ID: 791294
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 09:38:36
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://www.adobe.com/go/ConnectShell11 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
Process Tree 4
Yara Signatures 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
Mitre Att&ck Matrix 5
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
World Map of Contacted IPs 8
Public IPs 8
Private 8
General Information 8
Warnings 9
Created / dropped Files 9
C:\Users\eyup\AppData\Local\Microsoft\Windows\INetCache\IE\R9BYEINB\Payload11_2022_10_42[1].zip 9
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.Video.DirectShow.dll 9
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.Video.dll 10
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.dll 10
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\BouncyCastle.dll 11
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRClient.dll 11
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRLogTransport.exe 11
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRWindowsClientService.exe 12
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\Connect.exe 12
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\ConnectDetector.exe 12
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\EncoderHelper.exe 13
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.AForge.dll 13
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.AudioProcessing.dll 13
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Dmo.dll 14
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.JsonNet.dll 14
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Log4Net.dll 14
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.NAudio.dll 15
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Nvidia.dll 15
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.OpenH264.dll 15
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Opus.dll 16
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.SharpDX.dll 16
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Vpx.dll 16
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.WinForms.dll 17
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Wpf.dll 17
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.XirSys.dll 17
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Yuv.dll 18
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.dll 18
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\chrome_100_percent.pak 18
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\chrome_200_percent.pak 19
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\chrome_elf.dll 19
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\concrt140.dll 19
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\cr_win_client_config.cfg 20
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\d3dcompiler_47.dll 20
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\digest.s 20
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libEGL.dll 21
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libGLESv2.dll 21
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libaudioprocessingfm.dll 22
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libcef.dll 22
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libcrypto-1_1-x64.dll 22
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libnvidiafm.dll 23
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libopenh264fm.dll 23

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libopusfm.dll 23
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\librnnoise.dll 24
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libssl-1_1-x64.dll 24
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libvpxfm.dll 24
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libyuvfm.dll 25
C:\Users\eyup\Downloads\6bcc8cff-6afa-4c34-b8b1-3a042b0a5bd0.tmp 25
C:\Users\eyup\Downloads\ConnectShellSetup11.exe (copy) 25
C:\Users\eyup\Downloads\Unconfirmed 658627.crdownload 26
unknown (copy) 26
Static File Info 26

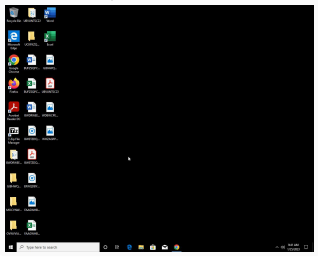
Windows Analysis Report

https://www.adobe.com/go/ConnectShell11

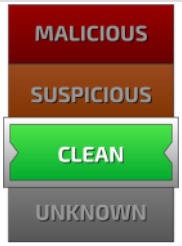
Overview

General Information

Sample URL:	https://www.adobe.com/go/ConnectShell11
Analysis ID:	791294
Infos:	



Detection

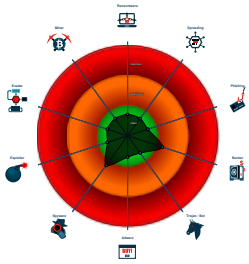


Score:	4
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

Signatures

- Drops files with a non-matching file …
- Queries the volume information (nam…
- Drops certificate files (DER)
- Drops PE files
- Tries to load missing DLLs
- Stores files to the Windows start me…
- Found dropped PE file which has no…
- Abnormal high CPU Usage

Classification



Analysis Advice

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

Sample searches for specific file, try point organization specific fake files to the analysis machine

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

Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 5324 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://www.adobe.com/go/ConnectShell11 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 1780 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2060 --field-trial-handle=1776,i,12495699109451929491,2760430471534754406,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6496 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilReadIcon --lang=en-US --service-sandbox-type=icon_reader --mojo-platform-channel-handle=5628 --field-trial-handle=1776,i,12495699109451929491,2760430471534754406,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6504 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilReadIcon --lang=en-US --service-sandbox-type=icon_reader --mojo-platform-channel-handle=5684 --field-trial-handle=1776,i,12495699109451929491,2760430471534754406,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 7064 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilReadIcon --lang=en-US --service-sandbox-type=icon_reader --mojo-platform-channel-handle=5924 --field-trial-handle=1776,i,12495699109451929491,2760430471534754406,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 7072 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilReadIcon --lang=en-US --service-sandbox-type=icon_reader --mojo-platform-channel-handle=5188 --field-trial-handle=1776,i,12495699109451929491,2760430471534754406,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - ConnectShellSetup11.exe (PID: 6580 cmdline: "C:\Users\eyup\Downloads\ConnectShellSetup11.exe" MD5: 00B6898BF01716F6FE6C1FC1E7256905)
    - ConnectDetector.exe (PID: 6716 cmdline: C:\Users\eyup\AppData\Roaming\Adobe\Connect\connectdetector.exe MD5: 77A4C18414964E80B8BBBADF52319578)
- Connect.exe (PID: 2228 cmdline: "C:\Users\eyup\AppData\Roaming\Adobe\Connect\Connect.exe" MD5: 6B2652F2F1395CC69F6059D5E8248D8B)
- Connect.exe (PID: 5224 cmdline: "C:\Users\eyup\AppData\Roaming\Adobe\Connect\Connect.exe" MD5: 6B2652F2F1395CC69F6059D5E8248D8B)
- Connect.exe (PID: 6124 cmdline: "C:\Users\eyup\AppData\Roaming\Adobe\Connect\Connect.exe" MD5: 6B2652F2F1395CC69F6059D5E8248D8B)
- **cleanup**

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.

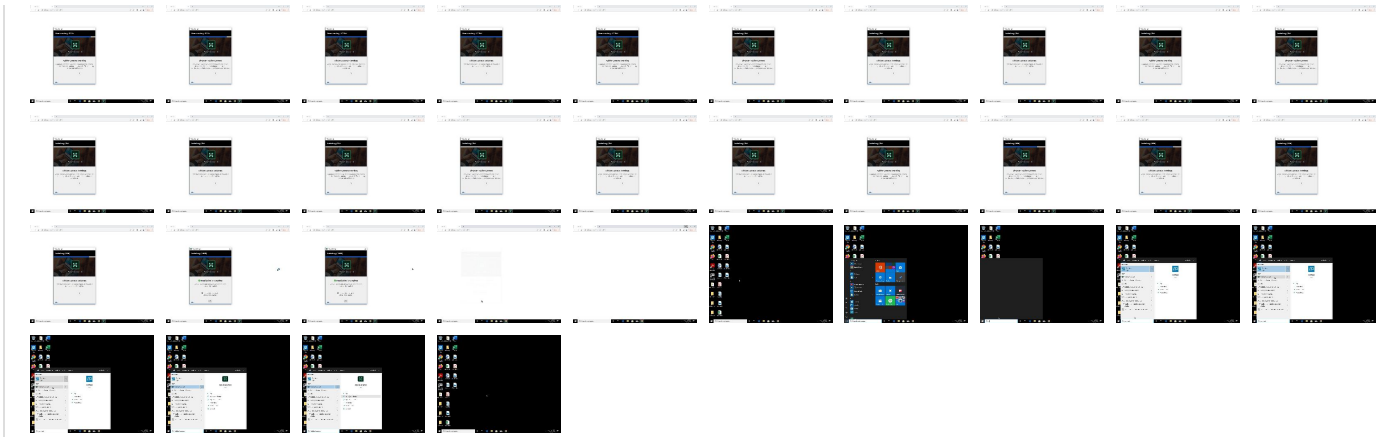
Mitre Att&ck Matrix

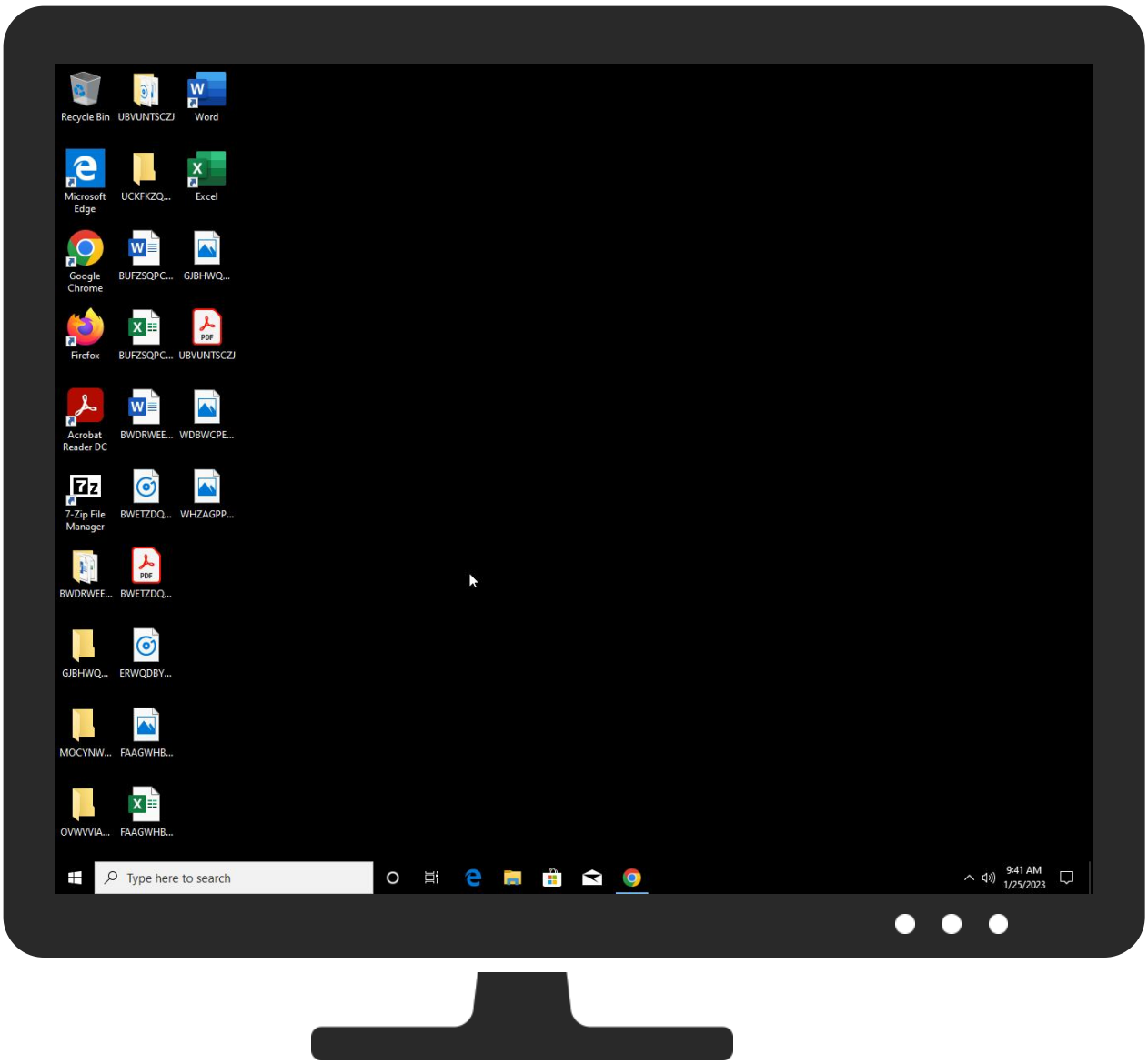
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 Windows Service	1 Windows Service	1 3 Masquerading	OS Credential Dumping	1 Process Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Process Injection	1 Process Injection	LSASS Memory	2 File and Directory 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	At (Linux)	1 1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	1 DLL Side-Loading	Security Account Manager	1 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 Registry Run Keys / Startup Folder	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

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
https://www.adobe.com/go/ConnectShell11	0%	Avira URL Cloud	safe	
https://www.adobe.com/go/ConnectShell11	0%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\eyup\Downloads\ConnectShellSetup11.exe (copy)	0%	ReversingLabs		
C:\Users\eyup\Downloads\ConnectShellSetup11.exe (copy)	1%	Virustotal		Browse
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.Video.DirectShow.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.Video.DirectShow.dll	0%	Virustotal		Browse
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.Video.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.Video.dll	0%	Virustotal		Browse
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.dll	0%	Virustotal		Browse
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\BouncyCastle.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\BouncyCastle.dll	0%	Virustotal		Browse
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRClient.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRLogTransport.exe	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRWindowsClientService.exe	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\Connect.exe	2%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\ConnectDetector.exe	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\EncoderHelper.exe	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.AForge.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.AudioProcessing.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Dmo.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.JsonNet.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Log4Net.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.NAudio.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Nvidia.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.OpenH264.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Opus.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.SharpDX.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Vpx.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.WinForms.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Wpf.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.XirSys.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Yuv.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\chrome_elf.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\concrt140.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\d3dcompiler_47.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libEGL.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libGLESv2.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libaudioprocessingfm.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libcef.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libcrypto-1_1-x64.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libnvidiafm.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libopenh264fm.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libopusfm.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\librnnoise.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libssl-1_1-x64.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libvpxfm.dll	0%	ReversingLabs		
C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libyuvfm.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

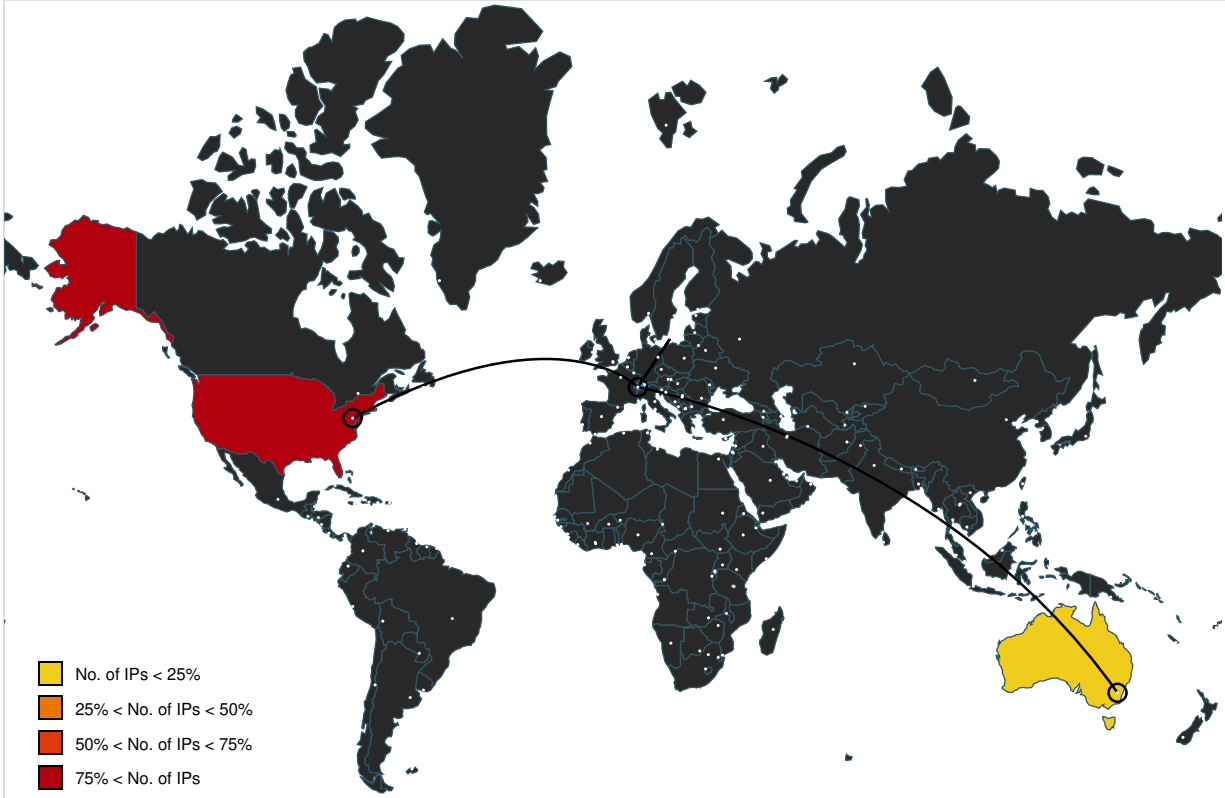
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.67	unknown	United States		15169	GOOGLEUS	false
142.250.185.78	unknown	United States		15169	GOOGLEUS	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
2.16.238.27	unknown	European Union		20940	AKAMAI-ASN1EU	false
172.217.18.4	unknown	United States		15169	GOOGLEUS	false
2.19.126.84	unknown	European Union		16625	AKAMAI-ASUS	false
2.16.238.9	unknown	European Union		20940	AKAMAI-ASN1EU	false
2.19.126.92	unknown	European Union		16625	AKAMAI-ASUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.184.205	unknown	United States		15169	GOOGLEUS	false
142.250.186.99	unknown	United States		15169	GOOGLEUS	false
142.250.74.196	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791294
Start date and time:	2023-01-25 09:38:36 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://www.adobe.com/go/ConnectShell11
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	21
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean4.win@39/50@0/86

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- VT rate limit hit for: C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRClient.dll

Created / dropped Files

C:\Users\eyup\AppData\Local\Microsoft\Windows\INetCache\IE\R9BYEINB\Payload11_2022_10_42[1].zip

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	136088419
Entropy (8bit):	**7.998238142178281**
Encrypted:	**true**
SSDEEP:	
MD5:	B14D7997ED15894BEFF9D994E5324B41
SHA1:	1930AB83F8E635CCB0F6696F71BC2925B1C633B4
SHA-256:	15826C13312125EAB6EA3C42F873D45A19D09F05E2BA7099BC19B4A93B0C7511
SHA-512:	BF49762C6AFA8FA1D5FD34B801162A9E6D2D1622F5984E1F40238A5AF0FE2D638FBEF230C4D42423FBF507B8404ED9FA0D52CC60C260159659565FE8680F6305
Malicious:	false
Reputation:	low
Preview:	PK.....;l[U..P.=...o.....AForge.dll.\wX.[..3...A.....j(R.4.EAA...D.....b..}v...u}..{y..{y...{gR.....?vwp..9..9..;.....+B[.{.B.~..i...m4?.J:..[...h..i.(G.R.u.l.HS..)T...TQ.Z&.....P..7}.t..{.....lu....=I.X.....X.....U%Bv../.#..MFl.b.D.....!....'4.B.mLp.N^....f..+.M.=.4ZM.....i.J5.Z.....]L.n..b.mH.3t8..m..y.....a...~4.T....t=..lc....>.^....f.cY..W....p.l[G..!....}Y..lO..i74.6,l..%.....].8a...&...%.....\/..T.:c..y...k...x.SQ< .q.....$.....!...H.....H..j..6c...3....*{...^.,...x...;..q-...m..4...k.M..&.....5...d@.f..K.%..).d.+.NPO....e.pe.e..Z./.as..~.m.i+..MZI..a..KF..2...l.!...{..B.\|."S...^E7...(~.>.P...B.9..a.X.....4L!.U:.v..b.Y...6..].....t.L..<..<m0...JN....b..:..!.b..A.>[.2.....M....4....eDbW..?..,.d.XjtS.....@.<...p...D..yjw.Zh=.Z.....x5...gX.....$.....E.E..s6^.C.....d....`(P..v..Z..8..... 7.q`./sm.P7.8.$8.}....3....x/.]9...n....;.....Q.{r|4.u....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.Video.DirectShow.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	72160

Entropy (8bit):	6.529928219154391
Encrypted:	false
SSDEEP:	
MD5:	F2D4A234480D899864AD5D702890F1B7
SHA1:	A5D7C5D44BFC44769D02C4736A86EC5119B8E6C9
SHA-256:	DFF6E2D4BDCEE7D012FBDE3A161C42F9FA15295A98C49A3D45CDF2AED395F3F7
SHA-512:	E05CA56BCE0D021515B075CBCBA7E7F1FB6A30EC910ED52DAB8AEC12DC3BD1E3FF773150E9379EB8546A7851F98359A5116F4EAA3E9A07308A76417A76A1D79E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q.Q.....!..... ... .@.. .....`..... ..@.....T...W.... .....)...@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....0|.....@\.....P .....nM.N.Z...K..Z..+.\.`.).....p.>S.5.HV.R....|..K}.....L..N6..+..`S..H..3.LM.WJ Q....q.F....._)..DQ.....]2....X.....3+.....(....*.0..3.....~....(...., r...p.....(....o....s.....~....*.~....*.....*...0.....(....r[..p~....o.....t....*.0..... b..3 ... .C. ....s !..... .... .]..... ....;. ....s!..... `..3 ... .C. .... .

