JoeSandbox Cloud BASIC

ID: 502663
Sample Name: setup.exe
Cookbook: default.jbs
Time: 08:36:46
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2

Windows Analysis Report setup.exe 3

- Overview 3
  - General Information 3
  - Detection 3
  - Signatures 3
  - Classification 3
- Process Tree 3
- Malware Configuration 3
- Yara Overview 3
- Sigma Overview 3
- Jbx Signature Overview 3
- Mitre Att&ck Matrix 4
- Behavior Graph 4
- Screenshots 4
  - Thumbnails 4
- Antivirus, Machine Learning and Genetic Malware Detection 5
  - Initial Sample 5
  - Dropped Files 5
  - Unpacked PE Files 5
  - Domains 6
  - URLs 6
- Domains and IPs 6
  - Contacted Domains 6
  - URLs from Memory and Binaries 6
  - Contacted IPs 6
- General Information 6
- Simulations 7
  - Behavior and APIs 7
- Joe Sandbox View / Context 7
  - IPs 7
  - Domains 7
  - ASN 7
  - JA3 Fingerprints 7
  - Dropped Files 7
- Created / dropped Files 7
- Static File Info 7
  - General 7
  - File Icon 8
  - Static PE Info 8
    - General 8
    - Entrypoint Preview 8
    - Rich Headers 8
    - Data Directories 8
    - Sections 8
    - Resources 8
    - Imports 8
    - Exports 8
    - Version Infos 8
    - Possible Origin 8
- Network Behavior 9
- Code Manipulations 9
- Statistics 9
- System Behavior 9
  - Analysis Process: setup.exe PID: 7152 Parent PID: 4616 9
    - General 9
    - File Activities 10
    - Registry Activities 10
      - Key Created 10
      - Key Value Created 10
- Disassembly 10
  - Code Analysis 10

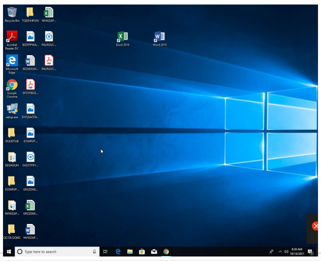
Windows Analysis Report setup.exe

Overview

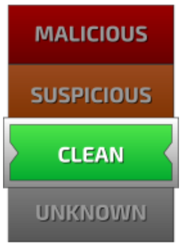
General Information

Sample Name:	setup.exe
Analysis ID:	502663
MD5:	fe5c2e1333b4477.
SHA1:	ce7e5a597b98eb..
SHA256:	fc91558efb40b16..
Infos:	

Most interesting Screenshot:



Detection

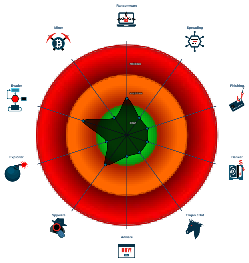


Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Uses 32bit PE files
- PE file contains strange resources
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Found evasive API chain (may stop…
- Contains functionality to check if a w…
- Contains functionality to dynamically…
- PE file contains executable resource…

Classification



Process Tree

- System is w10x64
- setup.exe (PID: 7152 cmdline: 'C:\Users\user\Desktop\setup.exe' MD5: FE5C2E1333B4477D029DEDC9C1B5DD4D)
- 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

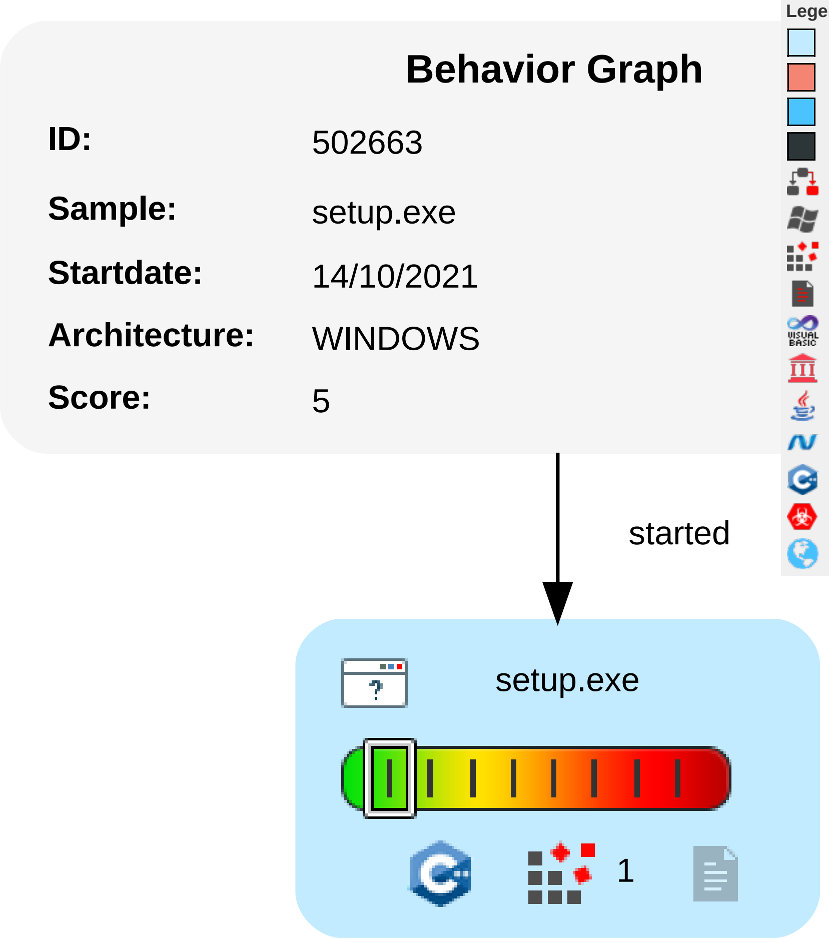
There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Path Interception	Software Packing 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	N S F
Default Accounts	Native API 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1 1	LSASS Memory	Application Window Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C E F

Behavior Graph

Hide Legend



Behavior Graph

ID: 502663

Sample: setup.exe

Startdate: 14/10/2021

Architecture: WINDOWS

Score: 5

Legend:

- □ Process
- 🟥 Signature
- 🟦 Created File
- ■ DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

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
setup.exe	1%	Virustotal		Browse
setup.exe	5%	Metadefender		Browse
setup.exe	7%	ReversingLabs		

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

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502663
Start date:	14.10.2021
Start time:	08:36:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	setup.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:	CLEAN
Classification:	clean5.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 26.7% (good quality ratio 25%) • Quality average: 73.1% • Quality standard deviation: 28.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

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

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Entropy (8bit):	7.907283747504906
TrID:	• Win32 Executable (generic) a (10002005/4) 99.39% • UPX compressed Win32 Executable (30571/9) 0.30% • Win32 EXE Yoda's Crypter (26571/9) 0.26% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	setup.exe
File size:	1466368
MD5:	fe5c2e1333b4477d029dedc9c1b5dd4d
SHA1:	ce7e5a597b98eb1ec36a48e4368997b787228544
SHA256:	fc91558efb40b16dd9f6b0e93c972a0f1ff85cad3ddefdd70 28c2628d75a9ab9
SHA512:	04892dfb3d356952a3bd4cac9026a3fac52b220af6b8a63 71e81293483dbdeb76f08e8182ae0301dedef4d2904a6c1 13d02d8d48307fe498a428b595b0ec03b4
SSDEEP:	24576:wJx22KNk+2ygEZZU6xUohcGGopn9iWsq/A9fzI DODmJfbtvyYtQEnRA2S/Y:w+29+2yn5+ohcGHpn97s7 JzIa6dY4/RC

General

File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......l...(.pA(.pA(.pA-./A,.pA...A+.pA!..A..pA!..A..pA6..A+.pA.K.A..pA.K.A7.pA(.qA..pA!..A..pA!..A).pA6..A).pA!..A).pARich(.pA.......

File Icon

Icon Hash:	80b0a4b4a4e4e4e4

Static PE Info

General

Entrypoint:	0x90cf20
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, REMOVABLE_RUN_FROM_SWAP, NET_RUN_FROM_SWAP, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x59E4BE15 [Mon Oct 16 14:11:33 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	ab8c7e344596e3e6d6c6a5375f98bde9

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x3c8000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x3c9000	0x145000	0x144200	False	0.985229162649	data	7.92638129371	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x50e000	0x22000	0x21a00	False	0.829874825743	data	7.3682539138	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

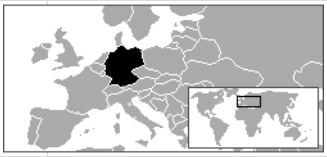
Imports

Exports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	
German	Germany	
French	France	
Japanese	Japan	
Korean	North Korea	
Korean	South Korea	
Chinese	China	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: setup.exe PID: 7152 Parent PID: 4616

General

Start time:	08:37:47
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\setup.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\setup.exe'
Imagebase:	0x400000
File size:	1466368 bytes
MD5 hash:	FE5C2E1333B4477D029DEDC9C1B5DD4D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis