ID: 605000
Sample Name: Proforma Inv.exe
Cookbook: default.jbs
Time: 17:20:10
Date: 07/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

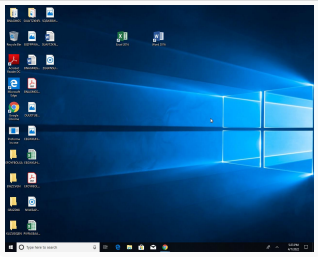
Windows Analysis Report

Proforma Inv.exe

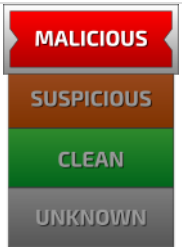
Overview

General Information

Sample Name:	Proforma Inv.exe
Analysis ID:	605000
MD5:	189ad2733ba3c8..
SHA1:	90d2762579dfd9..
SHA256:	d73763f8b8d4eb..
Tags:	agenttesla exe
Infos:	



Detection



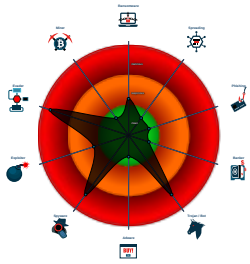
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- Proforma Inv.exe (PID: 6872 cmdline: "C:\Users\user\Desktop\Proforma Inv.exe" MD5: 189AD2733BA3C8BAA0D9FB41E4223D92)
  - Proforma Inv.exe (PID: 7096 cmdline: {path} MD5: 189AD2733BA3C8BAA0D9FB41E4223D92)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "ipdepartment@safalaw.com.ph",
  "Password": "#Risel767",
  "Host": "mail.safalaw.com.ph"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.508474036.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.508474036.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000000.262797800.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.262797800.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.263643345.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Proforma Inv.exe.3dff630.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Proforma Inv.exe.3dff630.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Proforma Inv.exe.3dff630.2.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30d32:$s10: logins • 0x30799:$s11: credential • 0x2cd78:$g1: get_Clipboard • 0x2cd86:$g2: get_Keyboard • 0x2cd93:$g3: get_Password • 0x2e074:$g4: get_CtrlKeyDown • 0x2e084:$g5: get_ShiftKeyDown • 0x2e095:$g6: get_AltKeyDown
2.0.Proforma Inv.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.0.Proforma Inv.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

.NET source code contains very large strings

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)

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)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

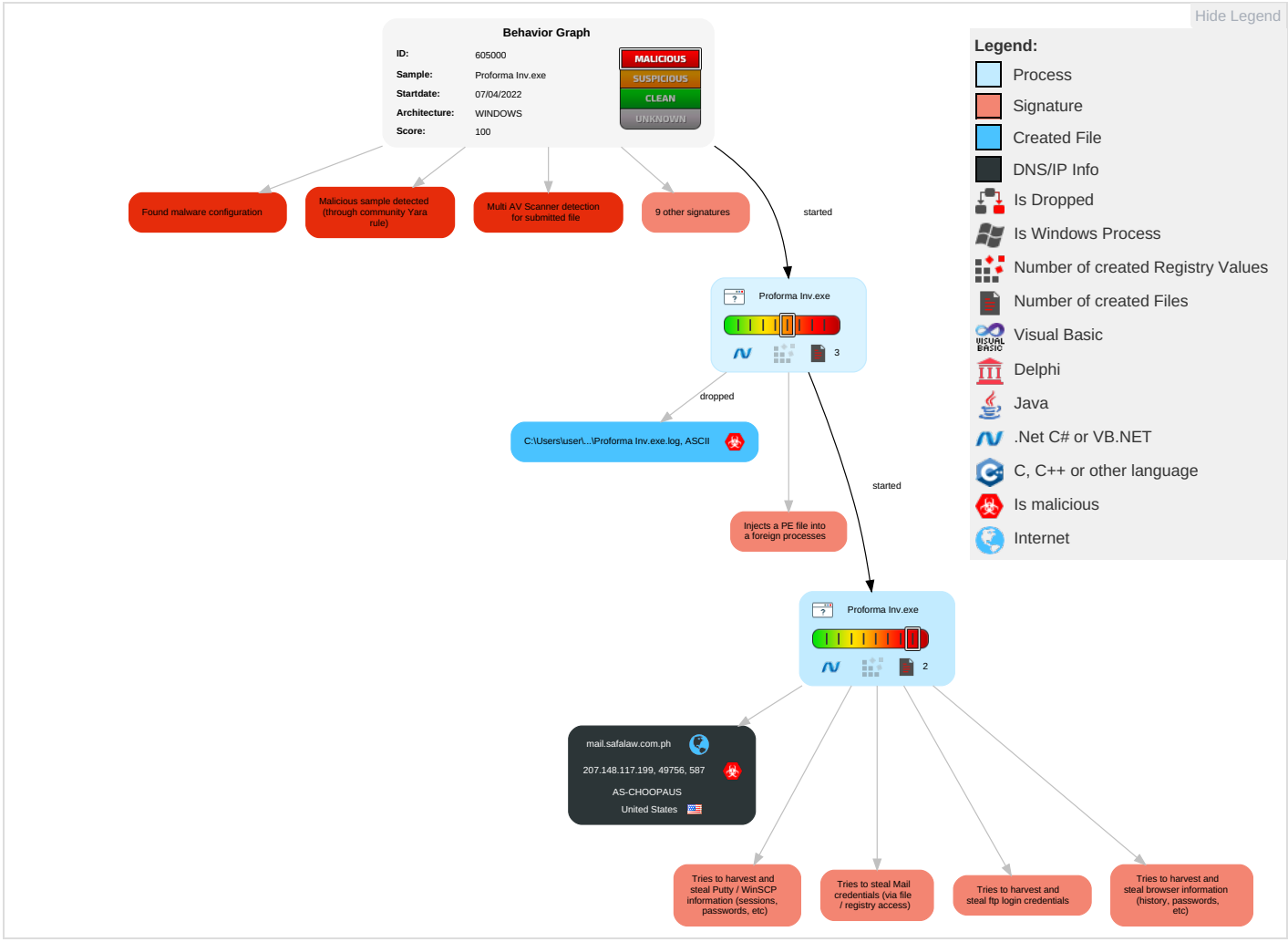
Remote Access Functionality

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

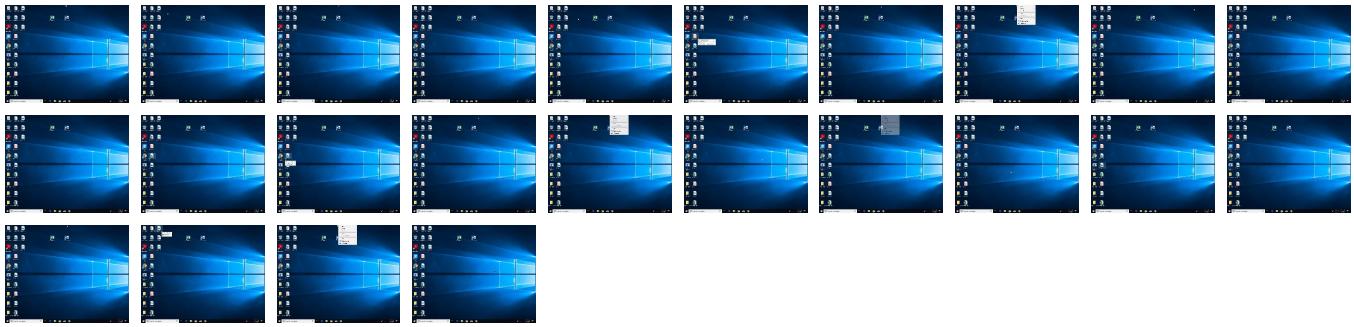
Behavior Graph



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 Inv.exe	33%	Virustotal		Browse
Proforma Inv.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.Proforma Inv.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Proforma Inv.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Proforma Inv.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Proforma Inv.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Proforma Inv.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.Proforma Inv.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://XudLs2COBNu.org1-5-21-3853321935-2125563209-4053062332-1002_Classes	0%	Avira URL Cloud	safe	
http://XudLs2COBNu.org	0%	Avira URL Cloud	safe	
http://www.fonts.comoth	0%	Avira URL Cloud	safe	
http://www.urwpp.deFv	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.krights	0%	Avira URL Cloud	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.fonts.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cny	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.founder.com.cn/cnudi	0%	Avira URL Cloud	safe	
http://www.fontbureau.comab	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comalic#	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/e(	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sandoll.co.krnta~	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comh	0%	Avira URL Cloud	safe	
http://WaIJyp.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.sajatypeworks.coms	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-ru	0%	Avira URL Cloud	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://mail.safalaw.com.ph	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasvi	0%	Avira URL Cloud	safe	
http://www.fontbureau.comL.TTF	0%	URL Reputation	safe	
http://www.sandoll.co.kre	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.comKfC	0%	Avira URL Cloud	safe	
http://www.tiro.comcom	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comcomF	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comionFt	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comitua	0%	Avira URL Cloud	safe	
http://www.fonts.comCH	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.safalaw.com.ph	207.148.117.199	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Proforma Inv.exe, 00000002.00000002.5100 96392.0000000002AC1000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://XudLs2COBNu.org1-5-21-3853321935-2125563209-4053062332-1002_Classes	Proforma Inv.exe, 00000002.00000003.2795 61854.0000000000C84000.00000004.00000020 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://XudLs2COBNu.org	Proforma Inv.exe, 00000002.00000002.5108 27489.0000000002E33000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comoth	Proforma Inv.exe, 00000000.00000003.2428 63799.0000000005DAB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deFv	Proforma Inv.exe, 00000000.00000003.2498 77134.0000000005D99000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krights	Proforma Inv.exe, 00000000.00000003.2439 05944.0000000005D96000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comic	Proforma Inv.exe, 00000000.00000003.2429 19450.0000000005DAB000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242891447.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cny	Proforma Inv.exe, 00000000.00000003.2445 37632.0000000005D94000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

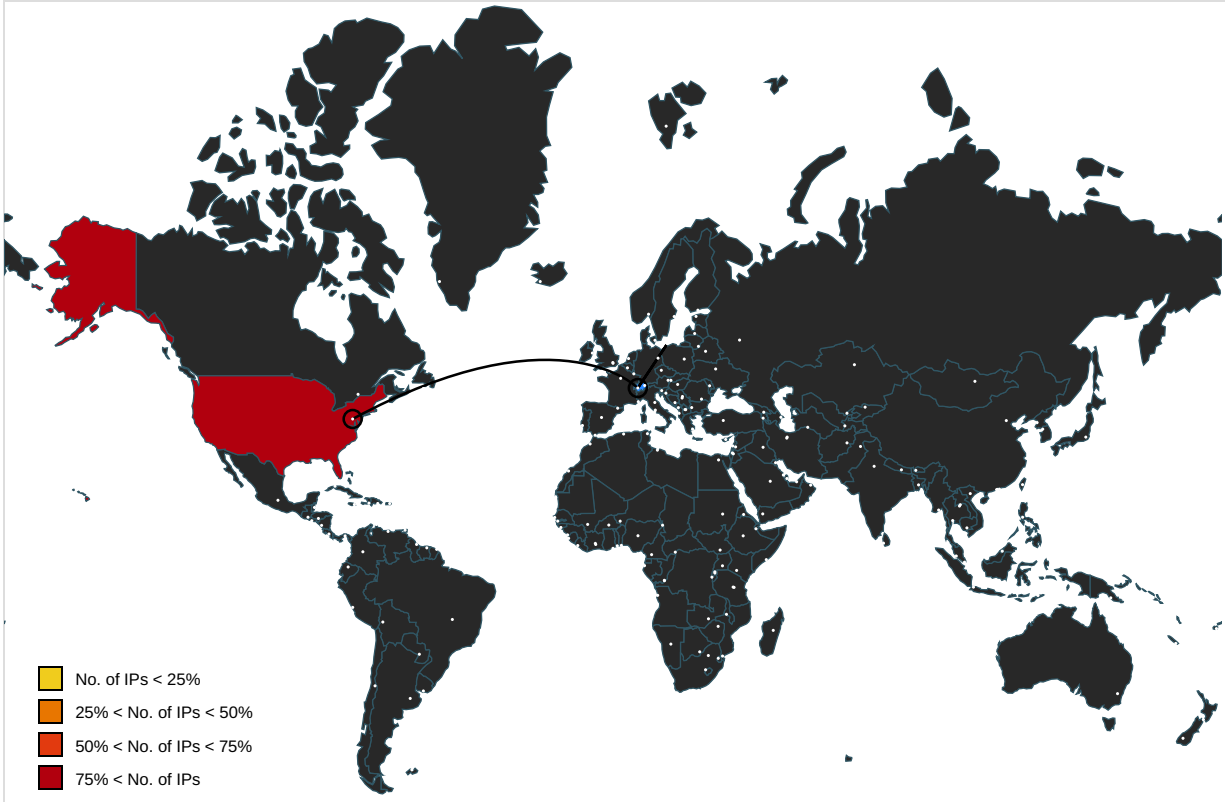
Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	Proforma Inv.exe, 00000002.00000002.5100 96392.0000000002AC1000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnudi	Proforma Inv.exe, 00000000.00000003.2447 88585.0000000005D94000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.244537632.000000000 5D94000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comab	Proforma Inv.exe, 00000000.00000003.2491 67454.0000000005D99000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn	Proforma Inv.exe, 00000000.00000003.2428 91447.0000000005DAB000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalic#	Proforma Inv.exe, 00000000.00000003.2498 77134.0000000005D99000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Proforma Inv.exe, 00000000.00000003.2428 44157.0000000005DAB000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242863799.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00002.279381567.0000000006FA2000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242891447.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.sandoll.co.kr	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/e(	Proforma Inv.exe, 00000000.00000003.2447 88585.0000000005D94000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	Proforma Inv.exe, 00000000.00000003.2498 77134.0000000005D99000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krnta~	Proforma Inv.exe, 00000000.00000003.2439 05944.0000000005D96000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.comh	Proforma Inv.exe, 00000000.00000003.2426 56361.0000000005DAB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://WaIJyp.com	Proforma Inv.exe, 00000002.00000002.5100 96392.0000000002AC1000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com=	Proforma Inv.exe, 00000000.00000003.2491 67454.0000000005D99000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Proforma Inv.exe, 00000000.00000002.2789 40493.0000000005D90000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.249877134.000000000 5D99000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00002.279381567.0000000006FA2000.0000000 4.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	Proforma Inv.exe, 00000000.00000003.2491 67454.0000000005D99000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	Proforma Inv.exe, 00000002.00000002.5107 35000.0000000002E0F000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.coms	Proforma Inv.exe, 00000000.00000003.2428 80391.0000000005DB4000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242844157.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242766852.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242698082.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242656361.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242798809.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242863799.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242819494.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242737289.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	Proforma Inv.exe, 00000002.00000002.5100 96392.0000000002AC1000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnu-ru	Proforma Inv.exe, 00000000.00000003.2445 17298.0000000005DCD000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comion	Proforma Inv.exe, 00000000.00000003.2491 67454.0000000005D99000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.safalaw.com.ph	Proforma Inv.exe, 00000002.00000002.5107 35000.0000000002E0F000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comasvi	Proforma Inv.exe, 00000000.00000003.2493 93177.0000000005D9A000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.249167454.000000000 5D99000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.248778008.0000000005D98000.0000000 4.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comL.TTF	Proforma Inv.exe, 00000000.00000003.2493 93177.0000000005D9A000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.249167454.000000000 5D99000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kre	Proforma Inv.exe, 00000000.00000003.2439 05944.0000000005D96000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	Proforma Inv.exe, 00000000.00000003.2491 67454.0000000005D99000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.248778008.000000000 5D98000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	Proforma Inv.exe, 00000000.00000003.2491 67454.0000000005D99000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://en.w	Proforma Inv.exe, 00000000.00000003.2428 80391.0000000005DB4000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242844157.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242766852.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242698082.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242656361.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242798809.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242392348.000000000145D000.0000000 4.00000020.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242863799.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242819494.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242737289.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comKfC	Proforma Inv.exe, 00000000.00000003.2428 44157.0000000005DAB000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242766852.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242698082.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242656361.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242798809.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242919450.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242863799.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242819494.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.242891447.0000000005DAB000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242737289.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comcom	Proforma Inv.exe, 00000000.00000003.2432 18227.0000000005DAB000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.243198712.000000000 5DAB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Proforma Inv.exe, 00000000.00000003.2447 88585.0000000005D94000.00000004.00000800 .00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.246769169.000000000 5D9D000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00002.279381567.0000000006FA2000.0000000 4.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.244537632.000000000 5D94000.00000004.00000800.00020000.00000 000.sdmp, Proforma Inv.exe, 00000000.000 00003.244899824.0000000005D9B000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Proforma Inv.exe, 00000000.00000002.2793 81567.0000000006FA2000.00000004.00000800 .00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.html	Proforma Inv.exe, 00000000.00000003.249428709.0000000005DC5000.00000004.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.249449455.0000000005DC5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comcomF	Proforma Inv.exe, 00000000.00000003.249393177.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.249167454.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comt	Proforma Inv.exe, 00000000.00000003.249877134.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Proforma Inv.exe, 00000000.00000002.279381567.0000000006FA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Proforma Inv.exe, 00000000.00000002.279381567.0000000006FA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comionFt	Proforma Inv.exe, 00000000.00000002.278940493.0000000005D90000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comals	Proforma Inv.exe, 00000000.00000003.249877134.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comitua	Proforma Inv.exe, 00000000.00000003.249877134.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comCH	Proforma Inv.exe, 00000000.00000003.242844157.0000000005DAB000.00000004.00000800.00020000.00000000.sdmp, Proforma Inv.exe, 00000000.00000003.242863799.0000000005DAB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.117.199	mail.safalaw.com.ph	United States		20473	AS-CHOOPAUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	605000
Start date and time:	2022-04-07 15:20:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proforma Inv.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@3/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:21:17	API Interceptor	790x Sleep call for process: Proforma Inv.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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 Inv.exe.log

Process:	C:\Users\user\Desktop\Proforma Inv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.85181290405052
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% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Proforma Inv.exe
File size:	444928
MD5:	189ad2733ba3c8baa0d9fb41e4223d92
SHA1:	90d2762579dfd97d7b767662566f3a623766dd0a
SHA256:	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b
SHA512:	a255eb116180e54ca4966b6596adccffb56deac442f64ed570814f2205811b3e5d2263ce4f0f2183851530b962f754fe3fe3561dda93dd3e20f6ac46dc6f0901
SSDEEP:	12288:wJrxvRItNiL65tIekTAEr4xwWEL9KHHvxosMKnd:8fsiL65t7kT1rjhKHH5os
TLSH:	2694DFA05A162183D2906F72C0E3CCB03AE5B1DA9259F7DEBC84DB543FE5198C644BBD

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....Nb.............P............v.... ....@.. ....@...............................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46de76
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:	0x624ECABA [Thu Apr 7 11:27:54 2022 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6de24	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6e000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x70000	0xc	.reloc
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6be7c	0x6c000	False	0.901538990162	data	7.86044321518	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x5b4	0x600	False	0.427734375	data	4.12184998186	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x6e090	0x324	data		
RT_MANIFEST	0x6e3c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

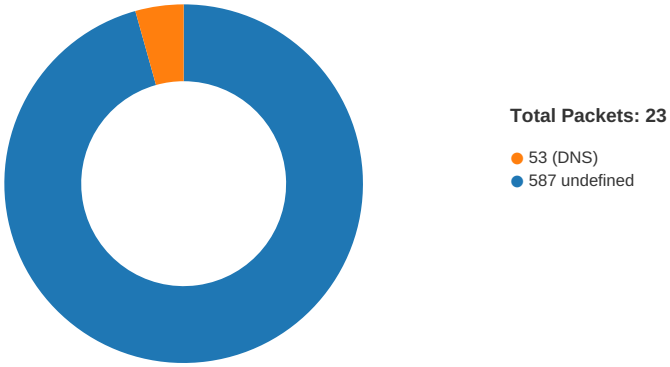
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	HEhUz.exe
FileVersion	1.0.0.0

Description	Data
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	Daily Notes
ProductVersion	1.0.0.0
FileDescription	Daily Notes
OriginalFilename	HEhUz.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2022 17:21:35.132299900 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:35.378325939 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:35.378420115 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:35.700582981 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:35.700885057 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:35.946814060 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:35.952491999 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:36.198868990 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:36.275157928 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:36.525212049 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:36.525239944 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:36.525254965 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:36.525265932 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:36.525348902 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:36.525912046 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:36.570353985 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:36.816478014 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:36.903961897 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:37.083776951 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:37.329756975 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:37.330904961 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:37.577114105 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:37.577652931 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:37.831244946 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:37.832106113 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:38.077944040 CEST	587	49756	207.148.117.199	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2022 17:21:38.078320026 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:38.325915098 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:38.326359034 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:38.572231054 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:38.573324919 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:38.573427916 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:38.574114084 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:38.574244022 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:21:38.819161892 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:38.819189072 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:38.819694042 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:38.819741011 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:39.898117065 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:21:40.113773108 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:23:14.007035017 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:23:14.293694973 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:23:14.816061020 CEST	587	49756	207.148.117.199	192.168.2.3
Apr 7, 2022 17:23:14.881441116 CEST	49756	587	192.168.2.3	207.148.117.199
Apr 7, 2022 17:23:14.908955097 CEST	49756	587	192.168.2.3	207.148.117.199

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2022 17:21:34.419188976 CEST	49327	53	192.168.2.3	8.8.8.8
Apr 7, 2022 17:21:35.039096117 CEST	53	49327	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2022 17:21:34.419188976 CEST	192.168.2.3	8.8.8.8	0xbb23	Standard query (0)	mail.safalaw.com.ph	A (IP address)	IN (0x0001)

DNS Answers

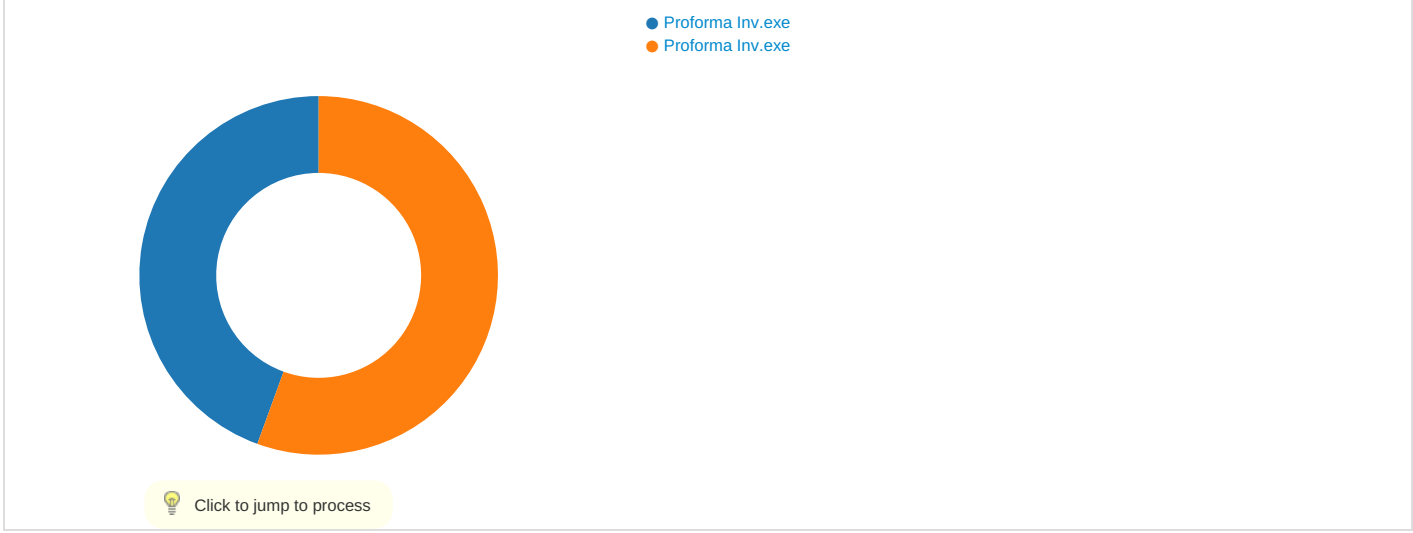
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2022 17:21:35.039096117 CEST	8.8.8.8	192.168.2.3	0xbb23	No error (0)	mail.safalaw.com.ph		207.148.117.199	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 7, 2022 17:21:35.700582981 CEST	587	49756	207.148.117.199	192.168.2.3	220-s482.sgp9.mysecurecloudhost.com ESMTP Exim 4.95 #2 Thu, 07 Apr 2022 15:21:35 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 7, 2022 17:21:35.700885057 CEST	49756	587	192.168.2.3	207.148.117.199	EHLO 688098
Apr 7, 2022 17:21:35.946814060 CEST	587	49756	207.148.117.199	192.168.2.3	250-s482.sgp9.mysecurecloudhost.com Hello 688098 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Apr 7, 2022 17:21:35.952491999 CEST	49756	587	192.168.2.3	207.148.117.199	STARTTLS
Apr 7, 2022 17:21:36.198868990 CEST	587	49756	207.148.117.199	192.168.2.3	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: Proforma Inv.exe PID: **6872**, Parent PID: **1668**

General

Target ID:	0
Start time:	17:21:09
Start date:	07/04/2022
Path:	C:\Users\user\Desktop\Proforma Inv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Proforma Inv.exe"
Imagebase:	0x960000
File size:	444928 bytes
MD5 hash:	189AD2733BA3C8BAA0D9FB41E4223D92
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: 00000000.00000002.272478585.0000000003D09000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.272478585.0000000003D09000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCBCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Proforma Inv.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFCC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Proforma Inv.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DFCC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB01B4F	ReadFile

Analysis Process: Proforma Inv.exe PID: **7096**, Parent PID: **6872**

General

Target ID:	2
Start time:	17:21:19
Start date:	07/04/2022
Path:	C:\Users\user\Desktop\Proforma Inv.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x680000
File size:	444928 bytes
MD5 hash:	189AD2733BA3C8BAA0D9FB41E4223D92
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: 00000002.00000002.508474036.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.508474036.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.262797800.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.262797800.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.263643345.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.263643345.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.262428568.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.262428568.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.263201971.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.263201971.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.510096392.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.510096392.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCBCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB01B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB01B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CB01B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6CB01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CB01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CB01B4F	ReadFile

Disassembly

No disassembly