ID: 482251
Sample Name: BK635636736_BOOKING CONFIRMATION.exe
Cookbook: default.jbs
Time: 15:29:03
Date: 13/09/2021
Version: 33.0.0 White Diamond

Table of Contents

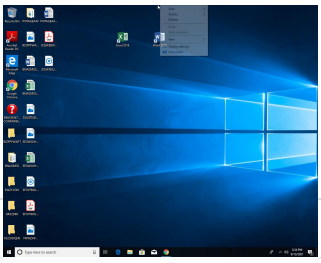
Windows Analysis Report BK635636736_BOOKING CON…

Overview

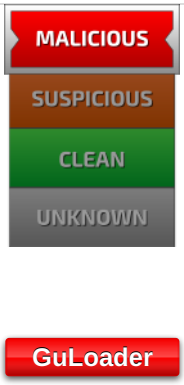
General Information

Sample Name:	BK635636736_BOOKING CONFIRMATION.exe
Analysis ID:	482251
MD5:	da33aac5f666cb1..
SHA1:	7a1c547f1c38b9f..
SHA256:	2217f0ae6d8b681.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



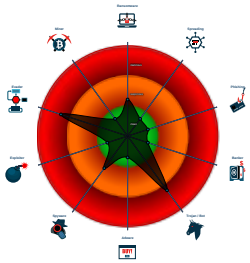
GuLoader

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Queries the volume information (nam…
- Sample file is different than original …
- PE file contains an invalid checksum
- PE file contains strange resources
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- BK635636736_BOOKING CONFIRMATION.exe (PID: 5588 cmdline: 'C:\Users\user\Desktop\BK635636736_BOOKING CONFIRMATION.exe' MD5: DA33AAC5F666CB19E32C78E1E8DDFEEF)
  - BK635636736_BOOKING CONFIRMATION.exe (PID: 2156 cmdline: 'C:\Users\user\Desktop\BK635636736_BOOKING CONFIRMATION.exe' MD5: DA33AAC5F666CB19E32C78E1E8DDFEEF)
- **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:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Hides threads from debuggers

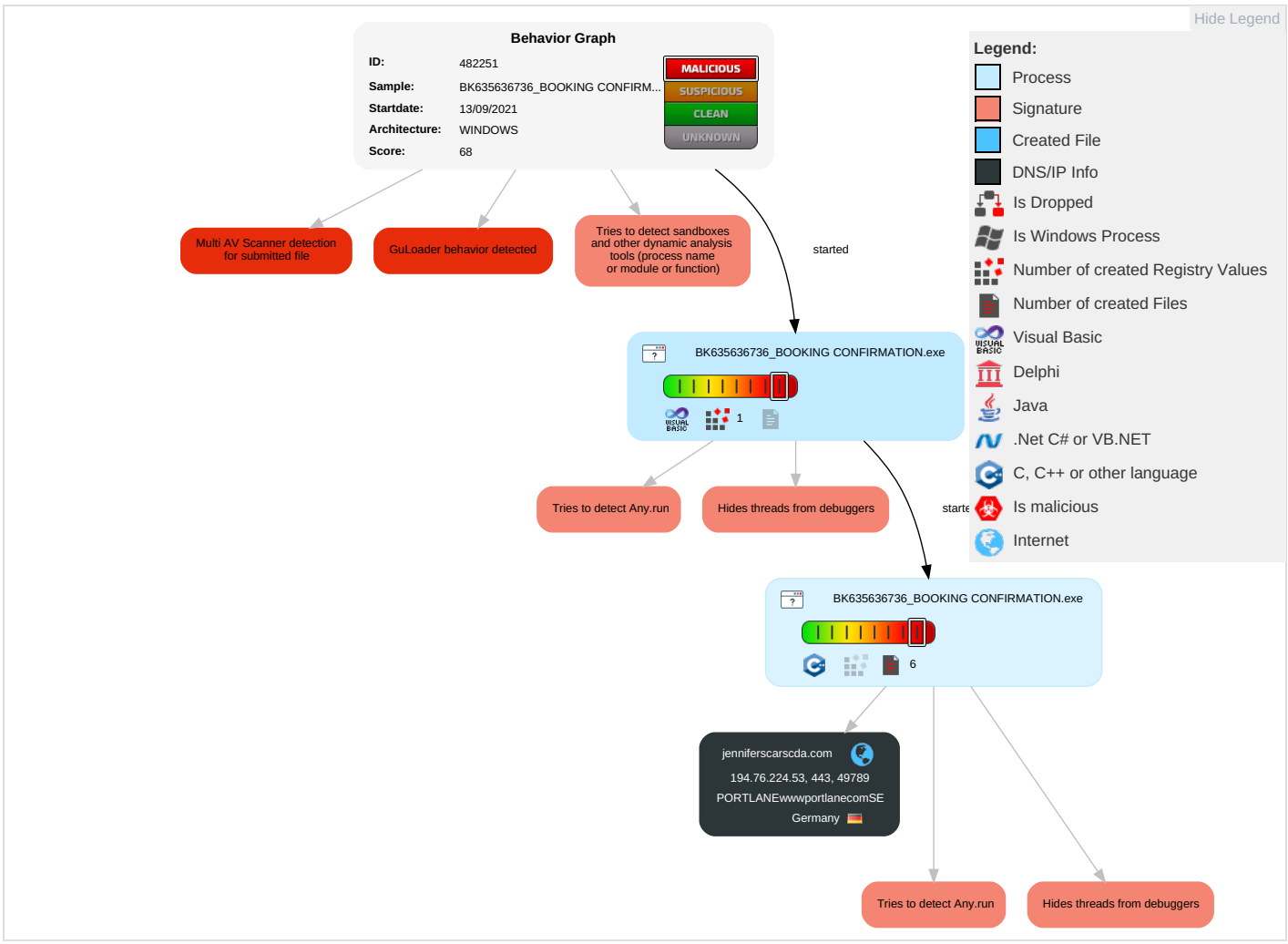
Stealing of Sensitive Information:

GuLoader behavior detected

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 2	Virtualization/Sandbox Evasion 2 1	Input Capture 1	Security Software Discovery 3 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location
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
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

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
BK635636736_BOOKING CONFIRMATION.exe	26%	Virustotal		Browse
BK635636736_BOOKING CONFIRMATION.exe	18%	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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jenniferscarscda.com	194.76.224.53	true	false		unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.76.224.53	jenniferscarscda.com	Germany		42708	PORTLANEwwwportlanecom SE	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482251
Start date:	13.09.2021
Start time:	15:29:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BK635636736_BOOKING CONFIRMATION.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:	31
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:	mal68.troj.evad.winEXE@3/0@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4% (good quality ratio 2.3%) • Quality average: 29.9% • Quality standard deviation: 27.3%
HCA Information:	• Successful, ratio: 76% • 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 • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.76.224.53	FC748478532_OCTOBER-SHIPMENT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
jenniferscarscda.com	FC748478532_OCTOBER-SHIPMENT.exe	Get hash	malicious	Browse	• 194.76.224.53

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PORTLANEwwwportlanecomSE	FC748478532_OCTOBER-SHIPMENT.exe	Get hash	malicious	Browse	• 194.76.224.53
	j3LQELTT0m	Get hash	malicious	Browse	• 188.126.80.93
	4nLik56DrD	Get hash	malicious	Browse	• 195.190.24 1.186
	message.html	Get hash	malicious	Browse	• 185.117.88.178
	qKxXZuMvtP	Get hash	malicious	Browse	• 5.254.217.55
	DF7049B8C4D704376BE3920232B1BA6B2C8CF2FF 0F9CF.exe	Get hash	malicious	Browse	• 46.21.100.248
	DF7049B8C4D704376BE3920232B1BA6B2C8CF2FF 0F9CF.exe	Get hash	malicious	Browse	• 46.21.100.248
	XwQCL6wkKk	Get hash	malicious	Browse	• 188.126.80.93
	document.htm .exe	Get hash	malicious	Browse	• 159.253.31.95
	ATTACHMENT.exe	Get hash	malicious	Browse	• 159.253.31.95
	ihdgexm.exe	Get hash	malicious	Browse	• 159.253.31.95
	letter.exe	Get hash	malicious	Browse	• 159.253.31.95
	readme.exe	Get hash	malicious	Browse	• 159.253.31.95
	ATTACHMENT.exe	Get hash	malicious	Browse	• 159.253.31.95
	ihdgexm.exe	Get hash	malicious	Browse	• 159.253.31.95
	letter.exe	Get hash	malicious	Browse	• 159.253.31.95
	readme.exe	Get hash	malicious	Browse	• 159.253.31.95
	adjunto.vbs	Get hash	malicious	Browse	• 188.126.90.9
	document.exe	Get hash	malicious	Browse	• 159.253.31.95
	document.exe	Get hash	malicious	Browse	• 159.253.31.95

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

General

Entropy (8bit):	4.2376796964620915
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	BK635636736_BOOKING CONFIRMATION.exe
File size:	471040
MD5:	da33aac5f666cb19e32c78e1e8ddfeef
SHA1:	7a1c547f1c38b9fe7b3a651787c863d490d294cc
SHA256:	2217f0ae6d8b681ae360e36dd03619b29c17bae98dbca0db4a9723ca0a386d37
SHA512:	5d803cc17e24157b27db6c0392399b5d1835b7c3eefecd272025a127059a6cfba5e4d8126b418e0b0a172f9f78972246f82500eb688c6a3836be84d9e089ff35
SSDEEP:	6144:xqqadRaFlGCfS/GLUCffBfRfBfBG/qFGGGGGGGG0GGGGGGGGGGGGGGGGGGLGGGGR:xdnFMnDeJDFE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...W...W...W...K...W...u...W...q...W..Rich.W.....PE..L....E.K.....`.....H.....p....@

File Icon

Icon Hash:	70f0a235b1b2f071

Static PE Info

General

Entrypoint:	0x401448
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4B8B45E6 [Mon Mar 1 04:43:18 2010 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:	01b006fd37878659f6f60ca0efdc2460

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x451e8	0x46000	False	0.270354352679	data	4.80062436371	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x47000	0x148c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x49000	0x2a13e	0x2b000	False	0.162342160247	data	3.15700240055	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
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 13, 2021 15:33:52.093537092 CEST	192.168.2.3	8.8.8.8	0x4e03	Standard query (0)	jennifersc arscda.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 13, 2021 15:33:52.133460999 CEST	8.8.8.8	192.168.2.3	0x4e03	No error (0)	jennifersc arscda.com		194.76.224.53	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: BK635636736_BOOKING CONFIRMATION.exe PID: 5588 Parent PID: 5864

General

Start time:	15:29:57
Start date:	13/09/2021
Path:	C:\Users\user\Desktop\BK635636736_BOOKING CONFIRMATION.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BK635636736_BOOKING CONFIRMATION.exe'
Imagebase:	0x400000
File size:	471040 bytes
MD5 hash:	DA33AAC5F666CB19E32C78E1E8DDFEEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: BK635636736_BOOKING CONFIRMATION.exe PID: 2156 Parent PID: 5588

General

Start time:	15:31:51
Start date:	13/09/2021
Path:	C:\Users\user\Desktop\BK635636736_BOOKING CONFIRMATION.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BK635636736_BOOKING CONFIRMATION.exe'
Imagebase:	0x400000
File size:	471040 bytes
MD5 hash:	DA33AAC5F666CB19E32C78E1E8DDFEEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

Disassembly

Code Analysis