

JOeSandbox Cloud BASIC



ID: 357266

Sample Name: FAKTURA I
UWAGI.bat

Cookbook: default.jbs

Time: 11:03:49

Date: 24/02/2021

Version: 31.0.0 Emerald

Table of Contents

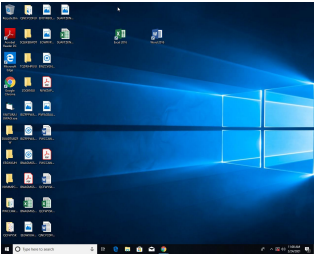
Table of Contents	2
Analysis Report FAKTURA I UWAGI.bat	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Memory Dumps	4
Sigma Overview	4
Signature Overview	5
AV Detection:	5
Compliance:	5
System Summary:	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
Anti Debugging:	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	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted IPs	8
General Information	8
Simulations	8
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	9
General	9
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	10
Data Directories	10
Sections	11
Resources	11
Imports	11
Version Infos	11
Possible Origin	11
Network Behavior	11
Code Manipulations	11

Statistics	12
System Behavior	12
Analysis Process: FAKTURA I UWAGI.exe PID: 6492 Parent PID: 5660	12
General	12
File Activities	12
Disassembly	12
Code Analysis	12

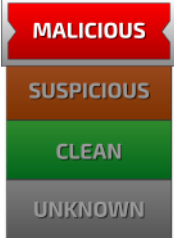
Analysis Report FAKTURA I UWAGI.bat

Overview

General Information

Sample Name:	FAKTURA I UWAGI.bat (renamed file extension from bat to exe)
Analysis ID:	357266
MD5:	2c3b4c255d8d78..
SHA1:	3cc1d799b6f92a3..
SHA256:	46c474c38fd6790..
Tags:	GuLoader
Infos:	 
Most interesting Screenshot:	
	

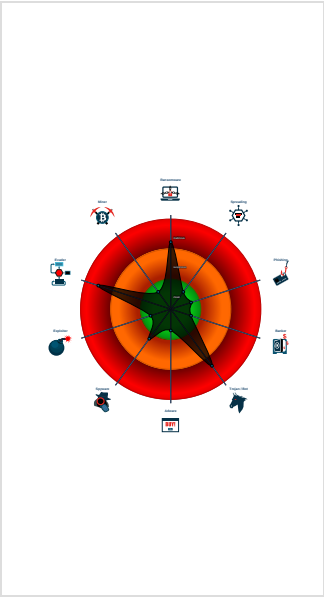
Detection

	
	
Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm...
Potential malicious icon found
Yara detected GuLoader
Contains functionality to detect hard...
Detected RDTSC dummy instruction...
Found potential dummy code loops (...)
Tries to detect sandboxes and other...
Tries to detect virtualization through...
Yara detected VB6 Downloader Gen...
Abnormal high CPU Usage
Contains functionality for execution ...
Contains functionality to query CPU ...
Contains functionality to read the PEB
Detected potential crypto function

Classification



Startup

▪ System is w10x64
•  FAKTURA I UWAGI.exe (PID: 6492 cmdline: 'C:\Users\user\Desktop\FAKTURA I UWAGI.exe' MD5: 2C3B4C255D8D786535C4832F5B7F7C0E)
▪ cleanup

Malware Configuration

No configs have been found

Yara Overview

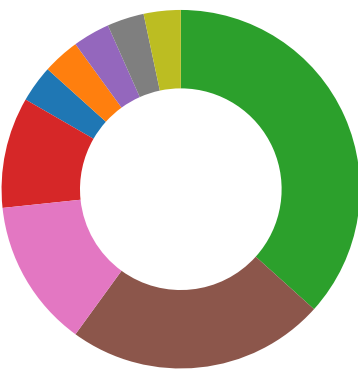
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: FAKTURA I UWAGI.exe PID: 6492	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: FAKTURA I UWAGI.exe PID: 6492	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

 Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Compliance:



Uses 32bit PE files

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Yara detected VB6 Downloader Generic

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:



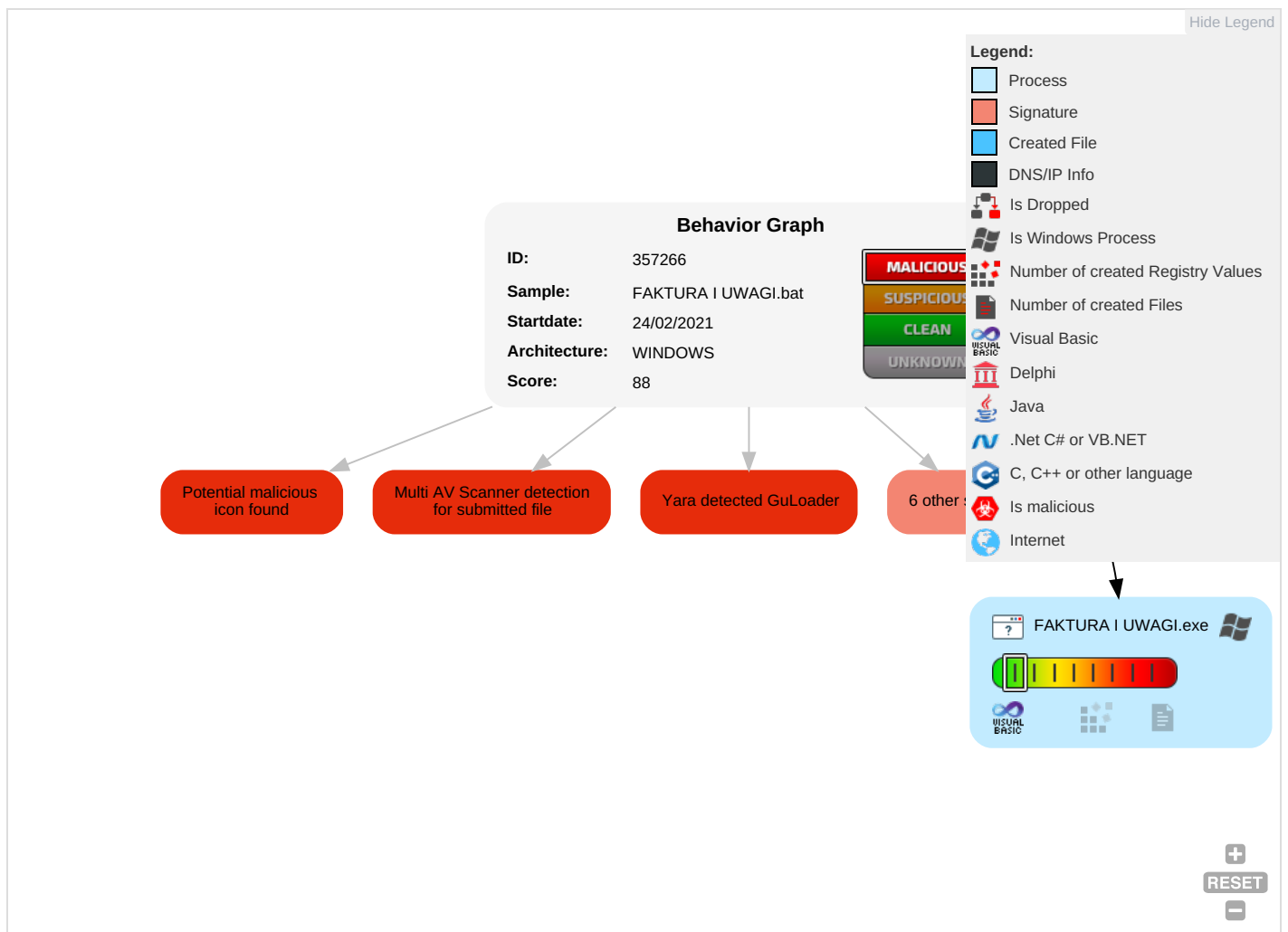
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Reported
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 5 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Reported by TTPs

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Risk Score
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Risk Score
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 SS7 to Track Device Location	Risk Score
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Risk Score

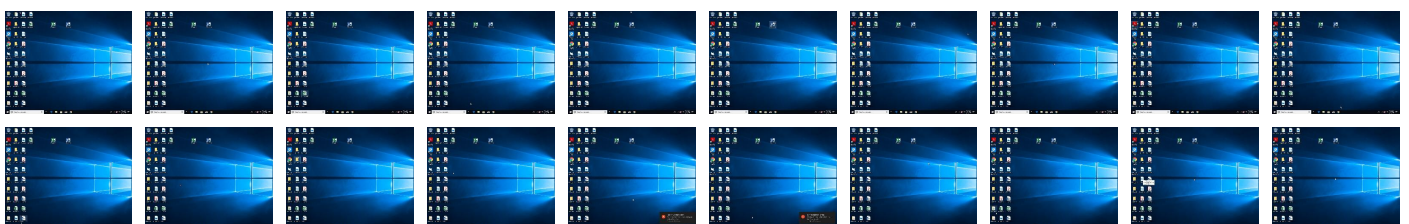
Behavior Graph



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
FAKTURA I UWAGI.exe	42%	Virustotal		Browse
FAKTURA I UWAGI.exe	36%	ReversingLabs	Win32.Trojan.VBObfuse	

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 IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357266
Start date:	24.02.2021
Start time:	11:03:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FAKTURA I UWAGI.bat (renamed file extension from bat to 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:	29
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:	mal88.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.1% (good quality ratio 14.5%) • Quality average: 34.6% • Quality standard deviation: 33.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe

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):	4.798232487088525
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:	FAKTURA UWAGI.exe
File size:	61440
MD5:	2c3b4c255d8d786535c4832f5b7f7c0e
SHA1:	3cc1d799b6f92a338cfa35d74d52b1c4f19a91e
SHA256:	46c474c38fd679025142a453fc46243a91e0820d4ab0449aab0bd92c29d0ee30
SHA512:	847d322ab76b98b24cc12c0591b2e4a8cf78afe8411e18aefc10eb1bc9824eb6251000a043403fc4ff6cebef523fbe3fd09554a2f442f1eea28ee25329a064e3
SSDEEP:	768:AZI4oR9Y0oIF+ik9FQGDMcZ7/R9hxiB6oRiU:IZR9FoIFo9FQgD1iVI
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode...\$.....#...B...B...B...L^...B...`...B...d...B..Rich.B.....PE.L...[.P.....0.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4012c4
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:	0x509C5BCE [Fri Nov 9 01:26:38 2012 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:	f8fb5be8a6ea86fb9d04da61d8bfeb3a

Entrypoint Preview

Instruction

push 004014F4h
call 00007F030C7AC163h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edx], ch
test dh, al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc234	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf000	0x9ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xd0	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb608	0xc000	False	0.456787109375	data	5.50676985986	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xd000	0x118c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xf000	0x9ac	0x1000	False	0.180419921875	data	2.10150879762	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xf87c	0x130	data		
RT_ICON	0xf594	0x2e8	data		
RT_ICON	0xf46c	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xf43c	0x30	data		
RT_VERSION	0xf150	0x2ec	data	Hungarian	Hungary

Imports

DLL	Import
MSVBVM60.DLL	_Cicos, _adj_fptan, __vbaVarMove, __vbaAryMove, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptionHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _Cilog, __vbaErrorOverflow, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarDup, _Clatan, __vbaCastObj, _allmul, _Cltan, _Clexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x040e 0x04b0
LegalCopyright	Copyright (C) AC
InternalName	dosisspspiro
FileVersion	1.00
CompanyName	AC
LegalTrademarks	Copyright (C) AC
Comments	AC
ProductName	AC
ProductVersion	1.00
FileDescription	AC
OriginalFilename	dosisspspiro.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Hungarian	Hungary	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: FAKTURA I UWAGI.exe PID: 6492 Parent PID: 5660

General

Start time:	11:04:36
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\FAKTURA I UWAGI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FAKTURA I UWAGI.exe'
Imagebase:	0x400000
File size:	61440 bytes
MD5 hash:	2C3B4C255D8D786535C4832F5B7F7C0E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Disassembly

Code Analysis