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.Video.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	31712
Entropy (8bit):	6.375575026807124
Encrypted:	false
SSDEEP:	
MD5:	53402447207D3969CCBD5D42D4DC448B
SHA1:	881E39FA58A44EEDBD9660A070096FC87BDFF730
SHA-256:	65C709F5511B10F41013AE71B04999BD61EE1209199E8CC1D498E17287C04FB0
SHA-512:	F4A9583E72A88939C1CF6CBA41AAEDA25FC87B378320D38AA7595AAA08A00853FD79B4685BB3243F1A4016EA842DFB7630CBFE34DC9539BEF25DFA462158EBFF
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q.Q.....!.....J.....h... .....@.. .....1... ..@.....g..K.....P.....R...).....dg..... ....H.....text...4H... ...J..... ..`.rsrc...P.....L.....@..@.rel oc.....P.....@..B.....h.....H.....H:...-.....P .....{hV[h..j...+I....k.rQ2..P+.C..O..k.p....`.v..W.+...&....o..".U..0."n.mZ.p.T..h..Z+...Q ...Rz}.j.....v..=./....MI4....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*6.{.....o....*6.{.....o....*6.{.....o....*6.{.....o....*..{....*..{....*"..}....*2.{....o....*2.{....o....*2.{....o....*....0.....{.....}.....*.0.....{....o.

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\AForge.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	28640
Entropy (8bit):	6.398055190229929
Encrypted:	false
SSDEEP:	
MD5:	7ABFC5592FA3F1F3107D44854D11CD5A
SHA1:	75C52AF7A2365CE6194A9181C4F49A5749FEED71
SHA-256:	D7FB60D87973C85F3B3E5E2160F576ABFAC1B1D0C2F8F0BF199393EB32B6EC75
SHA-512:	CC447359DFB8FA94E696B66EC0180DA82D240171F46C3A0A4B30A16ECED04993502AF32D3D0D304B5000E29A479FE5DB1A32FB62D340C70952227E45905A1ED0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q.Q.....!.....>.....\... ...`....@.. .....Q.. ..@.....\\..O....`..(.....F...).....[..... ....H.....text....<... ...>..... ..`.rsrc...(....`.....@.....@..@.rel oc.....D.....@..B.....\.....H.....6.. %.....P .....A..R.N.W.9z..W....C.L..Q.\[I..&.*G..J..D.%A...|M..h.T.r%..H..Lz...9...G...: [..1J.9.b-.....Q.0S.....T{..ix{g...N.....{....*z.(.....}.....}.....i}....*r.(.....}.....}.....}....*.0..'.....{.....{.....{.....{....(.....*b.{.....{.....{....(....*>..}.....}....*.0..-.....{.....{....Y..{.....{.. ..Y...Z..ZXl(....k*....0..(.....{....k..{....Y..{....k..{....Y...Z..ZX*...{....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\BouncyCastle.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2058208
Entropy (8bit):	5.969278031717462
Encrypted:	false
SSDEEP:	
MD5:	5A476B11A9309B6071B305136B28DDF6
SHA1:	E8AFE5C560B37BAC951F0CDA44C3CD51A82416E2
SHA-256:	36F7ED5D21CEB669FFE3645EBB9AEA2BBF20E12ECB198ED869FEA240793BFC73
SHA-512:	9E31D7023C25F89E7BDC5E65AC4A315DDD4A13903A908661A4D422C3D189010315D45CB7E61B7CDE8BF92700AC430A2CEFB2CFA15B280CBD5F99A915C2198 E6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*C^....." ..0..4.....n@... ...`..... .....: . ..@.....@..O....`..L.....>...)..... ....H.....text...<2... ...4..... ..`.rsrc...L....`.....6.....@..@.rel oc.....<.....@..B.....P@.....H.....?.....~....-*(....o....o....o.....~....-.~.....~....*..(....*.*N.(.....(.)..}....*..(.....(.....s.'..s .*..s.)..}....*..0..=.....(.....(:.....o....s....z...(.....o^...s.'..s.*..s.)..}....*.....f.(.....(....s.)..}....*..(.....s.(..s.)....(....s2*..s.)..}....*...0.."....{....o.)....,..o4*..o.'..o....*.*...0..".... {....o.)....,..o6*..o!)..o.(..*.*...0.....{....o.)...

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRClient.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1078240
Entropy (8bit):	6.324023488842526
Encrypted:	false
SSDEEP:	
MD5:	8E5BBF03A5535F0150D8CF8F0527E640
SHA1:	54E28824D81D6B9369F081652157FB68FAEACF70
SHA-256:	6D581AA932104C5B8C198536D85708054EFF1BB106D5E161C857DD2F81AD1FD5
SHA-512:	D64DA8BFC98B0BB9752EEBC3B741E3D201896535E59108CCAA203B185F59BEF7334285F7FA38EBAC7B64A4E68364B635E1901DBC378A52E198626E36C330B58 D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....3..l`..l`..l`q@.`..l`q@.`e.l`q@.`..l`..oa..l`..ia..l`..ha..l`.#.`..l`.#.`..l`.. m`>.l`W.ea..l`W.la..l`W..`..l`...`..l`W.na..l`Rich..l`.....PE..d.....^....." .....p'.....`A.....0k.....,q..... ..d....J...).....p.....(...@.....p.....text...R..... ..`.rdata..r.....@..@.data....q.....D...x.....@....pdata..d. .....@..@.tls.....L.....@....rsrc.....N.....@..@.reloc.....2.....@..B..... .....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRLogTransport.exe

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	565216
Entropy (8bit):	6.5823538059796
Encrypted:	false
SSDEEP:	
MD5:	793EF24C0B30AC343E9F5DD2550B7E7D
SHA1:	DDDAAA80E2C6EE2D8C321B8FBABEEFBEBB27D365
SHA-256:	1EAD67900D3A3DA1AF364899B944E0DE4A101BC3C8CAFA8F179A0BF32911ECD1
SHA-512:	93427A50B9028C6C7AFF7FD8D5B6FFB89B3FF54BB0A7EDFD502057EFF63F2FDF76DC6397F2319C3837ED8E979098775ED425F1AE825201F57A5E429DC4C455A A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}_4....}_6.e..}_7.....F.....<.....o..[.....[.:..... R....[.....Rich.....PE..L.....^.....6...L.....p.....P....@.....o.....@.....h...d...`.....v...)...p...K.....p.....|..... ...@..... ...P.....text....5.....6..... ..`.rdata.....P.....:.....@..@.data....-... .....@....tls.....P..... .....@....rsrc.....`....."..... @..@.reloc...K...p...L...*.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\CRWindowsClientService.exe

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	821728
Entropy (8bit):	6.252719655882823
Encrypted:	false
SSDEEP:	
MD5:	B1D2B5079FC5859CA3D5149EE7AEACCF
SHA1:	0EC38B6E2B29B56D62C565241D97DD143BB50EBA
SHA-256:	EF5FFDEFB493DA1898246C8D9F202E218188C28C6FCD695F34B0D12A2136D995
SHA-512:	F0DDD567B6C02127B91F7D61D1FF0F2F27BF811147A3184CAC7B70801F533B8127BE0C2A9003915BEC6B3212FBC1AF43BF91900132E60058CE02B355A1F93558
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-...~...~...~C:G~...~C:E~P..~C:D~.~.....~.....~.....~*Yf~...~*Y} ~.~...~K..~e...~e.!~...~..!~...~e.....~Rich...~.....PE..d.....^....."....0.....@.....~c...`.....p\.....0...v..... S...`...).....p4..p.....x5..(....4.....text...^..... ..`.rdata.....@..@.data....J...p...$...^.....@....pdata...S. .....T.....@..@.tls..... .....@....rsrc....v...0...v.....@..@.reloc.....N.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\Connect.exe

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37045216
Entropy (8bit):	7.2717345853234185
Encrypted:	false
SSDEEP:	
MD5:	6B2652F2F1395CC69F6059D5E8248D8B
SHA1:	0510D81EE1EEAF0CEE41A54A3ECCB3C01314E635
SHA-256:	62FE0232955662E7F06351A8B7DADC7FDF0B603B1F42F2CA7953A2398E2664AE
SHA-512:	4227CA344D4F52EEFB30E8AFB09A487A6B68DB104E1E41E443647C89E9A75075874D5C599D91C778D10CA857FFF019A077AD1763B722303F1332CB83E1A04DA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....h.....!..L.!This program cannot be run in DOS mode....$.....NF...'...'...'...W...'..IO..&%...y...'...H..,'...R../'...W...'..IHL..'..XR...'..XR ..5'...R...'...'..@'..XR..x'...W...'...W..?'...W...'...W..N'...R...'...'...$...R...%...R...'...RN..'...'&..'...R...'..Rich.'.....PE..d....@Zc.....".....o..R.....L.....@..... .....@9.....z.5...`..... ....Y.....Y.....D.....5..)...p8.|.....p.....(.....y.8.....o.....`.....text....o.....o..... ..`.rdata. .h.....o.....o.....@..@.data...`.N..`....J..F.....@....pdata..D.....@..@.rodata.....@..@_RDATA.....@..@.rsrc.....Y..... .Y.....@..@.reloc..|....p8.....R4.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\ConnectDetector.exe

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	659936
Entropy (8bit):	6.303894150235615
Encrypted:	false
SSDEEP:	
MD5:	77A4C18414964E80B8BBBADF52319578
SHA1:	389A72B64274B2C171548A6C899D4BBB0EE17CDF
SHA-256:	1BB861DCA97F170E7B454E136936A9838133EE7977887403F45362E019BA9F2F
SHA-512:	61ACC7AB259975915D312E16F63781BB9C5B841DA162E7F27E6174481EEA2AF31F64B44CB1D30269B5F36C42D1ECF49A91764754FB6E899B0582C8B5727709D9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V.A.8SA.8SA.8SU.;RJ.8SU.<RT.8SU.=R.8S..<RQ.8S..;RK .8S..=R..8SU.9RH.8SA.9S.8S..1RD.8S...S@.8SA..S@.8S..:R@.8SRichA.8S.....PE..d....=Zc.....".....t.....P.....@.....i....`..... .....d.....8e.....4M.....)...p.....p3..p.....5..(....3..8.....0.....text..... ..`.rdata.....@..@.data.....>..... .....@....pdata..4M.....N...$.....@..@_RDATA.....r.....@..@.rsrc...8e.....f...t.....@..@.reloc.....p.....@..B..... .....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\EncoderHelper.exe	
Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	480224
Entropy (8bit):	6.709169198224255
Encrypted:	false
SSDEEP:	
MD5:	136A540ED3C87AF402401646FF8C09A7
SHA1:	9C3228A4634039D826144FCB880234394B1CACAA
SHA-256:	C6616BD25BA2DF064BF9A7CF18C301BE03472CE73CF9A998FC9682914BD2BA92
SHA-512:	631C695A3B3C5BDD910C2125871D9B2AB1705A97478FEE58DD2AD677F6A46FC74DA15077B775D6034C768A4D29FB7C29E404719945AE09B1DDB30ACDF95494 3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6.T.X.T.X.T.X...i.U.X...h..X.]...u.X.]...o.X.]....X.sD#.].X.T.Y.(.X.] ...Q.X.J...U.X.]...U.X.RichT.X.....PE..L....p].....L.....n.....@.....@.....@.....p|..P.....*...)....., ...text..... ..`.rdata..p.....@..@.data...._.....t...t.....@....rsrc.....@..@.reloc...;..... <.....@..B..... .....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.AForge.dll	
Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	23008
Entropy (8bit):	6.5694648027398905
Encrypted:	false
SSDEEP:	
MD5:	042721E52D2319341D6DFA68142A178F
SHA1:	F7921E86921AE26B73EC2F46DC27E00DD4958810
SHA-256:	CBF3FDED17EB548969B3C295A6537487AE28DE69A6C91466690A571C21061C27
SHA-512:	CC4AECCFA16257E7B21BD960D0E76E96B311D01419251233A4EC66FE1B8CC120514871142A89AA71604C06B266D913E84F206C38D0CAB42710270EDB64B38EE C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0..&.....D... ...`..... ..... .`.....@D..O...`..0.....0...).....C..... ..... ..H.....text....$.. ...&..... ..`.rsrc...0....`.....(.....@..@.relo c.....@..B.....tD.....H.....8(.....{....*"..}....*..{....*"..}....*..(....*..{...*...0..n.....s....s....~....s....o.....+#.o....t.....o .....o....s....o.....o....-....u.....,...o.....o....o....&.*...../K.....r...p*6.(....(!...*....0.....~....s.....,o.o".....,T...o.....++.o....t.....o.....o#...($...,.....5..X..o....-..%.u.....,...o.....o% ....1...o&...*.*..*.....!.7X.....0.....s'.....o(....8....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.AudioProcessing.dll	
Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	21472
Entropy (8bit):	6.642084094697324
Encrypted:	false
SSDEEP:	
MD5:	65DD938E2C4FB23F965426639A12472E
SHA1:	7AA7E4E8C552409E0E6B41778FFE811E1378F2E9
SHA-256:	FA58BE83A100D8B1E52E25B3A35A433BC2A7A90309A7ECDA3B4A368A49A7FE47

SHA-512:	D97D1694F08F5D341E342A23EA9C3CE26D4836F9F2FE4D75A2915A270CA00A5A3EDB19E9F10C64F5F8A7DC706E603BEA5E2FD76C50470576860E18CE0F50318 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....3.a.........." ..0.. ....?... ...@....... ....e... ..`.................................8?..O....@..X...........*...)...`.......>.. ....H............text........ ... .`.rsrc...X....@......."..............@..@.rel oc.......`.......(..............@..B................I?......H........%...{....*f.. .....(....(....}....*.r...p*"..(....*&...(....*&...(....*&...(....*N. .....s.....(....*:..s..... (....*.. ....}......(..........(......o.....o....s....}....*V..o.....(......(....*..0..b........{......,W....(.....{....o......,...o......o.....o....o....&*.-!(....o ....3.(....o!....3...o....*...0...........{......,...o....*..("....{....,.. {....o......}....*.0..o........(#...($....3.r...p(....&+.r

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Dmo.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	84960
Entropy (8bit):	6.281695763074729
Encrypted:	false
SSDEEP:	
MD5:	797408A86A1E26BA934E1717089D19F0
SHA1:	77070A968A2AC31E6EAB201A9811D158B83314A2
SHA-256:	BD7CAFA1840E21DEABA9EDFDED81FC19074F642315B4ADC6D4FF5726B6D74D3F
SHA-512:	CC9197978716D1FF47D098C7238A7F01721BDC4F8E45CC456B5A80DE573747F9395896AD647E631678561422C060171791816F7052C159C24D21E9A4766FD4A1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....3.a.........." ..0.............v7... ...@....... ....Lx.. ..`.................................$7..O....@..............."...)...`.......5.. ....H............text...|.... ....`.rsrc........@......................@..@.rel oc.......`....... ....@..B................X7......H........f...r...p*2.(....(....*6..s(...()...*"..o*...*.*.(2...*.(s...*..{....*"..}....*..{....*"..}....*..{....*"..}....*.. {....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*". .}....*..{....*"..}....*...0...........(+.....9...

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.JsonNet.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	16864
Entropy (8bit):	6.8167359286211875
Encrypted:	false
SSDEEP:	
MD5:	E5E414993A811DA7D0E0168B24568905
SHA1:	1DA475B68A926829DE06C84AEEB5090176895BAA
SHA-256:	B07A1A9EB60BFA8353996915CB2775A2943C5F911E0F5D8697A169B8CB37062F
SHA-512:	463B0CF4AA0EF77BE6B6A847A03C300591C157A0314B0D6FA28D8914BE87C8EEAB4211DFEE9700BBA01DF2F62F3BA740ADE47C5A1237E59EA1CC4A154D1C7 A4C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....3.a.........." ..0.............N-... ...@....... ....`.................................,..O....@..$...............)...`.......+.. ....H............text...T.... ....`.rsrc...$....@......................@..@.rel oc.......`......................@..B................0-......H........ ....~....*.......*.~....*.......*...0..".......(......,.........(....*......(....*...0..........(......,...(...+*.(...+*.. (....*BSJB............v4.0.30319......l...H...#~..........#Strings............#US.........#GUID.......4...#Blob...........WU.........3...g....... ....l.....*..............................

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Log4Net.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	16864
Entropy (8bit):	6.816697483580518
Encrypted:	false
SSDEEP:	
MD5:	BC04AD8DA42F4066065D11ECC571691D

SHA1:	096C3502D59BF8B2FEAD503CE350EAF5DE83A32D
SHA-256:	3151AEF429915E30AA7DB46F19AE53A5DDDBDDA12B7116CAAB2369CA841DCA21
SHA-512:	EAAFEC5D58F3F7FC95FC3FE5F7D39EDD33C7E0D4E0085C39E741DCEB24A1A33C785FC06D1730ECF2BAAD78B979668B833A378AC2FC8255BFE92FA87E5B2DFD4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0.....N-... ...@..... ....`..... .....O....@..$.....)...`.....+..... ....H.....text...T.... ....`.rsrc...$....@.....@..@.rel oc.....`.....@..B.....0-.....H.....(!.....f.(....r...p(.....(....&*...0.....o.....YE...../...F...]...*~.....o.....o....o....*~.....o.. ...o....o....*~.....o.....o....o....*~.....o.....o....o....*~.....o.....o....o....*V.....(....(.....*...BSJB.....v4.0.30319.....l.....#~..P.....#Strings....H.....#US.\.....#GUID...I...0...#Blob.....WU.....3.....^.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.NAudio.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	29152
Entropy (8bit):	6.5056521509159335
Encrypted:	false
SSDEEP:	
MD5:	A3BB2B8E6A73CF5D3C152AF36FA93C0F
SHA1:	9057CF1BDEB7BF7A84C8E5E52F6C67620E06ACE5
SHA-256:	74593E4567F6064E77CF9E3CCD951FAAFFB28911539BFE99DDCCBC66FBC24E19
SHA-512:	15218BEA1A7AD980870A013B35B07F7E6F78BCA4A77A2F039620717834E264E2DB01864F22CC3EAC3742F2F05A1BC8AF1E2EFDBC588D64873531421823F00D42
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0..>.....\... ...`..... .....Z... ..`.....[..O....`.. .....H...).....Z..... ..... ..H.....text...$<... ...>..... ..`.rsrc... ....`.....@.....@..@.rel oc.....F.....@..B.....\.....H.....2...(.....{....*"..}....*..{....*"..}....*V.(.....(.....}....*.0..@.....(....o.....{....Y.(.....(....o.....(.. ..o.....{....X...(.....*"..(!...*.r...p*.0..Z.....s.....s.....+3.(.....(.....o.....(....s....o.....X..(...2...o!...o"...&.*.s8...%.}....%s#...}....%..9...s$...(%...{....*J.....s$...(&...*.0..\..... .o'.....s(.....,E...o)...o*....+!.o+.....o,....o-...(....,.....o/...-....,.

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Nvidia.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	28128
Entropy (8bit):	6.419430083083177
Encrypted:	false
SSDEEP:	
MD5:	E6855C04E63490063D0EDF9054254115
SHA1:	E89165247310A02FEA14A51F9EECC4739F85E369
SHA-256:	C3FB9F335930168B73F1D3500AA7944398C42EC2EB6F17B78388B70FBA8EFC39
SHA-512:	EC3A025C6ACD11CF9AA4A5897E457DDAE7C1EA67BCCE90BB2FBFDB511876EE28AD65CD5C5B7201D42951AFD70BF773F3DB823314F2239D4E4C3E2BF2B869E754
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0..:.....X... ...`..... .....o.. ..`.....tX..O....`..(.....D...).....<W..... ..... ..H.....text....8... ...:..... ..`.rsrc...(....`.....<.....@..@.rel oc.....B.....@..B.....X.....H.....,.*..... .....2.{....o<...*6.{.....o=...*..0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*n...(.....o....s>...}....*....0.....(.....(....-w.{.....(.....oD.....,0.o....,(.o....o....1...o.....o.....o....o ...&.,...(!....{.....,....o"....(.....,.r...p(#...*N.{....oA.....}....*2. {....o6...*6.{.....o7...*2.{....o:...*6.{.....o;...*....($.....o.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.OpenH264.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	55264
Entropy (8bit):	6.1599890245758235
Encrypted:	false

SSDEEP:	
MD5:	D0C3EE892C6A228769790CA621A930A1
SHA1:	54A15CBD69C5558853DD6BFDF48D8AB2FAE9EAE4
SHA-256:	5F9C2005FE2717DF76C73F56C3966E080A1F48BFF033652587DECC97F111D35E
SHA-512:	CDDACB053C1918E42C254631EA7769A2170BFD48D53DD7DEF7755A321735F44D54CA896BD3D4C147436EE27F5DA491F8570237DC09883476FD1CB11C82FA06
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....3.a.........." ..0.............&.... ....g.. ..`....................................O.......`................)... ....H............text...,..... ....`.rsrc...`..........................@..@.reloc........ ....@..B.........................H.......@L..\u..{....*"..}....*..(....*>.(.......(....*.~....*.~....*.~....*.~....*.~....*.~....*.~....*.~....*.~....*.~....*.~....* .~....*....0...........s..........s..........s..........s..........s..........s..........s..........s..........s...........s...........s...........s...........s.........*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*:.(.... ..(....*.~....*.~....*.~....*.~....*.~..

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Opus.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	34272
Entropy (8bit):	6.2922032052740065
Encrypted:	false
SSDEEP:	
MD5:	30031A90FCB9CBD701D7B76738EEB497
SHA1:	78E68C62B4C4B7CD9C2EB695C9DBB01C6232F50E
SHA-256:	616A9C369F92A3263959F78861956D8DFC12B1CAA8125ED0BC920B5799684ED7
SHA-512:	4B8D57A23053E9608E9D6B8DFDADF594A73DE76424EBBD73C67EB6B2A5AEE52DCEE58BA8BBC02C8F9DE5C50350744E5CEF96F48E0A2C2CCD3D2E123E098E F695
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....3.a.........." ..0..R..........*q... ....a... ..`.................................p..O...................\...)...........o............................................... ............... ..H............text...0Q... ...R.................. ..`.rsrc................T.............@..@.rel oc...............Z..............@..B.................q......H.........84..h;...{....*"..}....*..(....*:.(......(....*.~....*.~....*.~....*.~....*.~....*.~....*.~....*.~....*.0..y....... ....s......... ....s......... ....s......... ....s......... ....s......... ....s......... ....s......... ....s.........*..{....*"..}....*:.(......(....*.~....*.~....*.~....*.(F...s......... ....s......... ....s.........*..{....*"..}....*:.(......(.. ..*.~....*.~....*.~....*.~....*.~....*.~....*..0..

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.SharpDX.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	23008
Entropy (8bit):	6.641546690599725
Encrypted:	false
SSDEEP:	
MD5:	EDD820F6AABF88214032398717E5B3F3
SHA1:	A4AEE2576C3014307722BC5AD3FB3CF180A36438
SHA-256:	87DDDE6A84B04E63D5BDECF71667945321B4AECCD7F98E5128F49A666C3E3F0B
SHA-512:	4CF9B0EACE54512D37CEC3376FDD01EF05C01291BDF49BD55E828802D62E2ED6D1773512BF26A812BB5EF77EC631E8ED69B5A0A0AECDDFB7AB2914EC0058E 103
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....3.a.........." ..0..&...........E... ...`....... ...............................l.. ..`..................................D..O....`.. ............0...)...........C.............................................. ............... ..H............text...4%... ...&.................. ..`.rsrc... ....`.......(..............@..@.rel oc..............................@..B.................E......H........(..r...p*..{....*..{....*:..}.....(....*..{....*:..}.....(....*....0..1........s....}.....~....}.....(....(.............. (....*....0..-........s....}.....~....}......(..............(....*....0..-........s....}.....~....}......(..............(....*..s....}.....~....}.....(....(.......(....*..s....}.....~....}......(.......(....*..s....}.....~....}......(.......(....*..0.. ....(....o ...-..(....o!...-.r...ps

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Vpx.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	38368

Entropy (8bit):	6.226919736548019
Encrypted:	false
SSDEEP:	
MD5:	41878D1047F5D27B470D4968736AF2A3
SHA1:	076ADFD9A02063113405BDB0D3D18050022B0CD5
SHA-256:	C2AA79494B3389EF5315D0E8783359EE5BE688C12E19597ADB2607BFCA43B19B
SHA-512:	B0A6EE75CDF34A861358C10C235C4453FBE062593CDE091851882CD0E8C5DF3C2FF205B0CBE940B6D674E945BEFDF7217DD98A896FA40F9726687E5DB3AC52 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0..b.....b.... ....`.....O.....I...)..... ..... ..H.....text...ha... ...b..... ..`.rsrc.....d.....@..@.reloc..... .....j.....@..B.....D.....H.....p7..hH.....r...p*..*2.s....(!..*:.(.....(....*..(....*.r...p*....0..".....s....(*....($.....ox.....(+...&*:.(.....(....*.r 1..p*..*2.s....(!...*:.(.....(....*..(....*.rI..p*2.s....(*...*:.(.....(....*..{....*"..}....*..(....*:.(.....(....*.~....*.~....*.~....*.~....*..s.....s.....s.....s.....*2.{....o....*6.{.....o....*...(....(.....s.... }.....{.....o ...o....*...0..._.....(.....(..</td>

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.WinForms.dll	
Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	26592
Entropy (8bit):	6.596707784718348
Encrypted:	false
SSDEEP:	
MD5:	0F15CBBF554E12B62F5FB4A8CD2253E3
SHA1:	0F4D36FBB83C403B07CE29B8B0D96BB55FE3B77B
SHA-256:	A056FC0CED4006867E2574CBD0EA4AE8272DDFFA87762D85B17DE30C643071E8
SHA-512:	7955DD50261DB69B770F04792FE8B187BCD63D8A7942ECABF891DDAE6F1530FC2C0973A3EA6D7C5DAAD4DFD1D46B104B5772716BF7BCC2543109EBBAACF77 F03
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0..4.....S... ...`..... ..... ..`.....S..O....`.,.....>...).....pR..... ..... ..H.....text....4... ...4..... ..`.rsrc...,....`.....6.....@..@.rel oc.....<.....@..B.....S.....H.....+...&.....{....*..-.r...ps....z..}.....{.....s....o.....u....}.....(....*..(....*:..(.....(....*..o.....3..(....,.. {....-.r5..ps....z*&...(....*>..(.....(....*J.(....o.....o....*J.(....o.....o....*....0..3.....s<.....}.....}.....}.....(.....=...s....(9...*..0..i.....(.....(.....(.....(.....o.....+.....o ...(.....X. .....i2..(....o!.....(....o".....o.....o#....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Wpf.dll	
Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	27616
Entropy (8bit):	6.511491014558084
Encrypted:	false
SSDEEP:	
MD5:	EB5D3923C13EE0B9F5137D86B680310D
SHA1:	A01BFE4DEAB28471878A0304B51DDCF26A2E3D57
SHA-256:	9CC587C2AA3899500A79BBBA7C2240574C5611EB5EF8CA20B9AD17361BB5BC4C
SHA-512:	5539A93274CDE2C08F5FE473BC16C693D8E909FF4FE58AE9324B207B749FDF35508C8245188372C51D4A16AC216DB56817892084CAECC056092EBAC4369EC37
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0..8.....W... ...`..... ..... ..`.....pW..O....`.....B...).....8V..... ..... ..H.....text....7... ...8..... ..`.rsrc.....`.....:.....@..@.rel oc.....@.....@..B.....W.....H...../..t&.....{....*..{....*.0..F.....YE.....+(.{.....o....+..{.....o.....+..{.....o.....}....*..{....*". .}....*.r...p*F.(....o....(....*J.(....o.....(....*J.(....o.....(....*z.s....}.....(....(.....(....*j.s....}.....(.....(....*j.s....}.....(.....(....*z.s....}.....(....(.....(....*j.s....}.....(.....(....*j.s....}.....(.....(....* R.....s.....()...*....0.....s+.....}.....}.....{..

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.XirSys.dll	
Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	modified
Size (bytes):	29664
Entropy (8bit):	6.435785332756873
Encrypted:	false
SSDEEP:	
MD5:	B18A5755E3F42D5B00C0DC82C82D5E00
SHA1:	C4981E3EB180FFD616B864546FBBD5A59E61B16A
SHA-256:	CCBF2B5596D3AA4F75EF9BB98D7F1DD2F5650DDFCEFD1CB615264D89C5E23514
SHA-512:	43ABC9D9CBA9287D5C78D917A6C21DB037F250CAC2C6BC991FAE91934BA1E20A4133B095618C2130FDFB06F8B1F8C999E3D318E70D1EDC27AD2ABC26133D026
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0..@....._... ...`..... .....{y.. ..`.....^..O....`.....J...).....]..... ..... ..H.....text... ?... ...@..... ..`.rsrc.....`.....B.....@..@.rel oc.....H.....@..B.....^.....H...../...-.....~...*.....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*.....(...*..(... ...(.....(.....(.....(.....(....(....*.0.....s.....(.....*..0.....se.....}.....(....r...po....-..(....+..(.....(....o.....Yo.....r...p..(....(.....s....%.o....%.o.....o....r...pr1..prE..p.(.....(....(....(....(....(....o....(.....f...s!...o"...*.rU..p.....*..{....*"..

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.Yuv.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	28640
Entropy (8bit):	6.455925007527187
Encrypted:	false
SSDEEP:	
MD5:	BFDAE019489EEA9ED2048DD3EE087147
SHA1:	E8DFA882CD929414B0415650E59AF9F1FE8632CC
SHA-256:	5321FE3EB073F7A3441FD2DC91A8D3B5E6215F8CDC39CFABF4E3D1E1519D4074
SHA-512:	CC42035488BDDD15ADCBE049A484E8D5186A330253FE0B265BB1BCC38385EA58E1BDBE504D9530D33EED5A2B889C48667ACF89AA40792383508540944D415CA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0..<.....b[... ...`..... ..... ..`.....[..O....`.....F...).....Y..... ..... ..H.....text...h;... ...<..... ..`.rsrc.....`.....>.....@..@.rel oc.....D.....@..B.....D[.....H.....L3...&.....*..*..*..*..(....*.r...p*..{....*"..}....*..{....*"..}....*~...}.....(.....#.....?o....*....}.....(.. ...#.....?o....*V..o.....(.....(....*^....o.....(.....(....*.0.....{....-..s(...}.....o.....#.....3.#.....?..#.....?3).o....-!.(.....(....o.....o.....o....*...o ...&...(....(.....#.....?4....(.....o!...-..o"...,... (.....#.....?6....(.....(.....o#.....o.....,...o$.....o

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\FM.LiveSwitch.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2983392
Entropy (8bit):	6.041828239201356
Encrypted:	false
SSDEEP:	
MD5:	D4A244965DA27169F4540F9A3E32FED7
SHA1:	3A9331F67427F88A0A0D7166CC25A8C2163E0A62
SHA-256:	6724C5009AE426CAA1C3AD4A4C80BA609A2CE586E28984EAA022B63CFB520052
SHA-512:	9F28EAF4E3DF6A79DB765927543E37290C8A197A13BD47A3118535D5C33B5207086A014A5BBF90268A88FAF7114716C2722336DB45583E3D061668446467C311
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.a....." ..0..R-.....>h+.. ....-..... .....-.....h.-. ..`.....g+.O....-.....\-..)....-.....f+..... ..... ..H.....text....P-.. ...R-..... ..`.rsrc.....-.....T-.....@..@.rel oc.....-.....Z-.....@..B..... h+.....H.....c.....{....*..{....*V.(.....}.....}....*...0..A.....u.....4../(.....{.....{....o.....,(....{.....{....o !...*.*.*. ..G.)UU.Z(.....{....o"...X)UU.Z(....{....o#...X*...0..b.....r...p.....%..{.....%q2....2...-.&.+...2...o$....%..{.....%q>....>...-.&.+...>...o$....(%...*..{....*"..}....*..{....*"..}....*.. {....*"..}....*R.(.....(.....(....*..#.....(.....#.....(.....j}.....j}....*...0..

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\chrome_100_percent.pak

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	data
Category:	dropped
Size (bytes):	639501
Entropy (8bit):	7.9604966575130005
Encrypted:	false
SSDEEP:	
MD5:	E71E9363E542BBB9A25B46FBD4CD9865
SHA1:	C99CF477EAE30F5F04DA31513A9E92E16E43F858
SHA-256:	225207498D45DA5CA15705A98C7197521114AF0A5526DFB21BF89E56647676E3
SHA-512:	7C3485C9557968F91E269633818822D80F3C86A42968D719EECB6F3A7F6A5FEC0D20D82C435799340D8BA66A5EA263EDEA190EBAF22D1E324B42B90A94B2FB8E
Malicious:	false
Reputation:	low
Preview:	.....,.....n.....+...!.i...#.....$.....&.....).....:...../...../:..../...../...../x..../...../:..../...../...../_..../...../...../k..../...../ ..../q..../...../...../w..../8..../~..../...../` ..../...../...../s..../...../]..../X..../'..../...../~..../F..../...../...../...../A..../&..../...../v..../...../...../...../...../...../.)...../.)...../.*.../Q+.../.+.../.+.../...../.B...0.U...0%W...0.Y...0.\...0L_...09h...0.o...0lu...0.{...0.....0....0.....0....0s....0.....0.....0.....0.....0}....0.....0.....07....0=....0l....0.....0.....0.... 0J...!0...."0....#0.#..$0.+..%0C-..&0+K..'0.d..(0....)0...*0....+0x...,0....-0.....0..../0."..00.K..10$`..20.x..30....40...50....60/...70....80S...90....:0....;0A...<06...=0}...>0.&..?0./..@0e4..A0.?..B0.J..C0.N..H0.W..I0b]..J0(c..K0.g..L0.l..M0T~..N0....O01...P0...Q0....R0....S0....T0....U0....V0C...X0....[0{...\0U...]0....a0....b0....c0.<..d0.=..t0.>..u0.A..v0.G..w0.M..x0.T..y0.Z..z0._..{0.d..|0ok..}0.p..~0.....0.....0.....0_....J>....JC.

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\chrome_200_percent.pak

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	data
Category:	dropped
Size (bytes):	960892
Entropy (8bit):	7.952005369692832
Encrypted:	false
SSDEEP:	
MD5:	D84BE5F1BB86BD7F04E01CDBF183A247
SHA1:	868534E57E74D830729C66EBAFCF9816A8E0D14B
SHA-256:	C35FCF898F5D406E0F3BC3720EB6920617D0C2FE04F25AA57BA4D2C851F8DE4B
SHA-512:	9E7EA0764DEFE078936B46FE94CFDAA39E3D13B6534535B4567AC67B8DE753EE729CE0C76DA55ECDE59414B90333515F73669D3FA20EB6E8ABE50334CEFF17E4
Malicious:	false
Reputation:	low
Preview:	.....).....8...!..".:.#..".$.t#..&..$..)..$..:..&.../.(.../...../...../...../...../...../I..../...../C..../...../...../{...../...../I..../...../...../s..../...../6..../...../O..../...../h..../...../...../8..../...../e..../...../V..../...../f..../E..../...../...../H..../...../K..../...../...../u..../.:.../+b.../...../...../...../#..../...../...../...../...../...../...../...../...../09+...0,.,..0O/...0C5...0.:...0:P...0.a...0.p...0X....0.....0.....0%....0.....0.....0.....07....09....08 ...0./...0.B...0.V...0.n...0.....0.....0g....0.....0s... 0B...!0...."0>...#0B=..$0.U..%0.X..&0.v..'0....(0....)0b...*0G...+0$...,0{..-0.....0.;../0.N..00.w..10....20...30....40...50....60_...70D...80....90....:0}...;0.9..<0.C..=0.K..>0sS..?0.[..@0.a..A0.I..B0.v..C0.~..H0_...I0-...J0....K0....L0...M0~...N0....O0L-..P0.Y..Q0.z..R0h...S0....T0....U0....V0.'..X0B(..[0.)..\0.+..]0>-..a0....b00Q..c0Yk..d0.n..t0.o..u0.w..v0....w09...x0....y0....z0....{0...|0....}0....~0--...0.1...0.6...0.?...J.X...J.]

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\chrome_elf.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1188832
Entropy (8bit):	6.174390393464766
Encrypted:	false
SSDEEP:	
MD5:	B872E030CCAE6134A9B12AE86F69BDEE
SHA1:	FD6D91F8127D11046F5BD9181FDD46DE6023DA45
SHA-256:	6438515197781187BCAE1EDF19B160AEE1E5B807703AA865439D3A6094CA893F
SHA-512:	BE2307500D001F375F7B509262FAB7B468078E99144224D0E0F0BD66655A6939C204E18924F97E2A3B0B02DF8FB9D748E5CCC692C9B54C9FE503DE1C1741BE23
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d....|b....." .....(.....I....`A.....a...(.....x.....~.....).....8.....(...p...8.....text..._..... ..`.rdata...^.....`.....@..@.data.....@.....0.....@....pdata…~.....L.....@..@.00cfg..(....p.....@..@.crthunk@.....@..@.oldntma.....@....tls.....).....@....voltbl.D.....CPADinfo8.....@..._RDATA.....@..@.rsrc...x.....@..@.reloc.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\concrt140.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	317408
Entropy (8bit):	6.297883466364787
Encrypted:	false
SSDEEP:	
MD5:	DE9EDD37564BF089900CA3AB7B55262D
SHA1:	7986976BCBBA012963E92EE8009D6CD44D85D636
SHA-256:	929F0AB59E68BF68D64497AADC7D0D8F0821CD5FC563EBDB1ED35E6F04A892BE
SHA-512:	03CE567AE436CBA9113D4DF79425D4B31D2AD2189A2D02E4228FF80DC30F733B88A62D90D24E57B5AAB8E46FFF212564ED2B9B9BA02F4D442AB23D282430F9 E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S].Y.<...<...<...L...<...DR..<..EI...<...<...<..EI...<..EI...<..EI..C<..EI...<..EI>..<..EI...<..Rich.<.....PE..d....(.`.....".....0"....`A.....M...+.....6.....).....p....4..T.....p4..8.....text...\..... ..`.rdata...M.....N.....@..@.data....?...@...8.....@....pdata...6.....8...f.....@..@.rsrc.....@..@.reloc..p.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\cr_win_client_config.cfg

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	210
Entropy (8bit):	4.719325836911548
Encrypted:	false
SSDEEP:	
MD5:	0A5F7737B4D557942779D447A7D73F19
SHA1:	6105FBBE46C41639848F5A87804025CE2C33026D
SHA-256:	75D1E0CAF25ACA7AF0D4CC83E53694B4F1E65B7CFD8508D9AB1D9BC0F2F45778
SHA-512:	D0D93F06E14BA757A64561C6058CDCA8CD24AC20066E1A0C2EF51DD5D7AFF732E6AC0E19E3C6818E8A69DD0873BC5466DC6F9EC7CC16F041E229B91A7EFC/ CFF
Malicious:	false
Reputation:	low
Preview:	uploadUrl=https://apip.adobe.com/headlights/FileDataCaptureServlet..deleteCompressedFile = true..deleteInvalidLogFiles = false..deleteSuccessfullySentFiles = tr ue..crcnUrl = crlog-crcn.adobe.com..crcnPort = 443

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\d3dcompiler_47.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4893152
Entropy (8bit):	6.393518957966005
Encrypted:	false
SSDEEP:	
MD5:	6DCEF834269270335651849DBBFA4EDF
SHA1:	511F631AA97690FFDAF20CDAC77AFDB8A4327CC2
SHA-256:	B8AF8C7D667A272075973A50A0B886FDDA060A65596E3E8AA9398EE78936884E
SHA-512:	87B08C081E45C175F9D7464EA0152D8163481F2AB5F4FAE670509A9144F267AD2D1BD8367AD572A50BA6953C7DB0DD2B75A2B43936B444370A7D28A07ECD165
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c...c...c..Z....c...c../c....7..c.....c.....c..Z....c..Z...bc..Z....c..Z.. ..c..Z...6c..Z.[..c..Z....c..Rich.c.....PE..d...-L....." .....8.....`.(..... K.....K...`A.....F.x.....F.P.....J.@.....H.....J..)... .J.....vD.p.....<.(...P.<.8.....<.(.....text.....8.....8..... ..`.rdata...=....8..@....8.....@..@.data...@....F.....F.....@....pdata..... .H.....G.....@..@.rsrc...@.....J.....I.....@..@.reloc.....J.....I.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\digest.s

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe

File Type:	data
Category:	dropped
Size (bytes):	4509
Entropy (8bit):	6.397577636054845
Encrypted:	false
SSDEEP:	
MD5:	E41B11E4B777BED0033EE2B4C19B2FFC
SHA1:	D2DA219868807941D0B99612E9A38D9B4FE28F98
SHA-256:	20DE433450C490C71FEDB9B499B66744B66E20FBD439230116E0FE62AEC3AC81
SHA-512:	2A9A1401443E10396BE2B11B0AA13ECE00B759D37100E06DDA54C5FBB1924207DCD96CE44B0CE1F00FEEA4F5EFE882ED57BEE660F1FD12C8622F6B8323F83A7D
Malicious:	false
Reputation:	low
Preview:	0.....*.H.....0.....1.0...+.....0.....*.H.....<manifest>..<Reference URI="chrome_elf.dll" />..<Reference URI="Connect.exe" />..<Reference URI="ConnectDetector.exe" />..<Reference URI="CRClient.dll" />..<Reference URI="cr_win_client_config.cfg" />..<Reference URI="CRLogTransport.exe" />..<Reference URI="CRWindowsClientService.exe" />..<Reference URI="d3dcompiler_47.dll" />..<Reference URI="EncoderHelper.exe" />..<Reference URI="icudtl.dat" />..<Reference URI="libcef.dll" />..<Reference URI="libcrypto-1_1-x64.dll" />..<Reference URI="libEGL.dll" />..<Reference URI="libGLESv2.dll" />..<Reference URI="libssl-1_1-x64.dll" />..<Reference URI="rtmp.dll" />..<Reference URI="snapshot_blob.bin" />..<Reference URI="v8_context_snapshot.bin" />..<Reference URI="locales\am.pak" />..<Reference URI="locales\ar.pak" />..<Reference URI="locales\bg.pak" />..<Reference URI="locales\bn.pak" />..<Reference URI="locales\ca.pak" />..<Reference URI="locales\cs.pak" />..<Reference URI="locales\d

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libEGL.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	428512
Entropy (8bit):	6.359145784921531
Encrypted:	false
SSDEEP:	
MD5:	22B6BA6240495597D1F0F2F6AEBD3E94
SHA1:	B4770DEAD75F026FED7878919EA104FD3CDA6576
SHA-256:	D0CC62BBD9887254E4F00044A8883F9094C58A2308F8EFDC7831597520F0EE85
SHA-512:	C82E4D639E5EC9CD708940C488BC9A6C9F0738C7CAC47C2123270B57C6A7F2BD75A58C08D0AEC6441AF02179629AB5A34CFB5D98A54E68AD4847BCDB49266AC8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d....\|lb....." .....r.....`A.....0~.....(.....x....P...<...`...).....,...$w..8.....u..(...P...8.....text....p.....r..... ..`.rdata...n.....p...v.....@..@.data...\L..... .....@....pdata...<...P...>.....@..@.00cfg..(.....D.....@..@.tls....!.....F.....@....voltbl.8.....H....._RDATA..J.....@..@.rsrc...x.....L.....@..@.reloc..,.....R.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libGLESv2.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6352864
Entropy (8bit):	6.427171757940237
Encrypted:	false
SSDEEP:	
MD5:	28360667A17213D239B7F9040BC83431
SHA1:	BFE99B7584436D16D27D694939995D7493D29923
SHA-256:	C852898353C19D903B67C3D8EC71C377C8A50F3DAB9D2A8EAEBBC5B58DA182FB
SHA-512:	A615A76281AEEE26A42D81A690941FE5A297B662ED44C22AC75A5BBA2745936EB3D03C6FD72309ED66C3C665B7401305EF284DFB2DF007017DB8AF7DC79914A4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d....|lb....." .....nF..R.....zC.....a.....a...`A.....W....._.X.d....`.....^..S....`..)....`.....W.8.....X~W.(.....F.8.....P.X.....W.@.....text....mF.....nF..... ..`.rdata.....F.....rF.....@..@.data...h.....Y.....hY.....@....pdata...S....^..T...t].....@..@.00cfg..(....p`....._.....@..@.tls....1....`.....\_.....@....voltbl.F....`....._....._RDATA.....`.....\_.....@..@.rsrc.....`....._.....@..@.reloc.....`....._.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libaudioprocessingfm.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	935904
Entropy (8bit):	6.509829709376193
Encrypted:	false
SSDEEP:	
MD5:	EBD1D9C0C38A2E8DEC423CBF483EBE5A
SHA1:	74839F7748EFCA2825FDF35B246E6526E92F8753
SHA-256:	00C5391ACD30F320F75F76F841AE186E7B4D43B3262456DC410EA19BED6BCF29
SHA-512:	CB1C776EF7C6E070CE8CF554404FF6277E8D198CE41D7526124E42D0795D9E8EA62C5A3093DFA3EAA973A86B4A47E37DC1D9F83C9C76D1773209E810748D60E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e,h....e,j.q...e,k.....OR.....j.....f.....Rich.....PE..d....6[....." .....p.....q.....`.....f.....g..<...`.....@e.....)...p.....@*..p.....+..(....*.....text.....`.rdata.....@..@.data...07.....\.....@....pdata..@e.....f...x.....@..@_RDATA...*...0...,.....@..@.rsrc.....`.....@..@.reloc.....p.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libcef.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	170685920
Entropy (8bit):	6.67714452940272
Encrypted:	false
SSDEEP:	
MD5:	9F903159A932D7805E9BEE2EDCD142C1
SHA1:	C1D347E11ACCEC1E64AECF564B33AB776E19E3E1
SHA-256:	3CAB045E9542BBB2E03D524C49B62E67B5BE4E6D3D1C553A434E4E8DD368B896
SHA-512:	6947D203507BB302FA87A68855CD54EA23E05822C5700407CF890F9FE749F8614C78D120B84F96075D3D7BA342785ACAD0A30F4D4DF5FA49D42A49E36FF02285
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d....|lb....." .....>g.....0La.....0T.....x,...`A.....w...W.....\....@<..4...P...UQ..L,..)....>.\.....8.....(....cg.8.....H7...#.....text....=g.....>g..... ..`.rdata....R..Pg..R..Bg.....@..@.data...x.0..@.....*.....@....pdata...UQ..P...VQ.....@..@.00cfg..(.....;.....R.....@..@.retplnel.....;.....T.....rodata.....;.....V..... ..`.tls.....;.....h.....@....voltbl.t.....<.....I.....CPADinfo8.....<.....n.....@..._RDATA..... <.....p.....@..@malloc_h.....0<.....r..... ..`.rsrc...4...@<..6...t.....@..@.reloc..\.....>.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libcrypto-1_1-x64.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3418080
Entropy (8bit):	6.111105756924529
Encrypted:	false
SSDEEP:	
MD5:	8A4B40A18CD80A0A884B150C45861242
SHA1:	CD0FD960574519610A4831EFB6D7967FDEDA515A
SHA-256:	F69E2ACED60DFFA43BAB11394C7E211B41EBADC6FDE617BD4A018FA03B1D3CD2
SHA-512:	3A85346F97B70DD3603381814234759 97EC6BCCB66DF27EF77B6BD37775F4A5F5847052DB685BB63C82967EA85BE3FD1CF7FDC39ED08C2589B48A0B10C6AD04 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....xg..xg..xg.....xg..f..xg..d..xg..b..xg..c..xg..f..xg..xf.sxg..xg.. xg..c.zg..g..xg.....xg..e..xg.Rich.xg.....PE..d...)..\......" .....$..t.....Jp.....4.....8.4...`.....P"/.0f....3.@.....4.|.....2.`... ..3..)....4.tO.. .,.8.....`.,.....3.....text.....$.....$..... ..`.rdata.....$.....$.....@..@.data....f....1.,....p1.....@....pdata..|..... 2.....1.....@..@.idata..."....3..$...V3.....@..@.00cfg.....3.....z3.....@..@.rsrc...|.....4.....|3.....@..@.reloc..fx....4..z....3.....@..B..... .....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libnvidiafm.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	676832
Entropy (8bit):	6.054049052784219
Encrypted:	false
SSDEEP:	
MD5:	152B9B5CFD073255CD573579AFCF1B6C
SHA1:	CBBDDB2DF944F4B2F3608DF849DE7B7FE096B354
SHA-256:	6A1E7BCBA7D0A36A3B2D5A4DFB1FB7D2E3C9D3B6074884D2DF33BE0AF4A94F61
SHA-512:	FAFDF55CEB0843C7EFBED20800A08DDF357C4ECF0A61813B954897B823FB9DEFADB65B6F2E5538766953149F72DDC38210DBA00CB71DC8099AD34294F5CB72 35
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....`E...+X..+X..+X.e(Y..+X.e/Y..+X.e.Yf.+X.i.Y..+X.i/Y..+X.i(Y.. +XB`*Y..+X.e*Y..+X...X..+X..*Xb.+Xch/Y..+Xch.Y..+Xch+Y..+Xch.X..+Xch)Y..+XRich..+X.....PE..d...._.....` .....|.....p}.....`..... .....Pz..\....|..P....P.....|n...*...)...`..d.....T..... .....text...`..... ..`.rdata.....@..@ .data....E.....*...x.....@....pdata..|n.....p.....@..@.rsrc.....P.....@..@.reloc..d....`.....@..B..... .....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libopenh264fm.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	143328
Entropy (8bit):	6.3917775061081015
Encrypted:	false
SSDEEP:	
MD5:	87EBFC7BBC73564E86F4C29C7CDAA188
SHA1:	D150E6149858C79E276B229932B594D1C7836532
SHA-256:	066D0C980BE9474627129AA75BF684100511133BD419A7C207688F182BF14DDA
SHA-512:	B9A4AF9D8951FBB001B9BE4745F807C53155D9807B4FCB2B7F2EE350C67442F89327287B3442A9D163020486D2E690E828FD609A30BF25FB706412EC4919A54A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@...@...@}.$@...@}.&@...@}.'@...@...A...@...A...@...A.. .@...@...@.%.@...@...@...@..A...@..A...@.*@...@..A...@Rich...@.....PE..d...]..Z....." .....=.....`.....`.....0..... <....@..... ..t.....)...P.....@...p.....0..@.....text...`..... ..`.rdata.....0.....@..@.data...x..... @....pdata..t.... .....@..@.rsrc.....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libopusfm.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1036256
Entropy (8bit):	5.962459026443746
Encrypted:	false
SSDEEP:	
MD5:	D89109B8DE68329A0EDCE9908A4B3066
SHA1:	28C70BA2DBA2FBA514EB467ACB1452A269704E52
SHA-256:	C3CBCB1725A6C87FAC2C4EFEEDB4138B769953942E4A08836CFB213C0629FB78
SHA-512:	FAC3E86C3BFFAA57C2616C5A5364C32750C771BAE1A2B0376C0EA7FBB100A34036D45E338E64A4B47E9CED4EE47216A7004B4B0D3E96381C216F1755CCA237 22
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b.....A...A...A.k.@...A.k.@...A.k.@P..A.l.@...A.l.@...A.l.@.. .A.k.@...A...A...A?g.@P..ARs.@...ARs.@...ARs.A...ARs.@...ARich...A.....PE..d.....r`....." .....l...V.....C..... .....5....`..... .....x...(.....<....P..db.....).....tG..8.....G..0.....x.....text....k.....l..... ..`.rdata..s.....p.....@..@.data...i1..... .....@....pdata..\m...P...n.....@..@.idata.....v.....@..@.00cfg..Q.....@..@_RDATA.....@..@.rsrc...<..... ..@..@.reloc.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\librnnoise.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	153056
Entropy (8bit):	7.399708512360001
Encrypted:	false
SSDEEP:	
MD5:	9C694B1150A0459E9299D69D857CEB9C
SHA1:	560DA90E2885F341C4C01DDD08D1B2E5E1731244
SHA-256:	72FC0DA1FF38CDE730CE05FE5B910DD5E3DFDA88F1D87645876B221B7FF65E4E
SHA-512:	FD4A45B69445C8C8FCC7C14E924B085DA13553A49E0560A1FD56475509881E6B2C7DA2CC1A1C4EBE31FCDC8FEA97CCB30E721FCCDC65183E5A6EB8E9F8828 F24
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oN.. ... .v.... ..{!... ..{%... ..{$... ..{#... .N~!... ...!... ..{)... ..{ ... ..{... ..{"... .Rich.. .....PE..d....2Zc....." .....`.....&.....'.....`.....P..,.....)...p..l.....p..... .....8.....H.....text..... ..`.rdata..l.....n.....@..@.data.....0..... .....@....pdata..,....P.....".....@..@.rsrc.....`..... (.....@..@.reloc..l....p.....*.....@..B..... .....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libssl-1_1-x64.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	692192
Entropy (8bit):	5.548016622817644
Encrypted:	false
SSDEEP:	
MD5:	65C5EEDA06BC04BC0259B37C3BCB99A4
SHA1:	97BEFF8AD9B589E9932C6D08DFF7C3E6DE2AE434
SHA-256:	B01A264FA3C5F013CC7E01FB5D73166671D269EB74E91B01B02239CCB8CF03C3
SHA-512:	F5D95C8E2C3F1E8CA97AB634677D6ADBD56BABF65CF10AA3BFD793F6C669E6128BB080FA88A0668130446A9E5BFA2E432BB590F5A7A67EBD93C4C8E728E600 58
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../PQ.k1?Tk1?Tk1?TbI.Tg1?T9Y>Ui1?T.U>Ui1?T9Y<Uh1?T9Y:U `1?T9Y;Uc1?T.Y>Uh1?Tk1>T.0?T.Y;UG1?T.Y?Uj1?T.Y.Tj1?T.Y=Uj1?TRichk1?T.....PE..d...B..\.....".....(...D.....$.....E?....`... .....@....N...5.....s.....K...f...).....D... ...8.....`.....text....&.....(..... ..`.rdata..N#...@...$...,..... ..@..@.data...1M...p...D...P.....@....pdata...S.....T.....@..@.idata..wV... ...X.....@..@.00cfg.....@.....@..@.rsrc...s.....B..... ..@..@.reloc..,.....J.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libvpxfm.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2204128
Entropy (8bit):	6.623935160702264
Encrypted:	false
SSDEEP:	
MD5:	9DCB576C9F513FC70C3AFF2B27DA19C7
SHA1:	C96A5C033A1A7EF0977A646A4987A7E8E7CA239E
SHA-256:	7477362A1AF048D99A87EFF771F79CD590183964422060FA43C150A200FDC390

SHA-512:	64B395D1A145C76A8BB18CAC67C0C030626A5D55E714217A036CF8563869B52F0FF21DC4D106054ED39EA1BB5E7B3D64AB10ACDAA6688F89A1AB3E586AE04B B0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....]...3...3...3...7...3...0...3...6.R.3.B{....3...0...3...6...3...7...3...2...3... 2...3..;.r.3...3...3..7...3..3...3.....3..1...3.Rich..3.....PE..d..._..Z....." .....X...f.....t.....".....!..`.....0. .$...T. .(....!..... .....x!..)....!.....B..T.....B.....p..H.....text...PV.....X..... ..`.rdata.....p... ...\.....@..@.data...(V.... .....| .....@....pdata..... . ...@..@.rodata.....!.....V!.....@..@.rsrc.....!.....ll.....@..@.reloc.....!.....n!.....@..B.....

C:\Users\eyup\AppData\Local\Temp\ConB14B.tmp\libyuvfm.dll

Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1316832
Entropy (8bit):	5.902253584565249
Encrypted:	false
SSDEEP:	
MD5:	BF74361A1F5705ADFB3C1E1A9E4A4B3B
SHA1:	AD4F2027A4BBFC46A54BD8532ED85E1D41C48C0B
SHA-256:	055C976838EBBFDB88FF4FFD02A87D6181B055C60FFCA6D1BF514AB5BAAB3283
SHA-512:	644E48303422B1FC60C6FA1FC6CD07CEF638259092232290D97B3299C3FC7D2DD374152E130980B692582C5003A6B3AC0AB76102C6AC9E48E79AFB212CC4056
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R..o.a.<.a.<.a.<M..=.a.<M..=.a.<M..=.a.<...<.a.<...=4a.<...=.a. <...=.a.<M..=.a.<.a.<Ca.<.a.<)a.<...=.a.<...=.a.<..(<.a.<...=.a.<Rich.a.<.....PE..d...aS._.....".....T.....`.....`.....3 ..N.....(....0..<.....q.....)...@..|....U..8.....U..8.....text...|..... ..`.rdata..^5.....6.....@..@.data...!1..@.....(.. .....@....pdata..H~.....:.....@..@.idata..#.....@..@.00cfg..Q.....@..@_RDATA..... .....@..@.rsrc...<....0..... ..@..@.reloc..T....@.....@..B.....

C:\Users\eyup\Downloads\6bcc8cff-6afa-4c34-b8b1-3a042b0a5bd0.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	134903
Entropy (8bit):	6.346891578686829
Encrypted:	false
SSDEEP:	
MD5:	292A904E7EEB0FE1530B77CB3B7D1884
SHA1:	90BD2B0030272257CEE9745753B89A3A28B74401
SHA-256:	BA28BDC67EAD566663FBBD9711E5D568C30E1014FDD6D12D7533678623E50431
SHA-512:	98107FB9D2E1C2C9CC6A36BCDC392A6D32CA664905410F5AE896BAB6AEE9599EAD6B6A54BAB1D2EAD0A204C4110FA2DFD08CD1335040BC5BCF61AE823181 103
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t.n.0w..0w..0w..$...!w..$...w.....'w.....'w.....w.....8w..$...*w..$...1w ..$...)w..0w..'v.....7w.....1w..0w..1w.....1w..Rich0w.....PE..L...B.sb.....,...H.....@....@.....d.....@.....h.....f..(!...`...5...^..p.....8_..@.....@.....text....+.....,..... ..`.rdata...z...@...|...0.....@..@.data....+.....@....rsrc....h.....j. .....@..@.reloc...5...`...6...0.....@..B.....

C:\Users\eyup\Downloads\ConnectShellSetup11.exe (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	624424
Entropy (8bit):	6.896968533209531
Encrypted:	false
SSDEEP:	
MD5:	00B6898BF01716F6FE6C1FC1E7256905
SHA1:	AEDD9210F27091F9B8AD654B4558609C2688379D

SHA-256:	919ECA4E74525FE9A5CAAFCB0BE729BE64A9773D4607A2FB615F128F64B1FAAF
SHA-512:	48A0C45996F5165CCD86D2D6454F8738072F4911556E822A0FF6BA8F293802FCA39290659C30A394796857BBE8734B6F9FA1BC74EF4DC66D16BB87643C9D18A5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t.n.0w..0w..0w..$...!w..$...w.....'w.....'w.....w.....8w..$...*w..$...1w ..$...)w..0w.."v.....7w.....1w..0w..1w.....1w..Rich0w.....PE..L...B.sb.....,...H.....@....@.....d.....@.....h.....f..(!...`...5...^..p.....8_..@.....@.....text....+.....,..... ..`.rdata...z...@...|...0.....@..@.data....+.....@....rsrc....h.....j. .....@..@.reloc...5...`...6...0.....@..B..... .....

C:\Users\eyup\Downloads\Unconfirmed 658627.crdownload	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	624424
Entropy (8bit):	6.896968533209531
Encrypted:	false
SSDEEP:	
MD5:	00B6898BF01716F6FE6C1FC1E7256905
SHA1:	AEDD9210F27091F9B8AD654B4558609C2688379D
SHA-256:	919ECA4E74525FE9A5CAAFCB0BE729BE64A9773D4607A2FB615F128F64B1FAAF
SHA-512:	48A0C45996F5165CCD86D2D6454F8738072F4911556E822A0FF6BA8F293802FCA39290659C30A394796857BBE8734B6F9FA1BC74EF4DC66D16BB87643C9D18A5
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t.n.0w..0w..0w..$...!w..$...w.....'w.....'w.....w.....8w..$...*w..$...1w ..$...)w..0w.."v.....7w.....1w..0w..1w.....1w..Rich0w.....PE..L...B.sb.....,...H.....@....@.....d.....@.....h.....f..(!...`...5...^..p.....8_..@.....@.....text....+.....,..... ..`.rdata...z...@...|...0.....@..@.data....+.....@....rsrc....h.....j. .....@..@.reloc...5...`...6...0.....@..B..... .....

unknown (copy)	
Process:	C:\Users\eyup\Downloads\ConnectShellSetup11.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	28640
Entropy (8bit):	6.398055190229929
Encrypted:	false
SSDEEP:	
MD5:	7ABFC5592FA3F1F3107D44854D11CD5A
SHA1:	75C52AF7A2365CE6194A9181C4F49A5749FEED71
SHA-256:	D7FB60D87973C85F3B3E5E2160F576ABFAC1B1D0C2F8F0BF199393EB32B6EC75
SHA-512:	CC447359DFB8FA94E696B66EC0180DA82D240171F46C3A0A4B30A16ECED04993502AF32D3D0D304B5000E29A479FE5DB1A32FB62D340C70952227E45905A1ED 0
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q.Q.....!.....>.....\... ...`....@.. .....Q.. ..@.....\\..O....`..(.....F...).....[..... ....H.....text....<... ...>..... ..`.rsrc...(....`.....@.....@..@.rel oc.....D.....@..B.....\.....H.....6.. %.....P .....A..R.N.W.9z..W....C.L..Q.\[I..&.*G..J..D.%A...|M..h.T.r%..H..Lz...9...G...: [..1J.9.b-.....Q.0S.....T{..ix{g...N.....{....*z.(.....}.....}.....}.....i}....*r.(.....}.....}.....}....*.0..'.....{.....{....{.....{....(.....*b.{....{....{....(....*>..}.....}....*.0..-.....{.....{....Y..{.....{.. ..Y...Z..ZXl(....k*....0..(.....{....k..{....Y..{....k..{....Y...Z..ZX*...{....

Static File Info

No static file info