

JoeSandbox Cloud BASIC



ID: 458277

Sample Name: KHAWATMI
CO.IMPORT & EXPORT.exe

Cookbook: default.jbs

Time: 07:55:58

Date: 03/08/2021

Version: 33.0.0 White Diamond


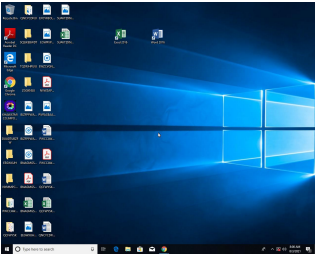
Table of Contents

Table of Contents	2
Windows Analysis Report KHAWATMI CO.IMPORT & EXPORT.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	4
AV Detection:	4
Networking:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Stealing of Sensitive Information:	4
Mitre Att&ck Matrix	4
Behavior Graph	5
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted URLs	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	9
Statistics	10
Behavior	10
System Behavior	10
Analysis Process: KHAWATMI CO.IMPORT & EXPORT.exe PID: 5948 Parent PID: 5608	10
General	10
File Activities	10
Analysis Process: KHAWATMI CO.IMPORT & EXPORT.exe PID: 5004 Parent PID: 5948	10
General	10
Disassembly	10
Code Analysis	10

Windows Analysis Report KHAWATMI CO.IMPORT & EX...

Overview

General Information

Sample Name:	KHAWATMI CO.IMPORT & EXPORT.exe
Analysis ID:	458277
MD5:	0153ae8cf4b1f54..
SHA1:	479858ef740172c.
SHA256:	97fee7e2c533d7a.
Tags:	exe
Infos:	
Most interesting Screenshot:	
	

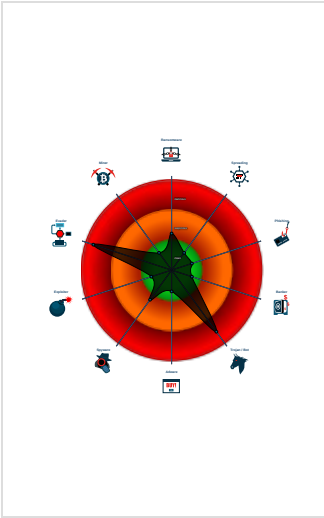
Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div> <div>GuLoader</div>	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%



Signatures

Found malware configuration
GuLoader behavior detected
Multi AV Scanner detection for subm...
Yara detected GuLoader
C2 URLs / IPs found in malware con...
Contains functionality to detect hard...
Detected RDTSC dummy instruction...
Found potential dummy code loops (...)
Hides threads from debuggers
Tries to detect Any.run
Tries to detect sandboxes and other...
Tries to detect virtualization through...

Classification



Process Tree

- System is w10x64
-  KHAWATMI CO.IMPORT & EXPORT.exe (PID: 5948 cmdline: 'C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe' MD5: 0153AE8CF4B1F546721332B5CB3F973C)
 -  KHAWATMI CO.IMPORT & EXPORT.exe (PID: 5004 cmdline: 'C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe' MD5: 0153AE8CF4B1F546721332B5CB3F973C)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/download?cid=7B0580AA0B18AE"
}
```

Yara Overview


Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.583437179.0000000003BD 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Networking:



C2 URLs / IPs found in malware configuration

Data Obfuscation:



Yara detected GuLoader

Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:



Found potential dummy code loops (likely to delay analysis)

Hides threads from debuggers

Stealing of Sensitive Information:

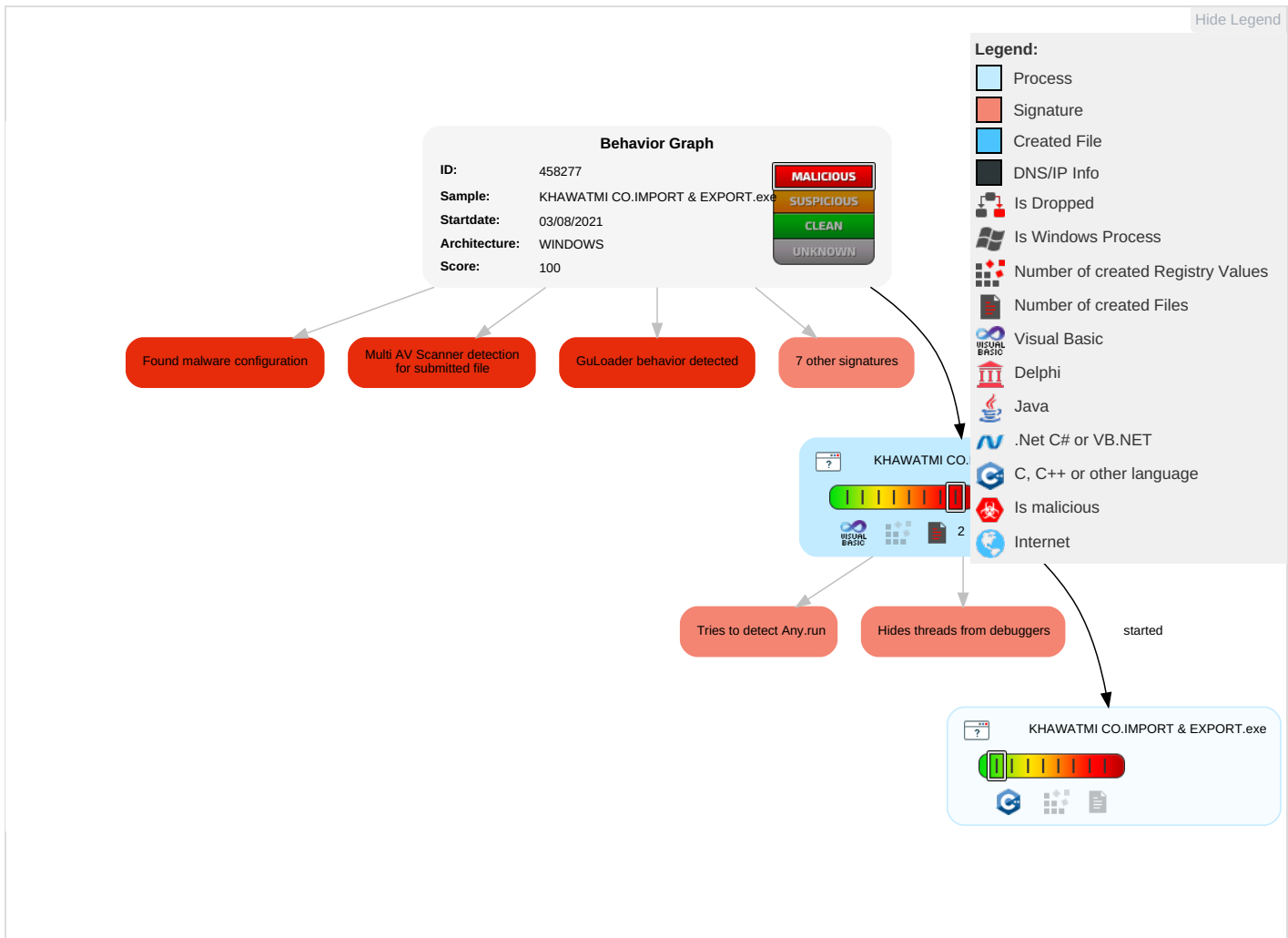


GuLoader behavior detected

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 3 1 1	Input Capture 1 1	Security Software Discovery 7 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop 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 3 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS Redirct F 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	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 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	System Information Discovery 3 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi

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
KHAWATMI CO.IMPORT & EXPORT.exe	13%	ReversingLabs	Win32.Trojan.AgentTesla	

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 URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=7B0580AA0B18AE	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458277
Start date:	03.08.2021
Start time:	07:55:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KHAWATMI CO.IMPORT & EXPORT.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:	33
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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 2.2% (good quality ratio 0.2%)• Quality average: 1.5%• Quality standard deviation: 4.5%
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 64%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• 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

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):	6.387725511048366
TrID:	<ul style="list-style-type: none">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:	KHAWATMI CO.IMPORT & EXPORT.exe
File size:	147456
MD5:	0153ae8cf4b1f546721332b5cb3f973c
SHA1:	479858ef740172cb3791527a9c9d0da76eec3af4
SHA256:	97fee7e2c533d7ad3854cd92d9d2dbcddeb3b08e3e0cb14214b431d3970cda45
SHA512:	1a6ae92b4937ea140069189487e669377f8a59ceffa29597f18c94d83646184344f4ba4d0fe42ce5153d95791ad31b3fe8b715b6a55fe3b923ce59fd4201bac1
SSDEEP:	1536:EtVr5LC183SqwDIse4yckz/50ZG8tnSSyeMn5iXDjTf8+Oh1K:E/5CIRwDdeZcFYeMn5iXDj5Oh1K
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$.#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...#.V.....0.....@.....

File Icon



Icon Hash:

c4e8c8ccce0e8e8

Static PE Info

General

Entrypoint:	0x4014b4
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:	0x56A2ED23 [Sat Jan 23 03:01:55 2016 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:	fef384fc3a66a559dff455f07d497ca0

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2010c	0x21000	False	0.378292199337	data	6.67763542403	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x11bc	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0xbfc	0x1000	False	0.310791015625	data	3.24011988097	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
Chinese	Taiwan	


Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: KHAWATMI CO.IMPORT & EXPORT.exe PID: 5948 Parent PID: 5608

General

Start time:	07:56:44
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	0153AE8CF4B1F546721332B5CB3F973C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.583437179.0000000003BD0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: KHAWATMI CO.IMPORT & EXPORT.exe PID: 5004 Parent PID: 5948

General

Start time:	07:59:42
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	0153AE8CF4B1F546721332B5CB3F973C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis

