ID: 358190
Sample Name: invoice.pdf.exe
Cookbook: default.jbs
Time: 07:44:45
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

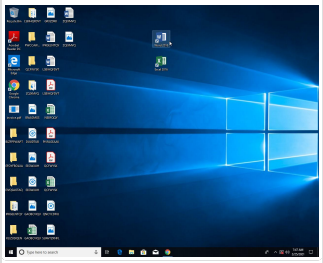
Analysis Report invoice.pdf.exe

Overview

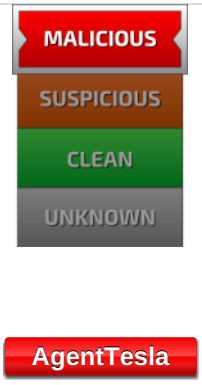
General Information

Sample Name:	invoice.pdf.exe
Analysis ID:	358190
MD5:	d3bb643f07aee4c.
SHA1:	a5804c4525cb33..
SHA256:	4e49cd4c9abc7a...
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



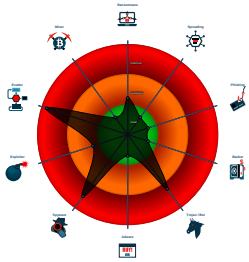
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- .NET source code contains very larg…
- Executable has a suspicious name (…
- Found evasive API chain (trying to d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- invoice.pdf.exe (PID: 6496 cmdline: 'C:\Users\user\Desktop\invoice.pdf.exe' MD5: D3BB643F07AEE4CC6BE3D303222BD2C9)
  - invoice.pdf.exe (PID: 6580 cmdline: C:\Users\user\Desktop\invoice.pdf.exe MD5: D3BB643F07AEE4CC6BE3D303222BD2C9)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "nasir@com-cept.comkhan@980.pkmail.com-cept.comlight@redwevamaldives.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.241020858.000000000370 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.240792649.000000000270 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.506799805.00000000036A 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.506799805.00000000036A 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000002.508855968.0000000003B2 E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 5 entries

Unpacked PEs

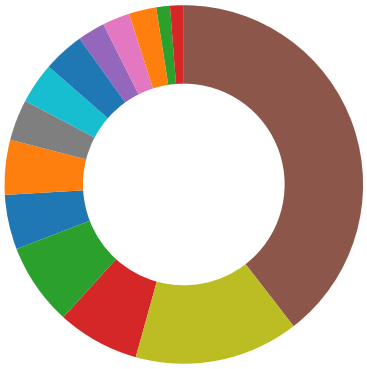
Source	Rule	Description	Author	Strings
1.2.invoice.pdf.exe.39bf710.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.invoice.pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.invoice.pdf.exe.39bf710.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.invoice.pdf.exe.27287c8.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
1.2.invoice.pdf.exe.38c2460.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

.NET source code contains very large strings

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

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM_3

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

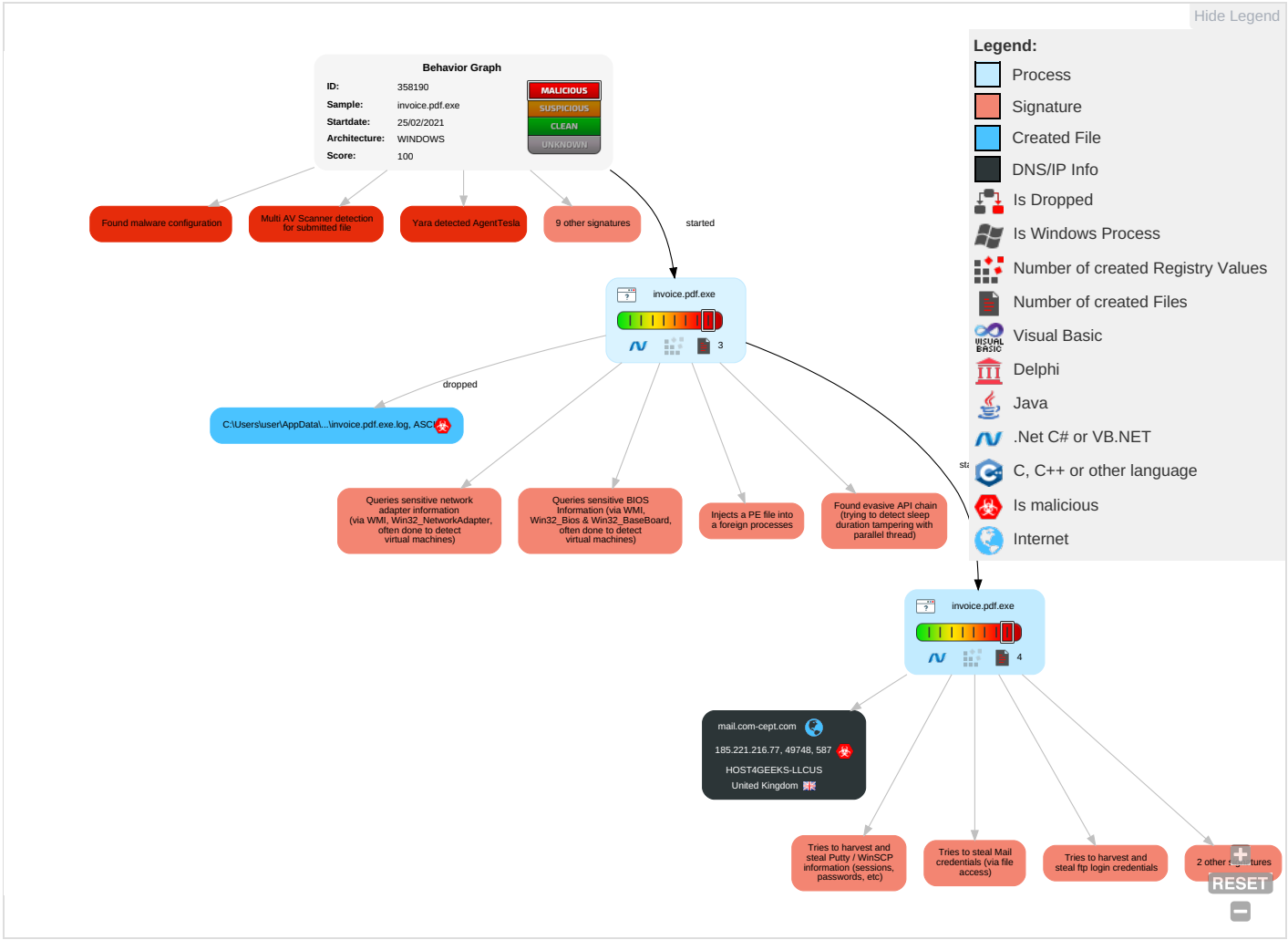
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress To Transfer 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Obfuscated Files or Information 1 3 1	Credentials in Registry 1	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Stand Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Virtualization/Sandbox Evasion 1 3	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Application Layer Protocol 2

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protc

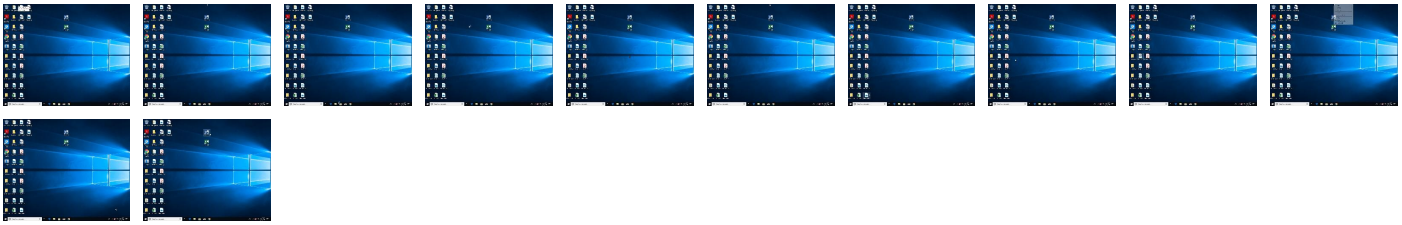
Behavior Graph



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
invoice.pdf.exe	34%	Virustotal		Browse
invoice.pdf.exe	21%	ReversingLabs	Win32.Trojan.Wacatac	
invoice.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.invoice.pdf.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.carterandcone.comechP	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/eO	0%	Avira URL Cloud	safe	
http://www.carterandcone.comeac	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTFnO	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/nO	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/tN	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/-OQ	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comAO	0%	Avira URL Cloud	safe	
http://HtsCZk.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.carterandcone.comext	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	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://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.fontbureau.comgrita$OX	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.fontbureau.comdiaoJO	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/JO	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0anSO7	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.carterandcone.comati	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://https://MFtHNrHfTnJ.net	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/JO	0%	Avira URL Cloud	safe	
http://www.gagalive.kr/livechat1.swf?chatroom=inchat-	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/on	0%	Avira URL Cloud	safe	
http://www.fontbureau.comeO	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6OJ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.com-cept.com	185.221.216.77	true	true		unknown

URLs from Memory and Binaries

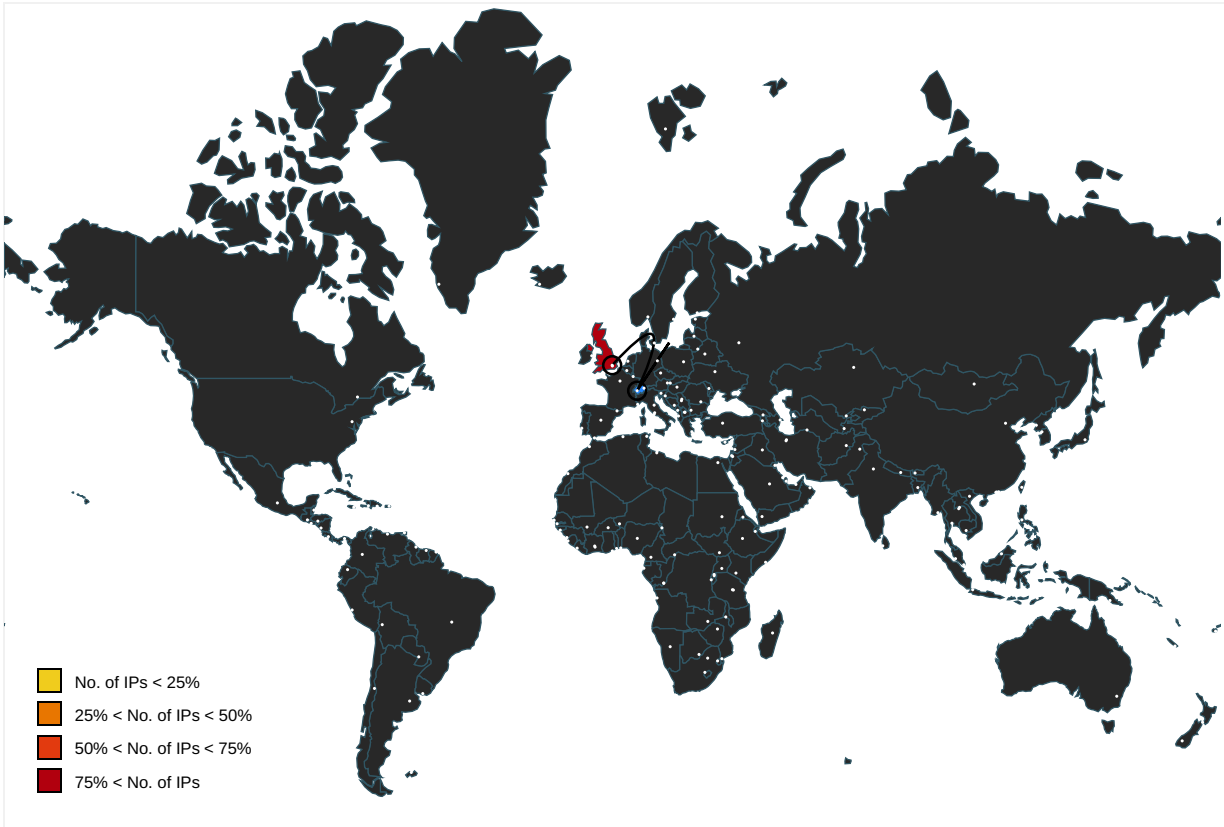
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	invoice.pdf.exe, 00000002.00000002.506799805.00000000036A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D8200.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false		high
http://www.carterandcone.comechP	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/eO	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false		high
http://www.carterandcone.comeac	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTFnO	invoice.pdf.exe, 00000001.00000003.236081460.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	invoice.pdf.exe, 00000001.00000002.240792649.0000000002701000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/nO	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/tN	invoice.pdf.exe, 00000001.00000003.233778392.0000000004B8900.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/-OQ	invoice.pdf.exe, 00000001.00000003.234841586.0000000004B7800.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comAO	invoice.pdf.exe, 00000001.00000003.236081460.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://HtsCZk.com	invoice.pdf.exe, 00000002.00000002.506799805.00000000036A100.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comext	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	invoice.pdf.exe, 00000002.00000002.506799805.00000000036A100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D80200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D82000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D82000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D82000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%	invoice.pdf.exe, 00000002.00000002.506799805.00000000036A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	invoice.pdf.exe, 00000001.00000002.241020858.0000000003701000.00000004.00000001.sdmp, invoice.pdf.exe, 00000002.00000002.501365134.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schooldb.inchat.kro.kr/	invoice.pdf.exe	false		high
http://www.fontbureau.comgrita$OX	invoice.pdf.exe, 00000001.00000003.239621781.0000000004B75000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coma	invoice.pdf.exe, 00000001.00000003.233981816.0000000004B84000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D82000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	invoice.pdf.exe, 00000001.00000003.236081460.0000000004B7A000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comdiaoJO	invoice.pdf.exe, 00000001.00000003.239621781.0000000004B75000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/JO	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0anSO7	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	invoice.pdf.exe, 00000002.00000002.506799805.00000000036A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comati	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	invoice.pdf.exe, 00000002.00000002.507278003.0000000003719000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://inchat.kro.kr	invoice.pdf.exe	false		high
http://www.carterandcone.comd	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://MFtHNrHfTnJ.net	invoice.pdf.exe, 00000002.00000002.506799805.00000000036A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	invoice.pdf.exe, 00000002.00000002.506799805.00000000036A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/JO	invoice.pdf.exe, 00000001.00000003.234841586.0000000004B78000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gagalive.kr/livechat1.swf?chatroom=inchat-	invoice.pdf.exe	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/on	invoice.pdf.exe, 00000001.00000003.234841586.0000000004B78000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comeO	invoice.pdf.exe, 00000001.00000003.239621781.0000000004B75000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	invoice.pdf.exe, 00000001.00000003.236081460.0000000004B7A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D82000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D8200.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D8200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/6OJ	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D8200.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/s	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/$OX	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comessedwO	invoice.pdf.exe, 00000001.00000003.236081460.0000000004B7A00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	invoice.pdf.exe, 00000001.00000002.244593418.0000000005D8200.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/ConnAO	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comang	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comituF$OX	invoice.pdf.exe, 00000001.00000003.236081460.0000000004B7A00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/vv	invoice.pdf.exe, 00000001.00000003.234841586.0000000004B7800.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/-OQ	invoice.pdf.exe, 00000001.00000003.235152791.0000000004B7A00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.221.216.77	unknown	United Kingdom		393960	HOST4GEEKS-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358190
Start date:	25.02.2021
Start time:	07:44:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoice.pdf.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:	26
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:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 65% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 92.122.145.220, 104.43.193.48, 168.61.161.212, 23.218.208.56, 51.11.168.160, 2.20.142.210, 2.20.142.209, 51.103.5.159, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
07:45:40	API Interceptor	999x Sleep call for process: invoice.pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.221.216.77	invoice copys.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.com-cept.com	invoice copys.exe	Get hash	malicious	Browse	• 185.221.216.77

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOST4GEEKS-LLCUS	synchronossTicket#513473.htm	Get hash	malicious	Browse	• 185.221.216.34
	invoice copys.exe	Get hash	malicious	Browse	• 185.221.216.77
	55-2912.doc	Get hash	malicious	Browse	• 66.85.46.76
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 66.85.46.76
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 66.85.46.76
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 66.85.46.76
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 66.85.46.76
	FILE_122020_VVY_591928.doc	Get hash	malicious	Browse	• 66.85.46.76
	Archivo_29_48214503.doc	Get hash	malicious	Browse	• 66.85.46.76
	Adjunto 29 886_473411.doc	Get hash	malicious	Browse	• 66.85.46.76
	Informacion_29.doc	Get hash	malicious	Browse	• 66.85.46.76
	Informacion_29.doc	Get hash	malicious	Browse	• 66.85.46.76
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 66.85.46.76
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 66.85.46.76
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 66.85.46.76
	DAT.doc	Get hash	malicious	Browse	• 66.85.46.76
	ARCHIVOFile_762-36284.doc	Get hash	malicious	Browse	• 66.85.46.76
	4640-2912-122020.doc	Get hash	malicious	Browse	• 66.85.46.76
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 66.85.46.76
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 66.85.46.76

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoice.pdf.exe.log

Process:	C:\Users\user\Desktop\invoice.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.588265788010279

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:	invoice.pdf.exe
File size:	486912
MD5:	d3bb643f07aee4cc6be3d303222bd2c9
SHA1:	a5804c4525cb33a8eb1a4c534e9da3824a826980
SHA256:	4e49cd4c9abc7a87bd4da347a31454701ab005bf1f9d929 5b9f16de4353f56dc
SHA512:	6fe8c0d2471df4ee732299628dedfaf575501cd8cb2efa1a 1ad2ab5e6dafa1e9941fd8da1359f2b9de7481406cd33d9 e4172df55ecf6b585ee9580b2ee74b693
SSDEEP:	12288:XH5M2ZZvHLaMoOsT8XvgynR2yLc5GOqhiyI3N 4Y:Xq2Z5uMcT8/pnLc585WN4
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... 6`.....P..d.....f.... .....@.. ..... .@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x478266
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:	0x6036D2FE [Wed Feb 24 22:28:14 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x78214	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7a000	0x5dc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7c000	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	0x7626c	0x76400	False	0.812343089323	data	7.60133626951	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7a000	0x5dc	0x600	False	0.43359375	data	4.22610011924	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7c000	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	0x7a090	0x34c	data		
RT_MANIFEST	0x7a3ec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

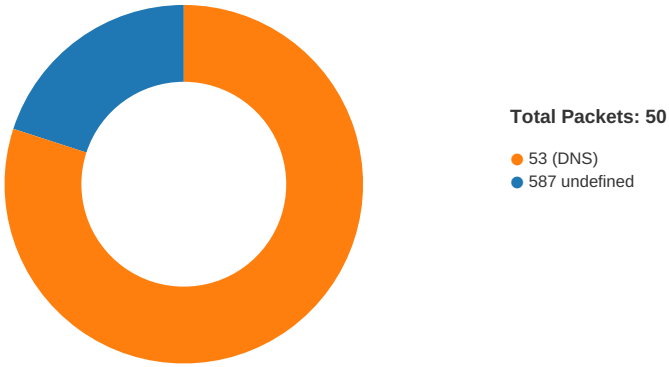
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016 - 2021
Assembly Version	1.0.0.0
InternalName	TRACEQUERYINFOCLASS.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ASM PS
ProductVersion	1.0.0.0
FileDescription	ASM PS
OriginalFilename	TRACEQUERYINFOCLASS.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:47:11.041878939 CET	49748	587	192.168.2.7	185.221.216.77
Feb 25, 2021 07:47:11.099550009 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.099716902 CET	49748	587	192.168.2.7	185.221.216.77
Feb 25, 2021 07:47:11.234230995 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.238316059 CET	49748	587	192.168.2.7	185.221.216.77
Feb 25, 2021 07:47:11.298199892 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.299180031 CET	49748	587	192.168.2.7	185.221.216.77
Feb 25, 2021 07:47:11.360979080 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.401804924 CET	49748	587	192.168.2.7	185.221.216.77
Feb 25, 2021 07:47:11.406331062 CET	49748	587	192.168.2.7	185.221.216.77
Feb 25, 2021 07:47:11.472676039 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.472706079 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.472729921 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.472743988 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.472771883 CET	49748	587	192.168.2.7	185.221.216.77
Feb 25, 2021 07:47:11.472800970 CET	49748	587	192.168.2.7	185.221.216.77
Feb 25, 2021 07:47:11.475091934 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.483385086 CET	49748	587	192.168.2.7	185.221.216.77
Feb 25, 2021 07:47:11.542651892 CET	587	49748	185.221.216.77	192.168.2.7
Feb 25, 2021 07:47:11.545597076 CET	49748	587	192.168.2.7	185.221.216.77

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:45:29.929872990 CET	53	53775	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:30.501810074 CET	51837	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:30.563373089 CET	53	51837	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:30.723601103 CET	55411	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:30.772183895 CET	53	55411	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:40.010601997 CET	63668	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:40.067771912 CET	53	63668	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:41.132278919 CET	54640	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:41.181118011 CET	53	54640	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:42.356674910 CET	58739	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:42.405380964 CET	53	58739	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:43.438487053 CET	60338	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:43.487229109 CET	53	60338	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:45.449098110 CET	58717	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:45.500652075 CET	53	58717	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:46.362993956 CET	59762	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:46.413685083 CET	53	59762	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:47.211992979 CET	54329	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:47.260826111 CET	53	54329	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:48.251665115 CET	58052	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:48.310827971 CET	53	58052	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:49.282202005 CET	54008	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:49.340861082 CET	53	54008	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:50.463219881 CET	59451	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:50.513267040 CET	53	59451	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:51.425451994 CET	52914	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:51.477083921 CET	53	52914	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:52.942915916 CET	64569	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:52.994226933 CET	53	64569	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:53.908653021 CET	52816	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:53.969897032 CET	53	52816	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:55.346628904 CET	50781	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:55.395332098 CET	53	50781	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:56.127955914 CET	54230	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:56.176606894 CET	53	54230	8.8.8.8	192.168.2.7
Feb 25, 2021 07:45:59.285716057 CET	54911	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:45:59.334491014 CET	53	54911	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:00.237407923 CET	49958	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:00.288676023 CET	53	49958	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:01.296257973 CET	50860	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:01.351079941 CET	53	50860	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:02.185996056 CET	50452	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:02.234764099 CET	53	50452	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:07.447736979 CET	59730	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:07.498127937 CET	53	59730	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:25.939229012 CET	59310	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:25.998996019 CET	53	59310	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:26.659382105 CET	51919	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:26.708070993 CET	53	51919	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:30.758517981 CET	64296	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:30.816822052 CET	53	64296	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:33.473304033 CET	56680	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:33.524985075 CET	53	56680	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:34.088426113 CET	58820	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:34.145903111 CET	53	58820	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:34.824124098 CET	60983	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:34.872814894 CET	53	60983	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:35.417375088 CET	49247	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:35.474327087 CET	53	49247	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:35.961294889 CET	52286	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:36.012943983 CET	53	52286	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:36.638849974 CET	56064	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:36.669473886 CET	63744	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:36.698359013 CET	53	56064	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:46:36.737001896 CET	53	63744	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:37.587342978 CET	61457	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:37.649615049 CET	53	61457	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:38.487600088 CET	58367	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:38.524760962 CET	60599	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:38.547660112 CET	53	58367	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:38.585912943 CET	53	60599	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:39.448039055 CET	59571	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:39.509650946 CET	53	59571	8.8.8.8	192.168.2.7
Feb 25, 2021 07:46:40.122548103 CET	52689	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:46:40.171725988 CET	53	52689	8.8.8.8	192.168.2.7
Feb 25, 2021 07:47:10.945453882 CET	50290	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:47:11.021434069 CET	53	50290	8.8.8.8	192.168.2.7
Feb 25, 2021 07:47:11.447138071 CET	60427	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:47:11.496120930 CET	53	60427	8.8.8.8	192.168.2.7
Feb 25, 2021 07:47:13.363775015 CET	56209	53	192.168.2.7	8.8.8.8
Feb 25, 2021 07:47:13.433437109 CET	53	56209	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 07:47:10.945453882 CET	192.168.2.7	8.8.8.8	0x68aa	Standard query (0)	mail.com-cept.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 07:47:11.021434069 CET	8.8.8.8	192.168.2.7	0x68aa	No error (0)	mail.com-cept.com		185.221.216.77	A (IP address)	IN (0x0001)

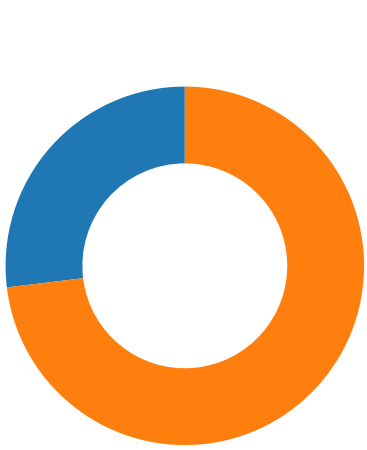
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 07:47:11.234230995 CET	587	49748	185.221.216.77	192.168.2.7	220-uksrv3.websiteserverbox.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 01:47:10 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 07:47:11.238316059 CET	49748	587	192.168.2.7	185.221.216.77	EHLO 724536
Feb 25, 2021 07:47:11.298199892 CET	587	49748	185.221.216.77	192.168.2.7	250-uksrv3.websiteserverbox.com Hello 724536 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 07:47:11.299180031 CET	49748	587	192.168.2.7	185.221.216.77	STARTTLS
Feb 25, 2021 07:47:11.360979080 CET	587	49748	185.221.216.77	192.168.2.7	220 TLS go ahead

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: invoice.pdf.exe PID: 6496 Parent PID: 5760

General

Start time:	07:45:37
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\invoice.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\invoice.pdf.exe'
Imagebase:	0xb0000
File size:	486912 bytes
MD5 hash:	D3BB643F07AEE4CC6BE3D303222BD2C9
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: 00000001.00000002.241020858.0000000003701000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.240792649.0000000002701000.00000004.00000001.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	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoice.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	724534A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoice.pdf.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7273A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile

Analysis Process: invoice.pdf.exe PID: 6580 Parent PID: 6496

General

Start time:	07:45:41
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\invoice.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\invoice.pdf.exe
Imagebase:	0xf80000
File size:	486912 bytes
MD5 hash:	D3BB643F07AEE4CC6BE3D303222BD2C9
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: 00000002.00000002.506799805.00000000036A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.506799805.00000000036A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.508855968.0000000003B2E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.501365134.0000000000402000.00000040.00000001.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	724660AC	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	724660AC	unknown
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	724660AC	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	724660AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	609113B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	609113B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	609113B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\902d6aee-087a-44a7-a139-9eb425bfe744	unknown	4096	success or wait	1	609113B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	609113B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	609113B	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	609113B	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	609113B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	609113B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	609113B	ReadFile

Disassembly

Code Analysis