ID: 433220
Sample Name:
Faktura_21611447.exe
Cookbook: default.jbs
Time: 13:23:20
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

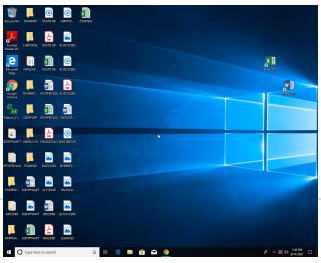
Analysis Report Faktura_21611447.exe

Overview

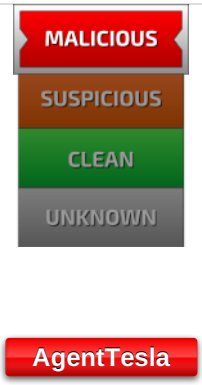
General Information

Sample Name:	Faktura_21611447.exe
Analysis ID:	433220
MD5:	37178995799dac..
SHA1:	7653bcfc4a5dc75..
SHA256:	b86fbdeb14cd6cd..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



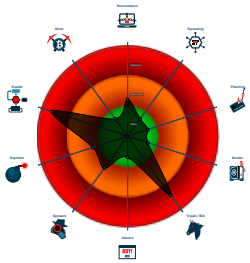
AgentTesla

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Faktura_21611447.exe (PID: 4632 cmdline: 'C:\Users\user\Desktop\Faktura_21611447.exe' MD5: 37178995799DAC98CF429B946925E324)
  - Faktura_21611447.exe (PID: 5800 cmdline: {path} MD5: 37178995799DAC98CF429B946925E324)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "administracion@gruposolve.estT^eJ7+z7MXqmail.gruposolve.esalfredbnolan@yandex.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.493773129.0000000002B1 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.493773129.0000000002B1 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000012.00000002.489763681.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.489763681.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.323889609.0000000003D5 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 8 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Faktura_21611447.exe.3e1adb8.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Faktura_21611447.exe.3e1adb8.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
18.2.Faktura_21611447.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.Faktura_21611447.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
18.0.Faktura_21611447.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

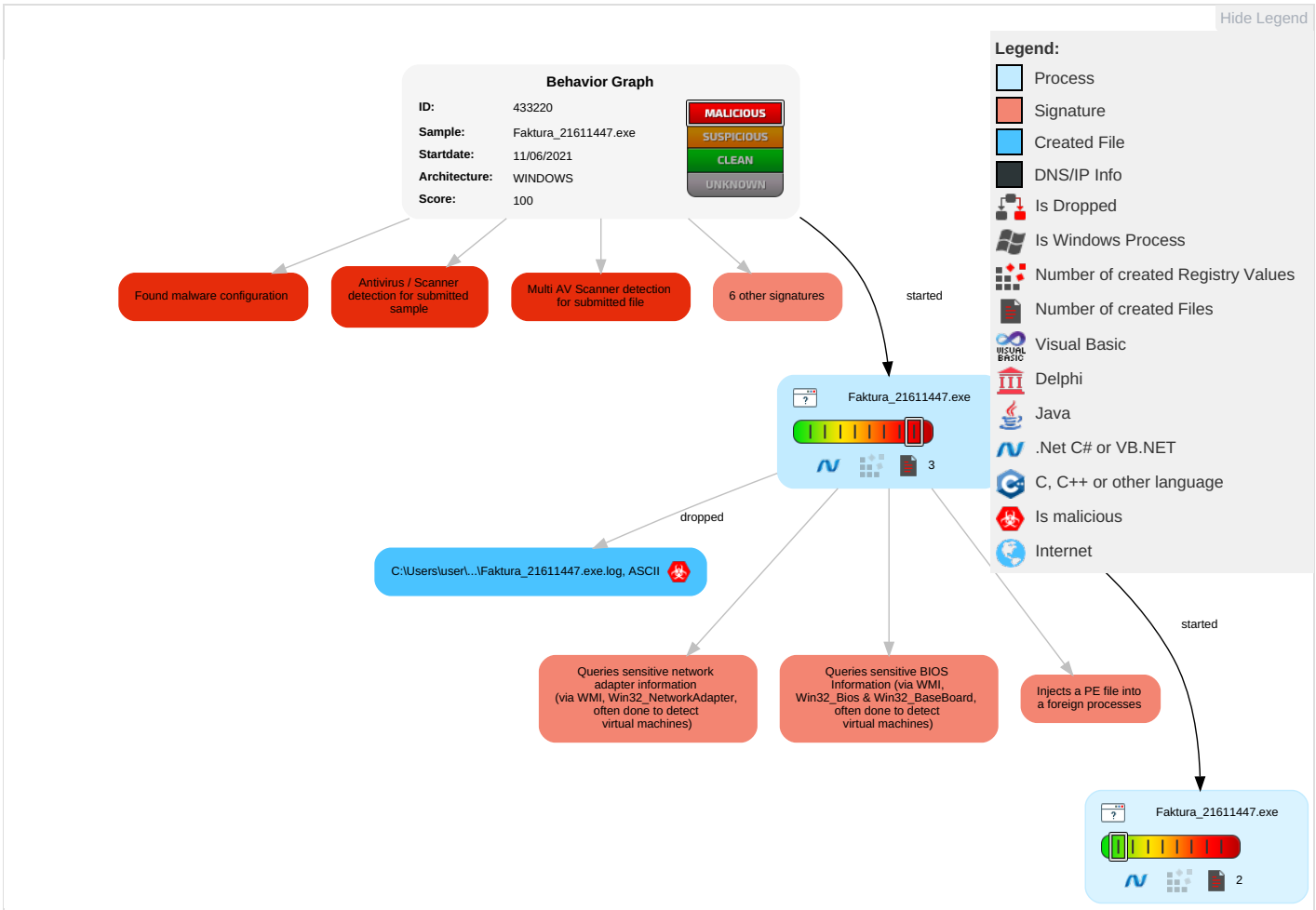
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	E
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E I N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A

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_21611447.exe	31%	Virustotal		Browse
Faktura_21611447.exe	100%	Avira	HEUR/AGEN.1129504	
Faktura_21611447.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Faktura_21611447.exe.880000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
18.2.Faktura_21611447.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.Faktura_21611447.exe.570000.2.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
18.0.Faktura_21611447.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.Faktura_21611447.exe.570000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
18.2.Faktura_21611447.exe.570000.1.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
0.2.Faktura_21611447.exe.880000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnv1	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cnE	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://IzzKkp.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.galapagosdesign.com/zY	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433220
Start date:	11.06.2021
Start time:	13:23:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Faktura_21611447.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:	28
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.evad.winEXE@3/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.4%) • Quality average: 42.6% • Quality standard deviation: 38.2%
HCA Information:	• Successful, ratio: 99% • 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
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:25:07	API Interceptor	470x Sleep call for process: Faktura_21611447.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Faktura_21611447.exe.log	
Process:	C:\Users\user\Desktop\Faktura_21611447.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.5725309673566645
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Faktura_21611447.exe
File size:	604160
MD5:	37178995799dac98cf429b946925e324
SHA1:	7653bcfc4a5dc75afa7efa2aa2531acd06b25679
SHA256:	b86fbdeb14cd6cd5b5e144d029844e1c7d6e51c82b1bb7c3f0f07f8ff07258c9

General

SHA512:	5eb6f61685fe7c1f4a280beedbee8b683ab0ace5779957fdf09555aa271cc52f2492ccaa022cece0ddd691f90b0c8196da0db9f8fd88fdb4fd7b593d59598138
SSDEEP:	12288:j/q6TjxgijIx2x6bg1ZXCtJ0TvbK3w9hhm45vnS8m2WhG4g7JLM+YtesminEY:eexvjYn81ZXoJMvby0hQ4JnjY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....%.`.....0.."..... @... ...`....@.. ....@.....

File Icon

Icon Hash:	18da1abcb2d2d2b0

Static PE Info

General

Entrypoint:	0x49408e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C325D1 [Fri Jun 11 08:58:57 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x92094	0x92200	False	0.804253100941	data	7.59684776596	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x96000	0x1058	0x1200	False	0.269748263889	data	2.8444952776	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x98000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Faktura_21611447.exe PID: 4632 Parent PID: 5856

General

Start time:	13:24:08
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Faktura_21611447.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Faktura_21611447.exe'
Imagebase:	0x880000
File size:	604160 bytes
MD5 hash:	37178995799DAC98CF429B946925E324
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.323889609.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.323889609.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.321816701.0000000002DAC000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Faktura_21611447.exe PID: 5800 Parent PID: 4632

General

Start time:	13:24:51
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Faktura_21611447.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x570000

File size:	604160 bytes
MD5 hash:	37178995799DAC98CF429B946925E324
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.493773129.0000000002B11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.493773129.0000000002B11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.489763681.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000002.489763681.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.318036726.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.318036726.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis