\thm.xml	0	5245	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 54 68 65 6d 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 69 78 74 6f 6f 6c 73 65 74 2e 6f 72 67 2f 73 63 68 65 6d 61 73 2f 74 68 6d 75 74 69 6c 2f 32 30 31 30 22 3e 0d 0a 20 20 3c 57 69 6e 64 6f 77 20 57 69 64 74 68 3d 22 35 38 31 22 20 48 65 69 67 68 74 3d 22 34 30 30 22 20 48 65 78 53 74 79 6c 65 3d 22 31 30 30 61 30 30 30 30 22 20 46 6f 6e 74 49 64 3d 22 30 22 3e 23 28 6c 6f 63 2e 43 61 70 74 69 6f 6e 29 3c 2f 57 69 6e 64 6f 77 3e 0d 0a 20 20 3c 46 6f 6e 74 20 49 64 3d 22 30 22 20 48 65 69 67 68 74 3d 22 2d 31 32 22 20 57 65 69 67 68 74 3d 22 35 30 30 22 20 46 6f 72 65 67 72 6f 75 6e 64 3d 22 30 30 30 30 30 30 22 20 42 61 63	<?xml version="1.0" encoding="utf-8"?><Theme xmlns="http://wixtoolset.org/schemas/thmutil/2010"> <Window Width="581" Height="400" HexStyle="100a0000" FontId="0">#(loc.Caption)</Window> <Font Id="0" Height="-12" Weight="500" Foreground="000000" Bac	success or wait	1	DC09AC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\thm.wxl	0	3899	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 57 69 78 4c 6f 63 61 6c 69 7a 61 74 69 6f 6e 20 43 75 6c 74 75 72 65 3d 22 65 6e 2d 75 73 22 20 4c 61 6e 67 75 61 67 65 3d 22 31 30 33 33 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 78 2f 32 30 30 36 2f 6c 6f 63 61 6c 69 7a 61 74 69 6f 6e 22 3e 0d 0a 20 20 3c 53 74 72 69 6e 67 20 49 64 3d 22 43 61 70 74 69 6f 6e 22 3e 5b 57 69 78 42 75 6e 64 6c 65 4e 61 6d 65 5d 20 53 65 74 75 70 3c 2f 53 74 72 69 6e 67 3e 0d 0a 20 20 3c 53 74 72 69 6e 67 20 49 64 3d 22 54 69 74 6c 65 22 3e 5b 57 69 78 42 75 6e 64 6c 65 4e 61 6d 65 5d 3c 2f 53 74 72 69 6e 67 3e 0d 0a 20 20 3c	<?xml version="1.0" encoding="utf-8"?> <WixLocalization Culture="en-us" Language="1033" xmlns="http://schemas.microsoft.com/wix/2006/localization"> <String Id="Caption">[WixBundleName] Setup</String> <String Id="Title">[WixBundleName]</String> <	success or wait	1	DC09AC	WriteFile
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\logo.png	0	11997	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 45 00 00 01 23 08 03 00 00 01 7c 7f 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 01 fd 50 4c 54 45 36 3a 40 68 60 30 6b 10 fd fd 00 fd fd 18 4f 4d 38 43 44 3c fd fd 1c fd 7c 24 fd fd 04 fd 08 fd 72 28 5b 56 34 fd fd 20 b5 0c fd fd 04 fd fd 1c 5c 57 34 fd 73 28 fd fd 20 fd fd 20 fd fd 0c 2b 28 19 1d 1d 1b 47 3f 16 fd 03 6f 05 64 55 12 fd fd 0a 39 33 18 fd fd 18 fd 7c 24 75 69 2c b4 0c 43 43 3c fd fd 14 fd fd fd fd fd fd fd fd 68 6b 70 fd fd 01 e4 06 6f 04 75 77 7c fd fd fd fd fd fd fd fd cd fd fd fd fd fd 68 6b 6f 43 46 4c fd fd fd fd 77 0d fd fd fd 4f 52 58 75 77 7b 74 78 7c 4f 53 57 fd fd 35 fd fd fd fd fd fd	PNGIHDRE#|sRGBgAMAaPLTE6:@h`0OM8CD<|$r([V4 \W4s(+ (G?dU93\|$ ui,CC<hkpuw|hkoCFLwORXuw{tx|OSW	success or wait	1	DC09AC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\BootstrapperApplicationData.xml	0	6856	fd fd 3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 75 00 74 00 66 00 2d 00 31 00 36 00 22 00 3f 00 3e 00 0d 00 0a 00 3c 00 42 00 6f 00 6f 00 74 00 73 00 74 00 72 00 61 00 70 00 70 00 65 00 72 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 20 00 78 00 6d 00 6c 00 6e 00 73 00 3d 00 22 00 68 00 74 00 74 00 70 00 3a 00 2f 00 2f 00 73 00 63 00 68 00 65 00 6d 00 61 00 73 00 2e 00 6d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 63 00 6f 00 6d 00 2f 00 77 00 69 00 78 00 2f 00 32 00 30 00 31 00 30 00 2f 00 42 00 6f 00 6f 00 74 00 73 00 74 00 72 00 61 00 70 00 70 00 65 00 72	<?xml version="1.0" encoding="utf-16"?> <BootstrapperApplicationData xmlns="http://schemas.microsoft.com/wix/2010/Bootstrapper	success or wait	1	DC09AC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	64	success or wait	1	DAB56F	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	24	success or wait	1	DAB621	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	36	success or wait	1	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	16	success or wait	8	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	8	success or wait	3	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	8	success or wait	3	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	unknown	8	success or wait	6	DC07DA	ReadFile
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\state.rsm	unknown	794	success or wait	2	DE3F42	ReadFile
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\license.rtf	unknown	4092	success or wait	1	7059B1A5	ReadFile
C:\Users\user\AppData\Local\Temp\{332EE04F-741A-4188-8924-1DBA26FBF992}\.ba\license.rtf	unknown	4092	success or wait	4	7059B1A5	ReadFile
\pipe\BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D}	unknown	4	success or wait	1	DB55A9	ReadFile
\pipe\BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D}.Cache	unknown	4	success or wait	1	DB55A9	ReadFile
\pipe\BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D}	unknown	8	success or wait	1	DB48EA	ReadFile
\pipe\BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D}	unknown	70	success or wait	1	DB49A2	ReadFile
\pipe\BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D}.Cache	unknown	8	success or wait	1	DB48EA	ReadFile
\pipe\BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D}.Cache	unknown	191	success or wait	2	DB49A2	ReadFile
\pipe\BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D}	unknown	8	success or wait	1	DB48EA	ReadFile
\pipe\BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D}	unknown	8	success or wait	8	DB48EA	ReadFile
\pipe\BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D}	unknown	8	success or wait	1	DB48EA	ReadFile

Analysis Process: msiexec.exe PID: **5384**, Parent PID: **576**

General

Target ID:	8
Start time:	07:50:14
Start date:	23/09/2022

Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff76c8e0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	79028	94	30 39 2f 32 33 2f 32 30 32 32 20 30 37 3a 35 30 3a 32 31 2e 34 31 39 20 5b 35 33 38 34 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	09/23/2022 07:50:21.419 [5384]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FF8753CBEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FF8753CBBC6	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: msiexec.exe PID: **3960**, Parent PID: **5384**

General

Target ID:	10
Start time:	07:50:26
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 094F350B1881CEA527676BAF5570DA2D
Imagebase:	0x980000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: taskkill.exe PID: 5268, Parent PID: 3960

General

Target ID:	11
Start time:	07:50:26
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\\System32\taskkill.exe" /F /IM jabra-direct.exe
Imagebase:	0x1120000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5984, Parent PID: 5268

General

Target ID:	12
Start time:	07:50:27
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: JabraDirectSetup.exe PID: 5136, Parent PID: 1240

General

Target ID:	17
Start time:	07:50:36
Start date:	23/09/2022
Path:	C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe" -q -burn.elevated BurnPipe.{9C247021-F0C8-4FC2-9304-77A36769657D} {3D1A53A5-B618-4AC6-9F29-86FEE8B34C1A} 1240
Imagebase:	0xda0000
File size:	602888 bytes
MD5 hash:	6D9E7D60EE823CDB1AEA3F0C4C5B6C56

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DA4173	CreateDirectoryW
C:\ProgramData\Package Cache\{316F5FBF-4536-4A14-8D29-C1A9A8D800B6}v5.12.06601\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DA4173	CreateDirectoryW
C:\ProgramData\Package Cache\{D662C345-04FD-4F6C-AB68-B9BC6D6A5D2F}v7.0.32822.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DA4173	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\DELC182.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	DA3FDB	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	cannot delete	1	DA3FB2	DeleteFileW
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\state.rsm	success or wait	1	DA3FB2	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{50c3bcea-1203-4bf1-9103-09af1bf52966}\JabraDirectSetup.exe	C:\Users\user\AppData\Local\Temp\DELC182.tmp	success or wait	1	DA3FFA	MoveFileExW

Analysis Process: svchost.exe PID: **5268**, Parent PID: **576**

General

Target ID:	19
Start time:	07:50:38
Start date:	23/09/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff61e220000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly