ID: 491978
Sample Name: Proforma Invoice.exe
Cookbook: default.jbs
Time: 08:38:14
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

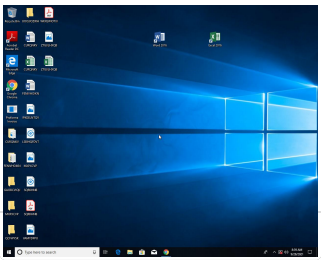
Windows Analysis Report Proforma Invoice.exe

Overview

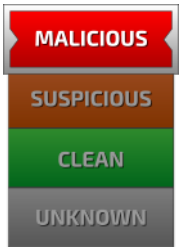
General Information

Sample Name:	Proforma Invoice.exe
Analysis ID:	491978
MD5:	05dea597f5e2fda..
SHA1:	6067e82bf295eb7.
SHA256:	6e6d502d455f4d1.
Tags:	exe Invoice
Infos:	

Most interesting Screenshot:



Detection

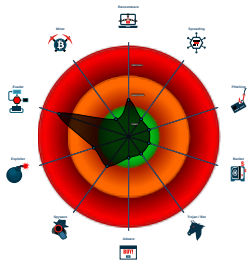


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Initial sample is a PE file and has a …
- .NET source code contains very larg…
- Executable has a suspicious name (…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Uses 32bit PE files
- Found inlined nop instructions (likely…
- Queries the volume information (nam…
- Sample file is different than original …
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (

Classification



Process Tree

- **System is w10x64**
- Proforma Invoice.exe (PID: 6612 cmdline: 'C:\Users\user\Desktop\Proforma Invoice.exe' MD5: 05DEA597F5E2FDAF7DD91DC2732EB54B)
  - Proforma Invoice.exe (PID: 6752 cmdline: C:\Users\user\Desktop\Proforma Invoice.exe MD5: 05DEA597F5E2FDAF7DD91DC2732EB54B)
  - Proforma Invoice.exe (PID: 6804 cmdline: C:\Users\user\Desktop\Proforma Invoice.exe MD5: 05DEA597F5E2FDAF7DD91DC2732EB54B)
  - Proforma Invoice.exe (PID: 6812 cmdline: C:\Users\user\Desktop\Proforma Invoice.exe MD5: 05DEA597F5E2FDAF7DD91DC2732EB54B)
  - Proforma Invoice.exe (PID: 6820 cmdline: C:\Users\user\Desktop\Proforma Invoice.exe MD5: 05DEA597F5E2FDAF7DD91DC2732EB54B)
  - Proforma Invoice.exe (PID: 6832 cmdline: C:\Users\user\Desktop\Proforma Invoice.exe MD5: 05DEA597F5E2FDAF7DD91DC2732EB54B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.384187519.0000000002D41000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.384252504.0000000002D84000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: Proforma Invoice.exe PID: 6612	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Proforma Invoice.exe.2d8482c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large strings

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

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

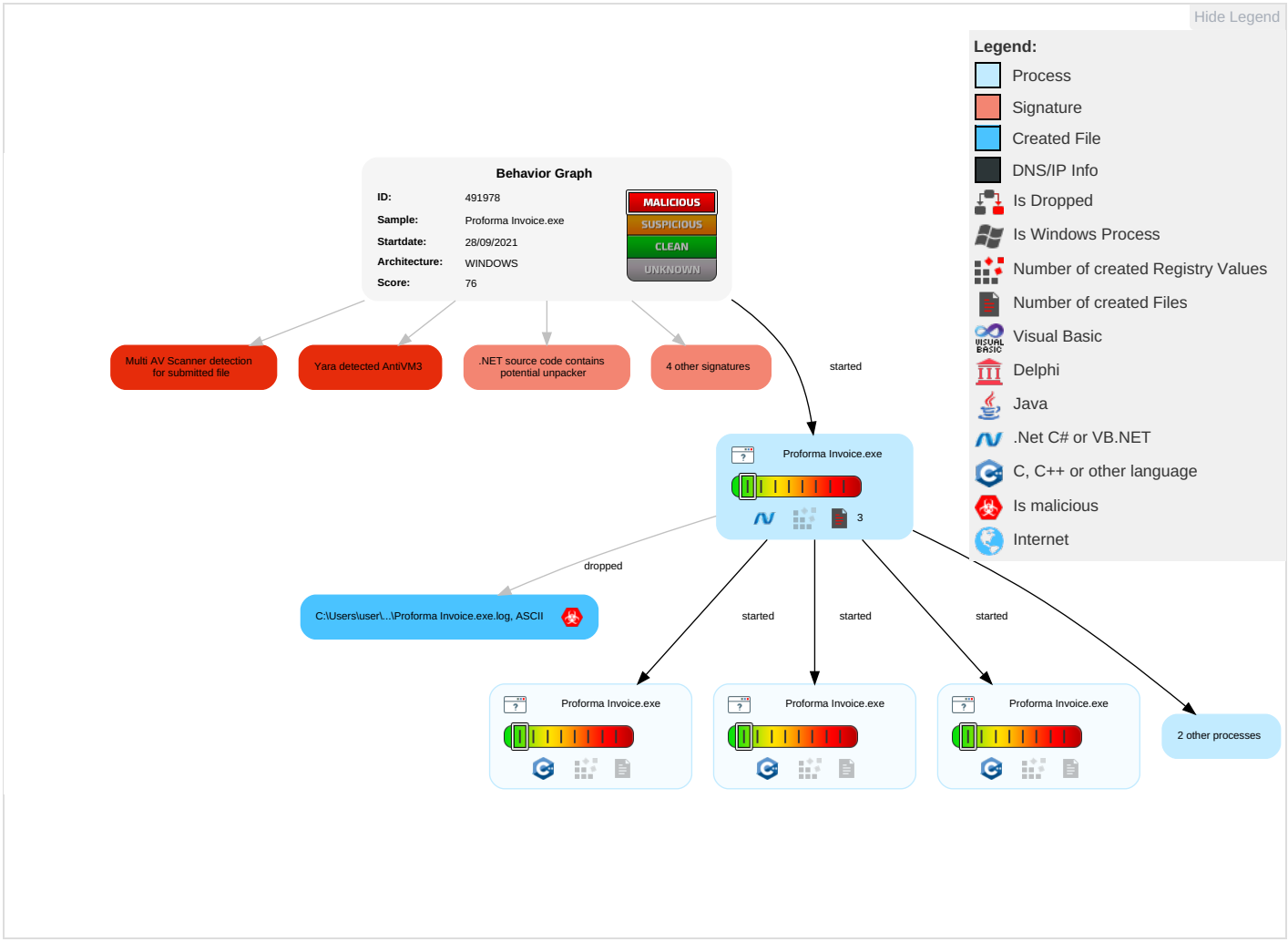
Yara detected AntiVM3

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	System Information Discovery 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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	19%	Virustotal		Browse
Proforma Invoice.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.m	0%	URL Reputation	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:	33.0.0 White Diamond
Analysis ID:	491978
Start date:	28.09.2021
Start time:	08:38:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 33s
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:	12
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:	mal76.evad.winEXE@11/1@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • 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 • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:39:15	API Interceptor	1x Sleep call for process: Proforma Invoice.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\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
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.4740779345585215

General

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:	Proforma Invoice.exe
File size:	420352
MD5:	05dea597f5e2fdaf7dd91dc2732eb54b
SHA1:	6067e82bf295eb76c415a5c4910ea578bae96933
SHA256:	6e6d502d455f4d1db45f465ff69d1d2f53a78afffbda8e6bc2b12c99ca012926
SHA512:	35d0436a5154a7b9b44b56a9f8cba583cea20a66c9149a54751f55a18bc4f75cb4467c64ef2636c395c6425aad00815a1c4c97522031574bd947e7e8410a5d31
SSDEEP:	6144:iubE9UmzhN23zG8KGBAOq+hKqr7tGUAI/njChopL3Woqz2ss1SJMllo:azhYz/Ni+hBr7IUAILVzAsvlo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...,.Ra.....0..^.....y... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4679ae
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:	0x6152A12C [Tue Sep 28 04:59:24 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	0x65dbc	0x65e00	False	0.595688746166	data	6.49089350535	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x68000	0x644	0x800	False	0.34619140625	data	3.51671275132	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6a000	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

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Proforma Invoice.exe PID: 6612 Parent PID: 3876

General

Start time:	08:39:12
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Proforma Invoice.exe'
Imagebase:	0x990000
File size:	420352 bytes
MD5 hash:	05DEA597F5E2FDAF7DD91DC2732EB54B
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: 00000001.00000002.384187519.0000000002D41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.384252504.0000000002D84000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Proforma Invoice.exe PID: 6752 Parent PID: 6612

General

Start time:	08:39:16
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Proforma Invoice.exe
Imagebase:	0x130000
File size:	420352 bytes
MD5 hash:	05DEA597F5E2FDAF7DD91DC2732EB54B
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: 6612

General

Start time:	08:39:16
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Proforma Invoice.exe
Imagebase:	0x80000
File size:	420352 bytes
MD5 hash:	05DEA597F5E2FDAF7DD91DC2732EB54B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Proforma Invoice.exe PID: 6812 Parent PID: 6612

General

Start time:	08:39:17
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Proforma Invoice.exe
Imagebase:	0x9a0000
File size:	420352 bytes
MD5 hash:	05DEA597F5E2FDAF7DD91DC2732EB54B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Proforma Invoice.exe PID: 6820 Parent PID: 6612

General

Start time:	08:39:20
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Proforma Invoice.exe
Imagebase:	0xcb0000
File size:	420352 bytes
MD5 hash:	05DEA597F5E2FDAF7DD91DC2732EB54B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Proforma Invoice.exe PID: 6832 Parent PID: 6612

General

Start time:	08:39:25
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Proforma Invoice.exe
Imagebase:	0x2b0000
File size:	420352 bytes
MD5 hash:	05DEA597F5E2FDAF7DD91DC2732EB54B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis