ID: 502592
Sample Name: Proforma Invoice.exe
Cookbook: default.jbs
Time: 05:18:10
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

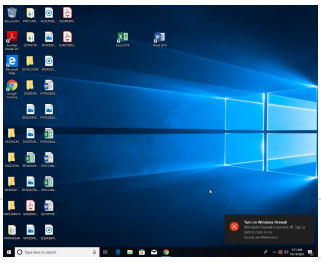
Windows Analysis Report Proforma Invoice.exe

Overview

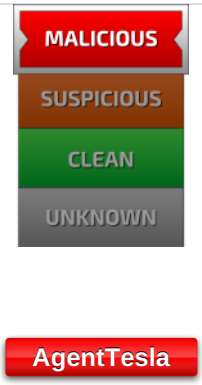
General Information

Sample Name:	Proforma Invoice.exe
Analysis ID:	502592
MD5:	dd00dde252a925..
SHA1:	44ca2aa75de6ca..
SHA256:	c0057025e69297..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

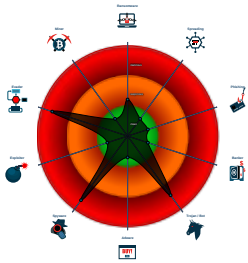


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Contains functionality to register a lo…
- Machine Learning detection for samp…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- Proforma Invoice.exe (PID: 6844 cmdline: 'C:\Users\user\Desktop\Proforma Invoice.exe' MD5: DD00DDE252A92512815C0D0D3679D1FD)
  - Proforma Invoice.exe (PID: 5608 cmdline: C:\Users\user\Desktop\Proforma Invoice.exe MD5: DD00DDE252A92512815C0D0D3679D1FD)
  - Proforma Invoice.exe (PID: 6804 cmdline: C:\Users\user\Desktop\Proforma Invoice.exe MD5: DD00DDE252A92512815C0D0D3679D1FD)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "kendakenda@karanex.com",
  "Password": "zarazita404",
  "Host": "webmail.karanex.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.560307423.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.560307423.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.309881173.00000000025A1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.310366268.00000000035A9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.310366268.00000000035A9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 6 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Proforma Invoice.exe.3846860.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Proforma Invoice.exe.3846860.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.Proforma Invoice.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.Proforma Invoice.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Proforma Invoice.exe.3846860.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

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

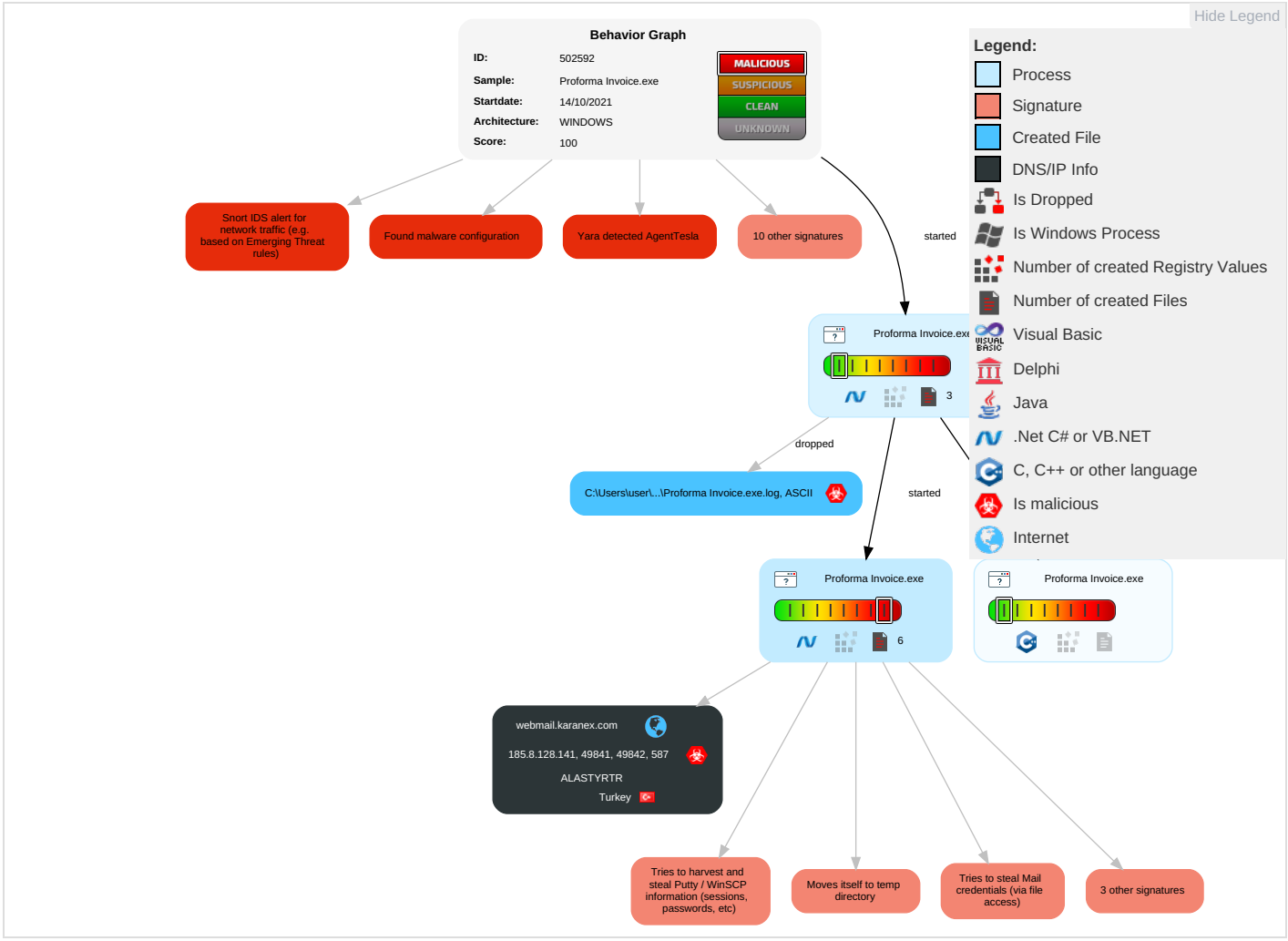
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1 1	OS Credential Dumping 2	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 2 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

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
Proforma Invoice.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Proforma Invoice.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
webmail.karanex.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://rafeBU.com	2%	Virustotal		Browse
http://rafeBU.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://webmail.karanex.com	1%	Virustotal		Browse
http://webmail.karanex.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://LqBkoD7aW7iu.org	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webmail.karanex.com	185.8.128.141	true	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.8.128.141	webmail.karanex.com	Turkey		3188	ALASTYRTR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502592
Start date:	14.10.2021
Start time:	05:18:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proforma Invoice.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:	21
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@5/2@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • 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
05:19:14	API Interceptor	748x Sleep call for process: Proforma Invoice.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.8.128.141	Invoice Lists.exe	Get hash	malicious	Browse	
	INV 20211012.exe	Get hash	malicious	Browse	
	October Final Order.exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	20211006 PO.exe	Get hash	malicious	Browse	
	New_Order_PO#96072380_MT_QuoteRFQ.exe	Get hash	malicious	Browse	
	PO 20213009.exe	Get hash	malicious	Browse	
	New_Order_PO#96072380_MT_QuoteMTO.exe	Get hash	malicious	Browse	
	New_Order_PO#960780_MT_Quote-MT-valve.exe	Get hash	malicious	Browse	
	New_Order_PO#960780_MT_Quote-MT-valve.exe	Get hash	malicious	Browse	
	New_Order_PO#960780_MT_Quote-MT.exe	Get hash	malicious	Browse	
	NEW ORDER.exe	Get hash	malicious	Browse	
	pDKtDOf1YMseKzN.exe	Get hash	malicious	Browse	
	New_Order_PO#960780_MT_Quote.exe	Get hash	malicious	Browse	
	New_Order_PO#960780_MT_Quote-MT-RFQ.exe	Get hash	malicious	Browse	
	9Jco42YF0nOEZbd.exe	Get hash	malicious	Browse	
	New_Order_PO#960780_MT_Quote-MT-RFQ.exe	Get hash	malicious	Browse	
	New_Order_PO#960780_MT_Quote-RFQ.exe	Get hash	malicious	Browse	
	New_Order_PO#960780_MT_Quote1678.exe	Get hash	malicious	Browse	
	#RFQ URGENT PO SAMPLE PRODUCT 09082021.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
webmail.karanex.com	Invoice Lists.exe	Get hash	malicious	Browse	• 185.8.128.141
	INV 20211012.exe	Get hash	malicious	Browse	• 185.8.128.141
	October Final Order.exe	Get hash	malicious	Browse	• 185.8.128.141
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 185.8.128.141
	20211006 PO.exe	Get hash	malicious	Browse	• 185.8.128.141
	RFQ-Quote-REF-HYODA KM-Request (R).exe	Get hash	malicious	Browse	• 185.8.128.141
	New_Order_PO#96072380_MT_QuoteRFQ.exe	Get hash	malicious	Browse	• 185.8.128.141
	PO 20213009.exe	Get hash	malicious	Browse	• 185.8.128.141
	Purchase Order NO202340.exe	Get hash	malicious	Browse	• 185.8.128.141
	NEW ORDER.exe	Get hash	malicious	Browse	• 185.8.128.141
	pDKtDOf1YMseKzN.exe	Get hash	malicious	Browse	• 185.8.128.141

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ALASTYRTR	Invoice Lists.exe	Get hash	malicious	Browse	• 185.8.128.141
	INV 20211012.exe	Get hash	malicious	Browse	• 185.8.128.141
	TEKL#U0130F TALEP RFQ_PDF.exe	Get hash	malicious	Browse	• 5.2.87.216
	October Final Order.exe	Get hash	malicious	Browse	• 185.8.128.141
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 185.8.128.141
	20211006 PO.exe	Get hash	malicious	Browse	• 185.8.128.141
	RESM#U0130 TEKL#U0130F VE F#U0130YAT TEK L#U0130F TALEB#U0130_PDF.exe	Get hash	malicious	Browse	• 5.2.87.216
	TEKL#U0130F TALEP VE #U00dcR#U00dcN #U00 d6ZELL#U0130KLER#U0130_PDF.exe	Get hash	malicious	Browse	• 5.2.87.216
	RESM#U0130 SATIN ALMA S#U0130PAR#U0130#U 015e#U0130_PDF.exe	Get hash	malicious	Browse	• 5.2.87.216
	New_Order_PO#96072380_MT_QuoteRFQ.exe	Get hash	malicious	Browse	• 185.8.128.141
	PO 20213009.exe	Get hash	malicious	Browse	• 185.8.128.141
	New_Order_PO#96072380_MT_QuoteMTO.exe	Get hash	malicious	Browse	• 185.8.128.141
	INVOICE.exe	Get hash	malicious	Browse	• 185.8.128.36
	Z#U0130RAAT BANKASI #U00d6DEME TAVS#U013 0YES#U0130_PDF.exe	Get hash	malicious	Browse	• 5.2.87.216
	New_Order_PO#960780_MT_Quote-MT-valve.exe	Get hash	malicious	Browse	• 185.8.128.141
	New_Order_PO#960780_MT_Quote-MT-valve.exe	Get hash	malicious	Browse	• 185.8.128.141
	New_Order_PO#960780_MT_Quote-MT.exe	Get hash	malicious	Browse	• 185.8.128.141
	NEW ORDER.exe	Get hash	malicious	Browse	• 185.8.128.141
	pDKtDOf1YMseKzN.exe	Get hash	malicious	Browse	• 185.8.128.141
	#U00d6DEME TAVS#U0130YES#U0130_PDF.exe	Get hash	malicious	Browse	• 5.2.87.216

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Proforma Invoice.exe.log

Process:	C:\Users\user\Desktop\Proforma Invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Proforma Invoice.exe.log	
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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.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

C:\Users\user\AppData\Roaming\ywwi1ck1.qnq\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Proforma Invoice.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.945284769091569
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Proforma Invoice.exe
File size:	368128
MD5:	dd00dde252a92512815c0d0d3679d1fd
SHA1:	44ca2aa75de6ca79ae39408b48cd605d384a9a9b
SHA256:	c0057025e69297714ba47f8fc982ec8fd8713f5a270a2d638257bcc395cad39f
SHA512:	1bb62ebaa9b13a7e6f97ce09d671c25f46a6f5383d9f0afde4b83d0284cf75408c404fe50d3eb8ed1b4ac7094fc781fec4b370c3bbb4693106c2c2616d2c9fe4
SSDEEP:	6144:K+7dXbJMkhB8krJuY9dUUlT7S6kTAzRZzJTON1AZkRGAY+w5SS6K4Wt+/y1Mt0cw:Kw+SBdQq0T7+8DFTODAZ/+dSP3k/y1M8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ga.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x45b3e6
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:	0x6167859B [Thu Oct 14 01:19:23 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	0x593ec	0x59400	False	0.957230939251	data	7.95675018012	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5c000	0x5a4	0x600	False	0.421875	data	4.07883026947	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5e000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/14/21-05:20:53.478836	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49841	587	192.168.2.3	185.8.128.141
10/14/21-05:20:55.450868	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49842	587	192.168.2.3	185.8.128.141

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 05:20:52.179286957 CEST	192.168.2.3	8.8.8.8	0x65b2	Standard query (0)	webmail.karanex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 05:20:52.264353991 CEST	8.8.8.8	192.168.2.3	0x65b2	No error (0)	webmail.karanex.com		185.8.128.141	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 14, 2021 05:20:53.105591059 CEST	587	49841	185.8.128.141	192.168.2.3	220-feronia.alastyr.com ESMTP Exim 4.94.2 #2 Thu, 14 Oct 2021 06:20:51 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Oct 14, 2021 05:20:53.106681108 CEST	49841	587	192.168.2.3	185.8.128.141	EHLO 899552
Oct 14, 2021 05:20:53.163875103 CEST	587	49841	185.8.128.141	192.168.2.3	250-feronia.alastyr.com Hello 899552 [102.129.143.33] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Oct 14, 2021 05:20:53.165122032 CEST	49841	587	192.168.2.3	185.8.128.141	AUTH login a2VuZGFrZW5kYUBrYXJhbmV4LmNvbQ==
Oct 14, 2021 05:20:53.222656012 CEST	587	49841	185.8.128.141	192.168.2.3	334 UGFzc3dvcmQ6
Oct 14, 2021 05:20:53.301810980 CEST	587	49841	185.8.128.141	192.168.2.3	235 Authentication succeeded
Oct 14, 2021 05:20:53.302635908 CEST	49841	587	192.168.2.3	185.8.128.141	MAIL FROM:<kendakenda@karanex.com>
Oct 14, 2021 05:20:53.359736919 CEST	587	49841	185.8.128.141	192.168.2.3	250 OK
Oct 14, 2021 05:20:53.360028028 CEST	49841	587	192.168.2.3	185.8.128.141	RCPT TO:<kendakenda@karanex.com>
Oct 14, 2021 05:20:53.420150995 CEST	587	49841	185.8.128.141	192.168.2.3	250 Accepted
Oct 14, 2021 05:20:53.420588017 CEST	49841	587	192.168.2.3	185.8.128.141	DATA
Oct 14, 2021 05:20:53.477816105 CEST	587	49841	185.8.128.141	192.168.2.3	354 Enter message, ending with "." on a line by itself
Oct 14, 2021 05:20:53.479703903 CEST	49841	587	192.168.2.3	185.8.128.141	.
Oct 14, 2021 05:20:53.542679071 CEST	587	49841	185.8.128.141	192.168.2.3	250 OK id=1marIa-008l8N-7s
Oct 14, 2021 05:20:54.913331032 CEST	49841	587	192.168.2.3	185.8.128.141	QUIT
Oct 14, 2021 05:20:54.971801043 CEST	587	49841	185.8.128.141	192.168.2.3	221 feronia.alastyr.com closing connection
Oct 14, 2021 05:20:55.091969967 CEST	587	49842	185.8.128.141	192.168.2.3	220-feronia.alastyr.com ESMTP Exim 4.94.2 #2 Thu, 14 Oct 2021 06:20:53 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Oct 14, 2021 05:20:55.092401028 CEST	49842	587	192.168.2.3	185.8.128.141	EHLO 899552
Oct 14, 2021 05:20:55.149497986 CEST	587	49842	185.8.128.141	192.168.2.3	250-feronia.alastyr.com Hello 899552 [102.129.143.33] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Oct 14, 2021 05:20:55.150111914 CEST	49842	587	192.168.2.3	185.8.128.141	AUTH login a2VuZGFrZW5kYUBrYXJhbmV4LmNvbQ==
Oct 14, 2021 05:20:55.207438946 CEST	587	49842	185.8.128.141	192.168.2.3	334 UGFzc3dvcmQ6
Oct 14, 2021 05:20:55.271754026 CEST	587	49842	185.8.128.141	192.168.2.3	235 Authentication succeeded
Oct 14, 2021 05:20:55.272250891 CEST	49842	587	192.168.2.3	185.8.128.141	MAIL FROM:<kendakenda@karanex.com>
Oct 14, 2021 05:20:55.329298973 CEST	587	49842	185.8.128.141	192.168.2.3	250 OK
Oct 14, 2021 05:20:55.330032110 CEST	49842	587	192.168.2.3	185.8.128.141	RCPT TO:<kendakenda@karanex.com>
Oct 14, 2021 05:20:55.390760899 CEST	587	49842	185.8.128.141	192.168.2.3	250 Accepted
Oct 14, 2021 05:20:55.391385078 CEST	49842	587	192.168.2.3	185.8.128.141	DATA
Oct 14, 2021 05:20:55.448453903 CEST	587	49842	185.8.128.141	192.168.2.3	354 Enter message, ending with "." on a line by itself
Oct 14, 2021 05:20:55.451704025 CEST	49842	587	192.168.2.3	185.8.128.141	.
Oct 14, 2021 05:20:55.512649059 CEST	587	49842	185.8.128.141	192.168.2.3	250 OK id=1marIc-008l8c-6v

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Proforma Invoice.exe PID: 6844 Parent PID: 3796

General

Start time:	05:19:08
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Proforma Invoice.exe'
Imagebase:	0x2a0000
File size:	368128 bytes
MD5 hash:	DD00DDE252A92512815C0D0D3679D1FD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.309881173.00000000025A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.310366268.00000000035A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.310366268.00000000035A9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Proforma Invoice.exe PID: 5608 Parent PID: 6844

General

Start time:	05:19:14
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Proforma Invoice.exe
Imagebase:	0x2e0000
File size:	368128 bytes

MD5 hash:	DD00DDE252A92512815C0D0D3679D1FD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Proforma Invoice.exe PID: 6804 Parent PID: 6844

General

Start time:	05:19:15
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Proforma Invoice.exe
Imagebase:	0xb20000
File size:	368128 bytes
MD5 hash:	DD00DDE252A92512815C0D0D3679D1FD
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: 00000004.00000002.560307423.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.560307423.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.562365344.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.562365344.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis