

JoeSandbox Cloud BASIC



ID: 394253

Sample Name: faktura_fk.exe

Cookbook: default.jbs

Time: 11:18:37

Date: 21/04/2021

Version: 31.0.0 Emerald

Table of Contents

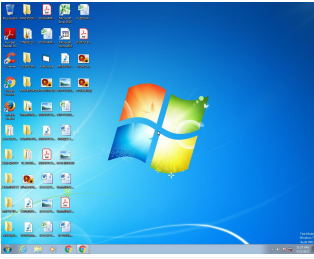
Table of Contents	2
Analysis Report faktura_fk.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: GuLoader	4
Yara Overview	4
Memory Dumps	4
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Networking:	5
System Summary:	5
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	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
Contacted IPs	8
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	10
General	10
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	11
Data Directories	11
Sections	12
Resources	12
Imports	12
Version Infos	12
Possible Origin	12

Network Behavior	13
Code Manipulations	13
Statistics	13
System Behavior	13
Analysis Process: faktura_fk.exe PID: 284 Parent PID: 2936	13
General	13
File Activities	13
Disassembly	13
Code Analysis	13

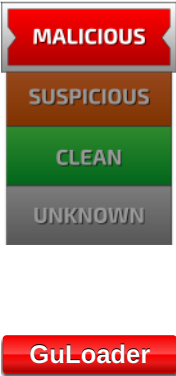
Analysis Report faktura_fk.exe

Overview

General Information

Sample Name:	faktura_fk.exe
Analysis ID:	394253
MD5:	66fb235f133e2f6...
SHA1:	12f471ad9d4f8ef...
SHA256:	168ca422e4a4dc...
Infos:	
Most interesting Screenshot:	

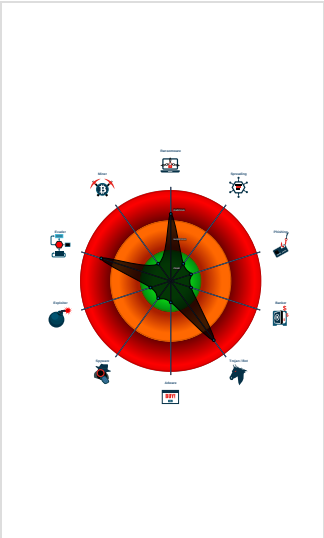
Detection

	
Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Potential malicious icon found
Yara detected GuLoader
C2 URLs / IPs found in malware con...
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
Allocates memory within range whic...
PE file contains strange resources

Classification



Startup

- System is w7x64
-  faktura_fk.exe (PID: 284 cmdline: 'C:\Users\user\Desktop\faktura_fk.exe' MD5: 66FB235F133E2F690184675FE27BCC32)
- cleanup

Malware Configuration

Threatname: GuLoader

<pre>{ "Payload URL": "https://drive.google.com/uc?export=download&id=107Zrj0oTVUPxo7h5le0qWms20f0kCgBK", "Injection Process": ["RegAsm.exe", "RegSvc.exe", "MSBuild.exe"] }</pre>
--

Yara Overview

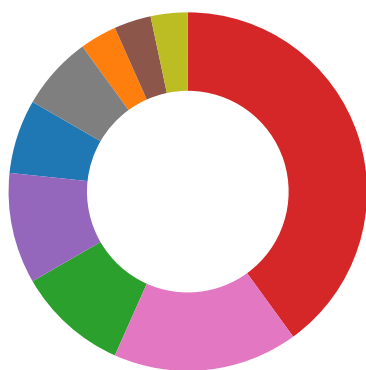
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.3147398939.00000000002 D0000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: faktura_fk.exe PID: 284	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: faktura_fk.exe PID: 284	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

💡 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

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:



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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
faktura_fk.exe	18%	Virustotal		Browse
faktura_fk.exe	7%	ReversingLabs	Win32.Worm.Wbvb	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	faktura_fk.exe, 00000000.00000 002.3151745116.000000000351700 0.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	faktura_fk.exe, 00000000.00000 002.3151288024.000000000333000 0.00000002.00000001.sdmp	false		high
http://investor.msn.com	faktura_fk.exe, 00000000.00000 002.3151288024.000000000333000 0.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	faktura_fk.exe, 00000000.00000 002.3151288024.000000000333000 0.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	faktura_fk.exe, 00000000.00000 002.3151745116.000000000351700 0.00000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	faktura_fk.exe, 00000000.00000 002.3151745116.000000000351700 0.00000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.hotmail.com/oe	faktura_fk.exe, 00000000.00000 002.3151288024.000000000333000 0.00000002.00000001.sdmp	false		high
http://investor.msn.com/	faktura_fk.exe, 00000000.00000 002.3151288024.000000000333000 0.00000002.00000001.sdmp	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	394253
Start date:	21.04.2021
Start time:	11:18:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	faktura_fk.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	2
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:	mal96.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 76% (good quality ratio 50.6%) • Quality average: 35.2% • Quality standard deviation: 31%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): dllhost.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):	5.743984981466137
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_fk.exe
File size:	208896
MD5:	66fb235f133e2f690184675fe27bcc32
SHA1:	12f471ad9d4f8ef90cc548d1e0eb498c12ed0230
SHA256:	168ca422e4a4dc429c9fb4a65cdd1b3f1f32119475581b3d00c94ff6e4a82f77
SHA512:	1dd20f688ab25131fc8b9c8a2b68d87f468e45ae7b69594e78012353aad2cbde1c3f82f9eecb605d1787e56c9b7b26dfc6f4abc2164d1b347d08516824b8aa8c
SSDEEP:	3072:+tYMTBHA4Pid5lQrh5aAf1gaVcjQ0Rkkw7OAEvkcvdzHRe4YJv:UQjPOE1gaVBsDYEbvdLq
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...I..`.....0.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401d94
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:	0x607FB66C [Wed Apr 21 05:21:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General		
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:		e1435fa7344f6ab2e745b6e31d83ea55

Entrypoint Preview

Instruction		
push 00401FF4h		
call 00007F92C08182E5h		
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-7F47AE6Eh], dh		
sar eax, cl		
dec esp		
call far B1A4h : AFF4E401h		
xor al, byte ptr [eax]		
add byte ptr [eax], al		
add byte ptr [eax], al		
add byte ptr [ecx], al		
add byte ptr [eax], al		
add byte ptr [eax], al		
add byte ptr [eax+49030A64h], ah		
dec esi		
inc esp		
inc esp		
dec ebx		
dec esi		
dec ecx		
dec esi		
inc edi		
add byte ptr [ecx+00h], al		
and byte ptr [eax], cl		
inc ecx		
add byte ptr [eax], al		
add byte ptr [eax], al		
add bh, bh		
int3		
xor dword ptr [eax], eax		
push es		
pop ecx		
jnb 00007F92C08182F8h		
mov dh, 2Bh		
pop esp		
cli		
dec ebx		
stosd		
mov ebx, 4D7B8DF1h		
retf		

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2fa64	0x28	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x33000	0x958	.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	0x1bc	.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	0x2f0a8	0x30000	False	0.339920043945	data	5.91772288462	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x31000	0x1228	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x33000	0x958	0x1000	False	0.1708984375	data	2.02469330583	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x33828	0x130	data		
RT_ICON	0x33540	0x2e8	data		
RT_ICON	0x33418	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x333e8	0x30	data		
RT_VERSION	0x33150	0x298	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_Cicos, __adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, __adj_fdiv_m64, __vbaFreeObjList, __adj_fprem1, __vbaRecAnsiToUni, __vbaSetSystemError, __vbaHresultCheckObj, __adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, __adj_fdiv_m16i, __vbaObjSetAddr, __adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaObjVar, DllFunctionCall, __adj_fpatan, __vbaLateIdCall, __vbaRedim, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __adj_fprem, __adj_fdivr_m64, __vbaFPEException, _Cilog, __vbaFileOpen, __vbaNew2, __adj_fdiv_m32i, __adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, __vbaDerefAry1, __adj_fdivr_m32, __adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaVarDup, __vbaStrToAnsi, __vbaStrComp, _Clatan, __vbaStrMove, __vbaCastObj, __allmul, __vbaLateIdSt, _Cltan, _Clexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0404 0x04b0
InternalName	Knudepunkternes2
FileVersion	1.00
CompanyName	eSafe Solutions
ProductName	eSafe Solutions
ProductVersion	1.00
FileDescription	eSafe Solutions
OriginalFilename	Knudepunkternes2.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Language of compilation system	Country where language is spoken	Map

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: faktura_fk.exe PID: 284 Parent PID: 2936

General

Start time:	11:19:32
Start date:	21/04/2021
Path:	C:\Users\user\Desktop\faktura_fk.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\faktura_fk.exe'
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	66FB235F133E2F690184675FE27BCC32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000000.00000002.3147398939.00000000002D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

Disassembly

Code Analysis