ID: 508276
Sample Name: btc1exch06_2021-10-24_12_30_07.zip
Cookbook: default.jbs
Time: 19:31:38
Date: 24/10/2021
Version: 33.0.0 White Diamond

Table of Contents

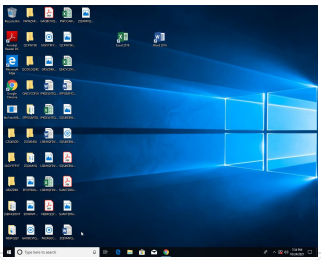
Windows Analysis Report btc1exch06_2021-10-24_12_3…

Overview

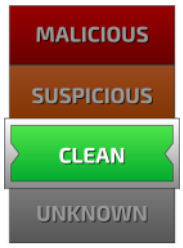
General Information

Sample Name:	btc1exch06_2021-10-24_12_30_07.zip
Analysis ID:	508276
MD5:	55b2aed249f0734.
SHA1:	69465885111c48..
SHA256:	bba536f8adeed06.
Infos:	

Most interesting Screenshot:



Detection

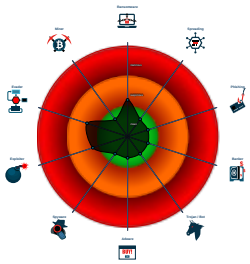


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found inlined nop instructions (likely…
- May sleep (evasive loops) to hinder …
- Creates a process in suspended mo…
- Contains long sleeps (>= 3 min)
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- unarchiver.exe (PID: 4780 cmdline: 'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\btc1exch06_2021-10-24_12_30_07.zip' MD5: DB55139D9DD29F24AE8EA8F0E5606901)
  - 7za.exe (PID: 6740 cmdline: 'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\amgha5zs.gqf' 'C:\Users\user\Desktop\btc1exch06_2021-10-24_12_30_07.zip' MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
    - conhost.exe (PID: 4340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

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

Mitre Att&ck Matrix

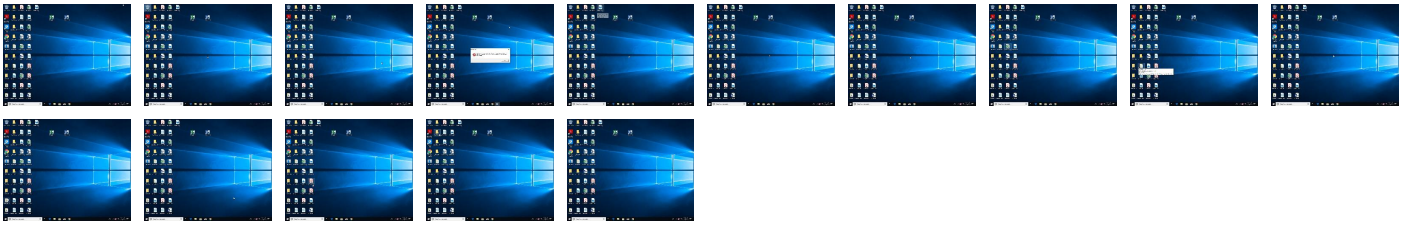
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Disable or Modify Tools 1	OS Credential Dumping	Virtualization/Sandbox Evasion 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

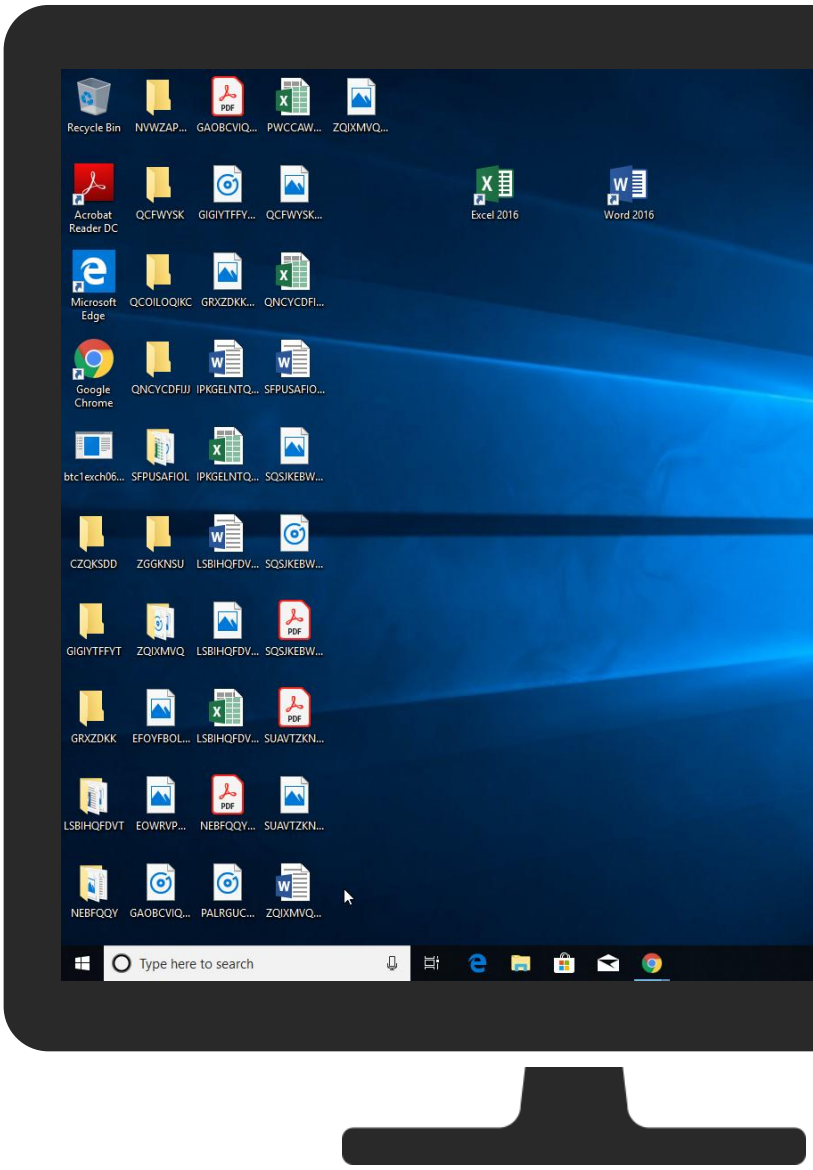
Behavior Graph

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508276
Start date:	24.10.2021
Start time:	19:31:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	btc1exch06_2021-10-24_12_30_07.zip
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:	24
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:	CLEAN
Classification:	clean2.winZIP@4/2@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .zip
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	388
Entropy (8bit):	5.2529463157768355
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk7v:MLF20NaL329hJ5g522r0
MD5:	FF3B761A021930205BEC9D7664AE9258
SHA1:	1039D595C6333358D5F7EE5619FE6794E6F5FDB1
SHA-256:	A3517BC4B1E6470905F9A38466318B302186496E8706F1976F1ED76F3E87AF0F
SHA-512:	1E77D09CF965575EF9800B1EE8947A02D98F88DBFA267300330860757A0C7350AF857A2CB7001C49AFF1F5BD1E0AE6E90F643B27054522CADC730DD14BC3DE1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Temp\o21fgc1p.ykx\unarchiver.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2042
Entropy (8bit):	5.079284227182979
Encrypted:	false
SSDEEP:	48:9cgWdEG0Gb0G0GpOG4VG0Gpmg/G0GBjGeG0GbyGjg/Gc/GBjGeGxG0G0GmbG0GR3:9onV5x
MD5:	83E3D2A747734B22BA209184848CE656
SHA1:	6981E7C2AABDD280ACAB31905F50D3E57744A28C
SHA-256:	8D218AB5EFDBE2F377BFA7FAFC131A6EA80CFD1C5CAEEF4D179B159F14161CC3
SHA-512:	2D86E26750925713E26B702DDA97390B219F17672EF7F85E3D6F16220F7ADA201A3B591A2D309028515CEE5B6A6A9D23D655A9AF42315A0E62E436185E0E47A6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\o21fgc1p.ykx\unarchiver.log	
Preview:	10/24/2021 7:32 PM: Unpack: C:\Users\user\Desktop\btc1exch06_2021-10-24_12_30_07.zip..10/24/2021 7:32 PM: Tmp dir: C:\Users\user\AppData\Local\Temp\amgha5zs.gqf..10/24/2021 7:32 PM: Received from standard out: ..10/24/2021 7:32 PM: Received from standard out: 7-Zip 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30..10/24/2021 7:32 PM: Received from standard out: ..10/24/2021 7:32 PM: Received from standard out: Scanning the drive for archives:..10/24/2021 7:32 PM: Received from standard out: 1 file, 268 bytes (1 KiB)..10/24/2021 7:32 PM: Received from standard out: ..10/24/2021 7:32 PM: Received from standard out: Extracting archive: C:\Users\user\Desktop\btc1exch06_2021-10-24_12_30_07.zip..10/24/2021 7:32 PM: Received from standard out: ..10/24/2021 7:32 PM: Received from standard out: WARNINGS:..10/24/2021 7:32 PM: Received from standard out: Headers Error..10/24/2021 7:32 PM: Received from standard out: ..10/24/2021 7:32 PM: Received from standard out: --..10/24/2021

Static File Info

General

File type:	Zip archive data, at least v4.5 to extract
Entropy (8bit):	5.530880604643101
TrID:	• ZIP compressed archive (8000/1) 100.00%
File name:	btc1exch06_2021-10-24_12_30_07.zip
File size:	268
MD5:	55b2aed249f07346fb34a72c0ddd0ee1
SHA1:	69465885111c48e07efd98e7e0f363f29229f206
SHA256:	bba536f8adeed06f60f9ce85f04e4d32cd7860f69eff026a58336ef02b11424c
SHA512:	f3a26304cdd879537481aee94de98856159e77c9ee85af1bcd5757f74d29af4f0d7108f33215ca84a3ce598bacfb65a33092a1d5e03f8907b3e290eed8478e71
SSDEEP:	6:5jvCeIK5A8+V2z2v2Bq6THkNzZzSvCe4Ec5jll+l8:5jv3Fz2eBpTEzzSvEEG/a8
File Content Preview:	PK..-..... ..|.....manifest.json.....k.O..9.W...-..j9..k).....e...,d...}A....PT?....._B4..T.}s.r..~..... FCs..r.r?.....O..0..%i..H..)...XZ.....SLPK..... ..|.....manifest.jsonPK.....

File Icon

Icon Hash:	00828e8e8686b000

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: unarchiver.exe PID: 4780 Parent PID: 6488

General

Start time:	19:32:23
Start date:	24/10/2021
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\btc1exch06_2021-10-24_12_30_07.zip'
Imagebase:	0x7b0000
File size:	10240 bytes
MD5 hash:	DB55139D9DD29F24AE8EA8F0E5606901
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 7za.exe PID: 6740 Parent PID: 4780

General

Start time:	19:32:24
Start date:	24/10/2021
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\amgha5zs.gqf' 'C:\Users\user\Desktop\btc1exch06_2021-10-24_12_30_07.zip'
Imagebase:	0x1180000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: conhost.exe PID: 4340 Parent PID: 6740

General

Start time:	19:32:25
Start date:	24/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis