ID: 483803
Sample Name:
oYIQVnvsyG.exe
Cookbook: default.jbs
Time: 14:05:02
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

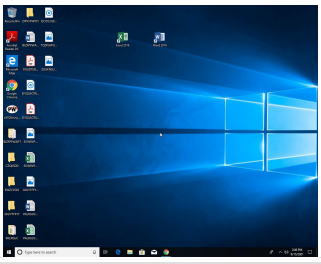
Windows Analysis Report oYIQVnvsyG.exe

Overview

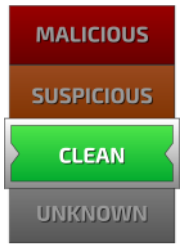
General Information

Sample Name:	oYIQVnvsyG.exe
Analysis ID:	483803
MD5:	43c573966b2b1d..
SHA1:	a08966162e39fa0.
SHA256:	d062fa8446a39ad.
Infos:	

Most interesting Screenshot:



Detection

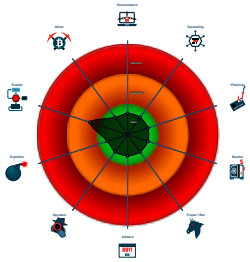


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- May sleep (evasive loops) to hinder …
- Contains long sleeps (>= 3 min)

Classification



Process Tree

- **System is w10x64**
- oYIQVnvsyG.exe (PID: 6364 cmdline: 'C:\Users\user\Desktop\oYIQVnvsyG.exe' MD5: 43C573966B2B1D5D87ECD57EB2A81C33)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

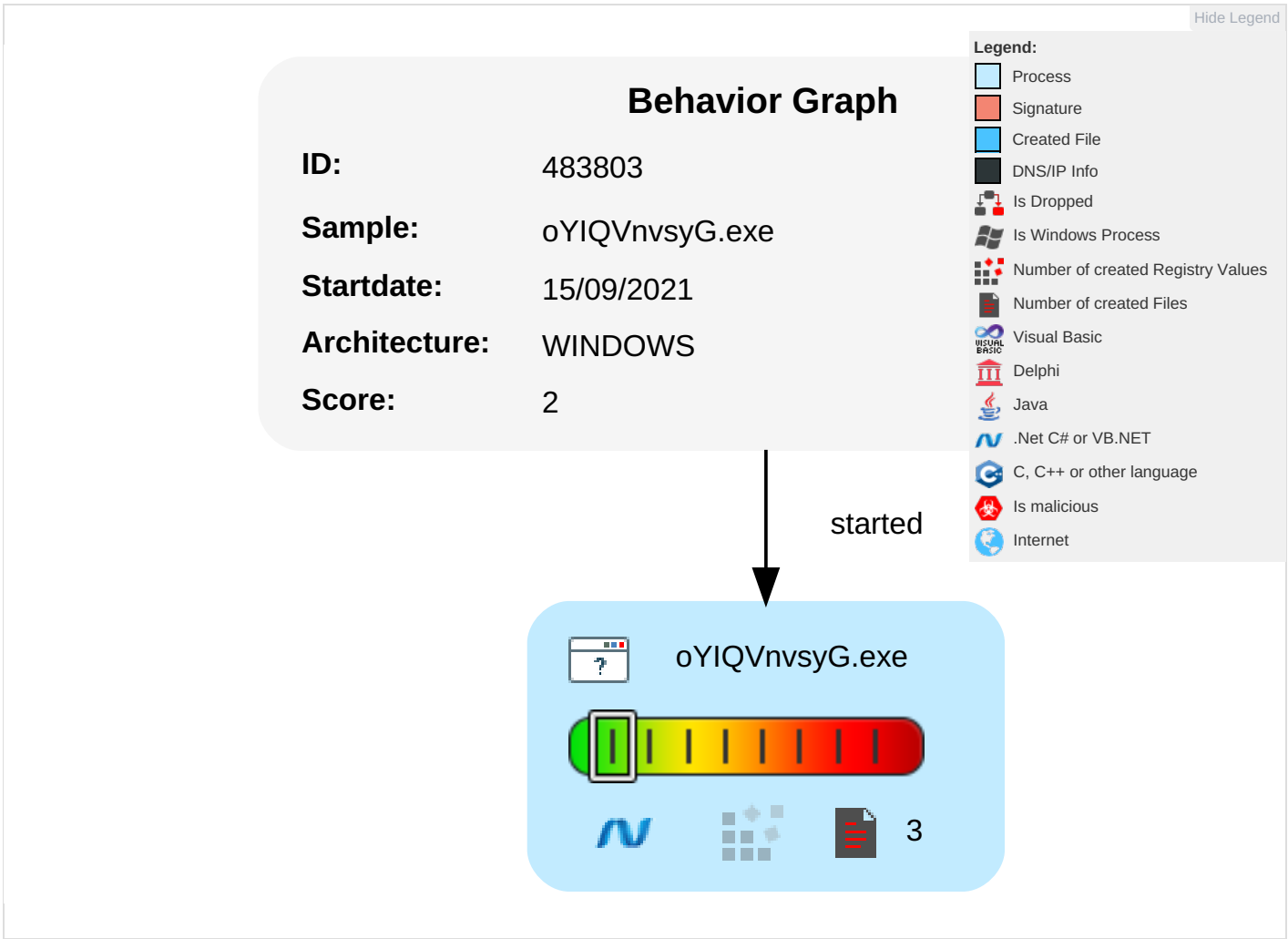
Click to jump to signature section

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	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	Virtualization/Sandbox Evasion 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C Ba

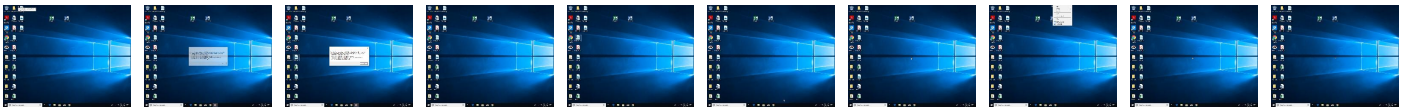
Behavior Graph



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
oYIQVnvsyG.exe	2%	Virustotal		Browse
oYIQVnvsyG.exe	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://go.microsz.R	0%	Avira URL Cloud	safe	

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:	483803
Start date:	15.09.2021
Start time:	14:05:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	oYIQVnvsyG.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:	28
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.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.3% (good quality ratio 27.3%) • Quality average: 86.3% • Quality standard deviation: 13.5%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\oYIQVnvsyG.exe.log	
Process:	C:\Users\user\Desktop\oYIQVnvsyG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	388
Entropy (8bit):	5.23028103270434
Encrypted:	false
SSDEEP:	6:Q3LadLCDDXTg+Q+OLC/7OHHHYyVLS71OiOLCMM3RUVb52RsM3RLWJiv:Q3LaJcP0kaHYGLi1B01kKVdisk7v
MD5:	1BD2C34B7EABD73D2C0CDDE3CEE7FDCF
SHA1:	BF6B01758B557773ED227763B3BEC9DA78470DCE
SHA-256:	EC866DF47E958210640D673E172656EE8F000C284FD7EAF60A309F7B4759FCD0
SHA-512:	7A00F54FDBC9E30F53CA8032A1E84599AC943B544E941569763E35BE0BEAC863AEE7E260158B512C2DCF080414173B66E948DD244B579E5EAB0AA14315260945
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System\1201f26cb986c93f55044bb4fa22b294\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\b12bbcf27f41d96fe44360ae0b566f9b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\454c09ea87bde1d5f545d60232083b79\System.Windows.Forms.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	2.7837838503558805

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	oYIQVnvsyG.exe
File size:	77824
MD5:	43c573966b2b1d5d87ecd57eb2a81c33
SHA1:	a08966162e39fa04e39d93b1d121f1bef6b3ec86
SHA256:	d062fa8446a39adb2182c2a506e96801792855bbb0da2a9f278134630a5e5de2
SHA512:	89c260ac4a42a9b706ed71b6a617d54980a09db512416(149126f3ebdd9d6165903828bf0e253acab04454ead0f58357c2893edb8174b0d11c5f9487d1af29ab
SSDEEP:	384:rvcXSvb3A9/96uiJII+Fv2chVzlzlzlzZehyik9WUZcXVJII+FXwQ5:rvDiF2ac09DZcXViJH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....5.\.....p..... ....`..... @.....

File Icon

Icon Hash:	daae97d9c8f6c6c6

Static PE Info

General

Entrypoint:	0x1100880e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x11000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5C12350C [Thu Dec 13 10:31:40 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6814	0x7000	False	0.231689453125	data	4.02819798601	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa000	0x9528	0xa000	False	0.0977783203125	data	2.04158250876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14000	0xc	0x1000	False	0.008544921875	data	0.0131269437212	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: oYIQVnvsyG.exe PID: 6364 Parent PID: 5384

General

Start time:	14:06:02
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\oYIQVnvsyG.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\oYIQVnvsyG.exe'
Imagebase:	0xf60000
File size:	77824 bytes
MD5 hash:	43C573966B2B1D5D87ECD57EB2A81C33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis