ID: 511181
Sample Name: 0klWxH7lko.exe
Cookbook: default.jbs
Time: 18:17:03
Date: 28/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

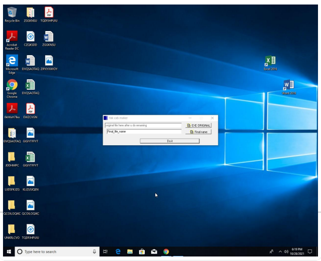
Windows Analysis Report 0klWxH7lko.exe

Overview

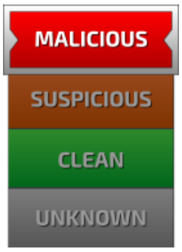
General Information

Sample Name:	0klWxH7lko.exe
Analysis ID:	511181
MD5:	8b1a607ffb0fc28…
SHA1:	a806a148512d7d..
SHA256:	07c670b4ae4318..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

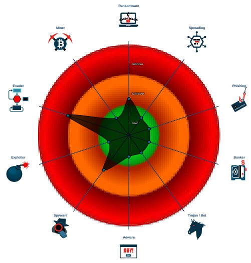


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Contains functionality to detect slee…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Sample file is different than original …
- Extensive use of GetProcAddress (o…
- Contains functionality to query locale…
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Found potential string decryption / a…
- Contains functionality to call native f…
- Contains functionality to retrieve info…
- Contains functionality to check if a w

Classification



Process Tree

- **System is w10x64**
- 0klWxH7lko.exe (PID: 4440 cmdline: 'C:\Users\user\Desktop\0klWxH7lko.exe' MD5: 8B1A607FFB0FC28A2CFC74782C86639E)
- **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

AV Detection:

Multi AV Scanner detection for submitted file

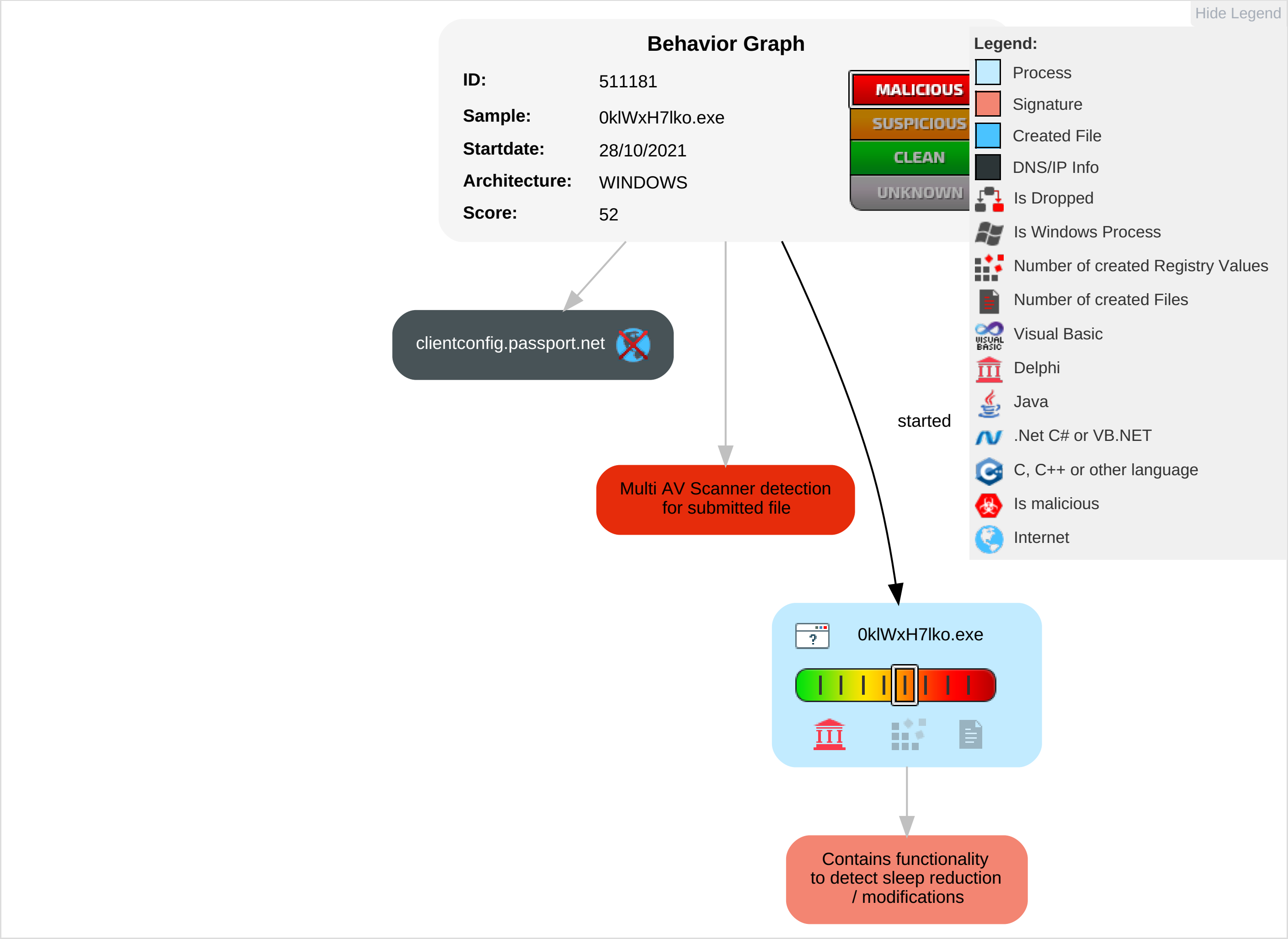
Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Ren Ser Effe
Valid Accounts	Native API 1	Application Shimming 1	Process Injection 1	Process Injection 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Ren Trac With Auth
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Security Software Discovery 1 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Ren Wip With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obta Dev Clou Bac
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Application Window Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

Behavior Graph



Behavior Graph

ID: 511181

Sample: 0klWxH7lko.exe

Startdate: 28/10/2021

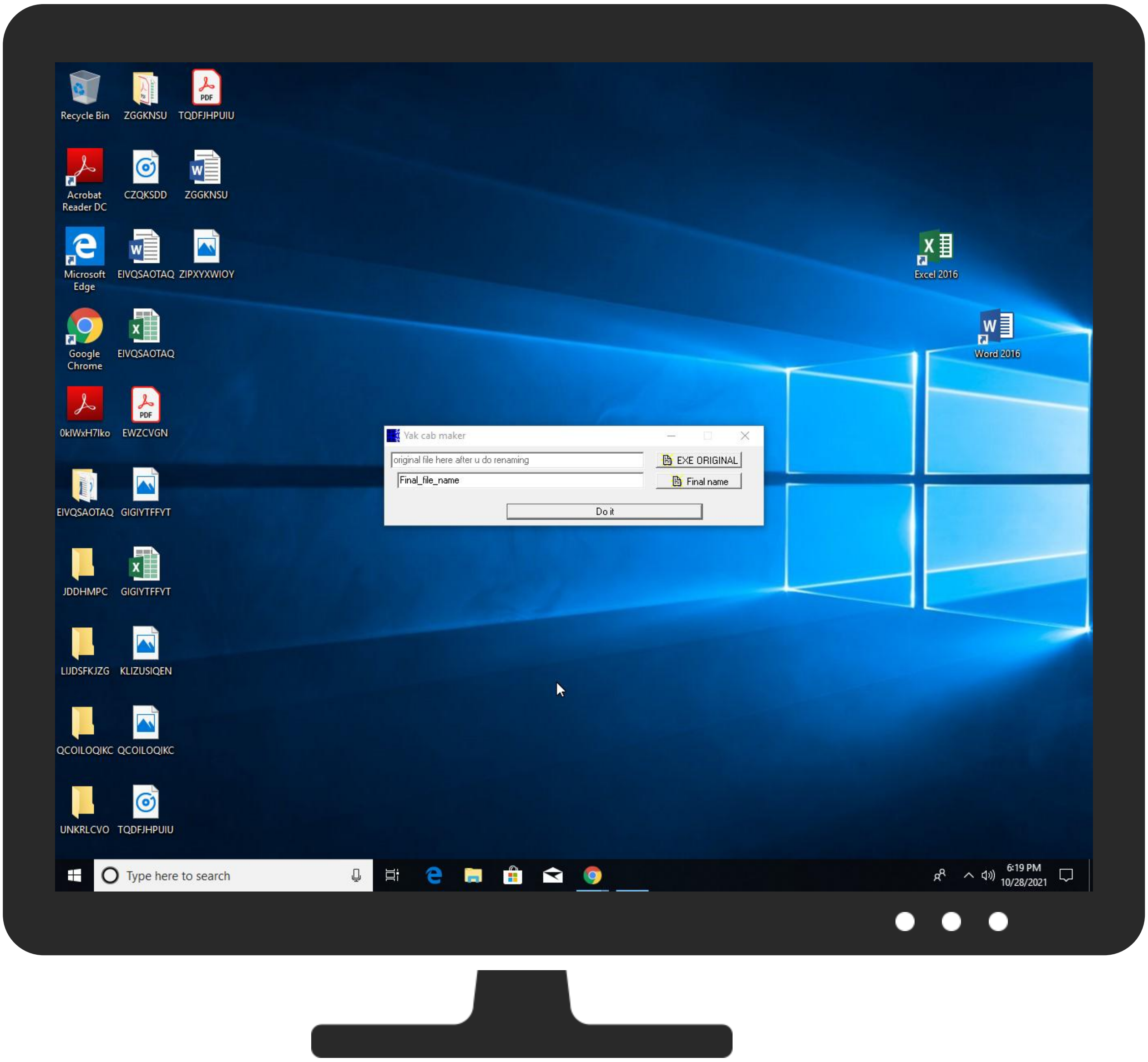
Architecture: WINDOWS

Score: 52

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
0kIWxH7lko.exe	20%	Virustotal		Browse
0kIWxH7lko.exe	23%	ReversingLabs	Win32.Trojan.Zusy	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.0kIWxH7lko.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clientconfig.passport.net	unknown	unknown	false		unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	511181
Start date:	28.10.2021
Start time:	18:17:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0klWxH7lko.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:	23
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:	mal52.evad.winEXE@1/0@1/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 99.4% (good quality ratio 97.1%) • Quality average: 85.7% • Quality standard deviation: 23.5%
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
Entropy (8bit):	6.588384260973668
TrID:	• Win32 Executable (generic) a (10002005/4) 99.66% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	0klWxH7lko.exe
File size:	494080
MD5:	8b1a607ffb0fc28a2cfc74782c86639e
SHA1:	a806a148512d7dcf8a3d5578bc8f76d8408ddc50
SHA256:	07c670b4ae43186e7e56124048946ba2f7324226359c10e344241e633773e6f0
SHA512:	8f9fe78bd44bb56030bfc811764fc12ba326e8026dfb82f5d39ea21b245355fb2a6b1daf023df9d8c82752e8c4f07495182757bd0eb6f75bdf8a8e20403b7c08
SSDEEP:	12288:3Tx+95sGgcw0q4UA6DzO35PCgPF+QhTW:3FGZJSoPF+Q9
File Content Preview:	MZP....................@..!..L.!..This program must be run under Win32..$7..

Static PE Info

General

Entrypoint:	0x455c38
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI

General

DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	099c74df59ac4f2d4be1deabe16b5180

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x54c80	0x54e00	False	0.532331553756	data	6.53716362692	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x56000	0x157f0	0x15800	False	0.510537790698	data	6.15046698513	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x6c000	0xba1	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x6d000	0x209e	0x2200	False	0.356158088235	data	4.91292422553	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x70000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x71000	0x18	0x200	False	0.05078125	data	0.164765012351	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x72000	0x5fdc	0x6000	False	0.624348958333	data	6.67168022676	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x5c00	0x5c00	False	0.296917459239	data	4.34148899694	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 18:18:14.673420906 CEST	192.168.2.5	8.8.8.8	0x5973	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 18:18:11.816294909 CEST	8.8.8.8	192.168.2.5	0xad19	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 18:18:14.695940971 CEST	8.8.8.8	192.168.2.5	0x5973	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: 0klWxH7lko.exe PID: 4440 Parent PID: 5912

General

Start time:	18:18:03
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\0klWxH7lko.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\0klWxH7lko.exe'
Imagebase:	0x400000
File size:	494080 bytes
MD5 hash:	8B1A607FFB0FC28A2CFC74782C86639E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal