ID: 320280
Sample Name: invoicePDF.exe
Cookbook: default.jbs
Time: 08:30:20
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

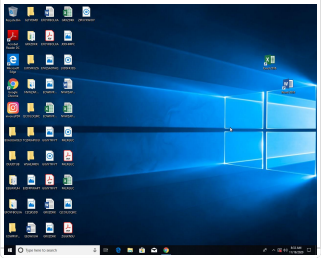
Analysis Report invoicePDF.exe

Overview

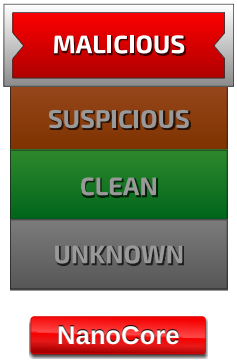
General Information

Sample Name:	invoicePDF.exe
Analysis ID:	320280
MD5:	71fbb96e66805ff…
SHA1:	deb4d9f604ac150.
SHA256:	78323d67f56b427.
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

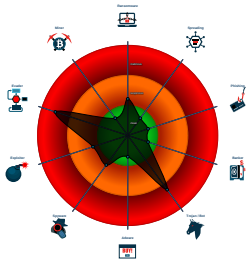


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- Executable has a suspicious name (…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- invoicePDF.exe (PID: 5548 cmdline: 'C:\Users\user\Desktop\invoicePDF.exe' MD5: 71FBB96E66805FFC1F477B3CD89E1A99)
  - schtasks.exe (PID: 4392 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\qOrsEUNRoVVp' /XML 'C:\Users\user\AppData\Local\Temp\tmp69A8.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - invoicePDF.exe (PID: 4532 cmdline: {path} MD5: 71FBB96E66805FFC1F477B3CD89E1A99)
  - invoicePDF.exe (PID: 3440 cmdline: {path} MD5: 71FBB96E66805FFC1F477B3CD89E1A99)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.255600273.0000000006D61000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1da8ad:$x1: NanoCore.ClientPluginHost • 0x2844ed:$x1: NanoCore.ClientPluginHost • 0x1da8ea:$x2: IClientNetworkHost • 0x28452a:$x2: IClientNetworkHost • 0x1de41d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x28805d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.255600273.0000000006D61000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.255600273.0000000006D6 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1da615:$a: NanoCore • 0x1da625:$a: NanoCore • 0x1da859:$a: NanoCore • 0x1da86d:$a: NanoCore • 0x1da8ad:$a: NanoCore • 0x284255:$a: NanoCore • 0x284265:$a: NanoCore • 0x284499:$a: NanoCore • 0x2844ad:$a: NanoCore • 0x2844ed:$a: NanoCore • 0x1da674:$b: ClientPlugin • 0x1da876:$b: ClientPlugin • 0x1da8b6:$b: ClientPlugin • 0x2842b4:$b: ClientPlugin • 0x2844b6:$b: ClientPlugin • 0x2844f6:$b: ClientPlugin • 0x12f462:$c: ProjectData • 0x1da79b:$c: ProjectData • 0x2843db:$c: ProjectData • 0x13017b:$d: DESCrypto • 0x1db1a2:$d: DESCrypto
00000000.00000002.252586380.000000000312 2000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: invoicePDF.exe PID: 5548	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

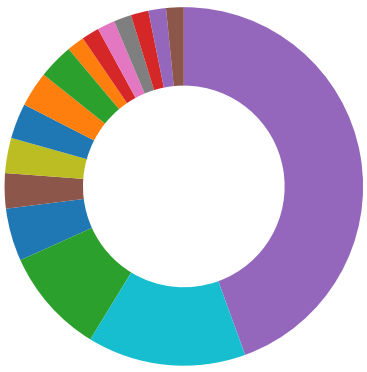
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



Click to jump to signature section

- AV Detection
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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

Initial sample is a PE file and has a suspicious name

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM_3

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 Nanocore RAT

Remote Access Functionality:

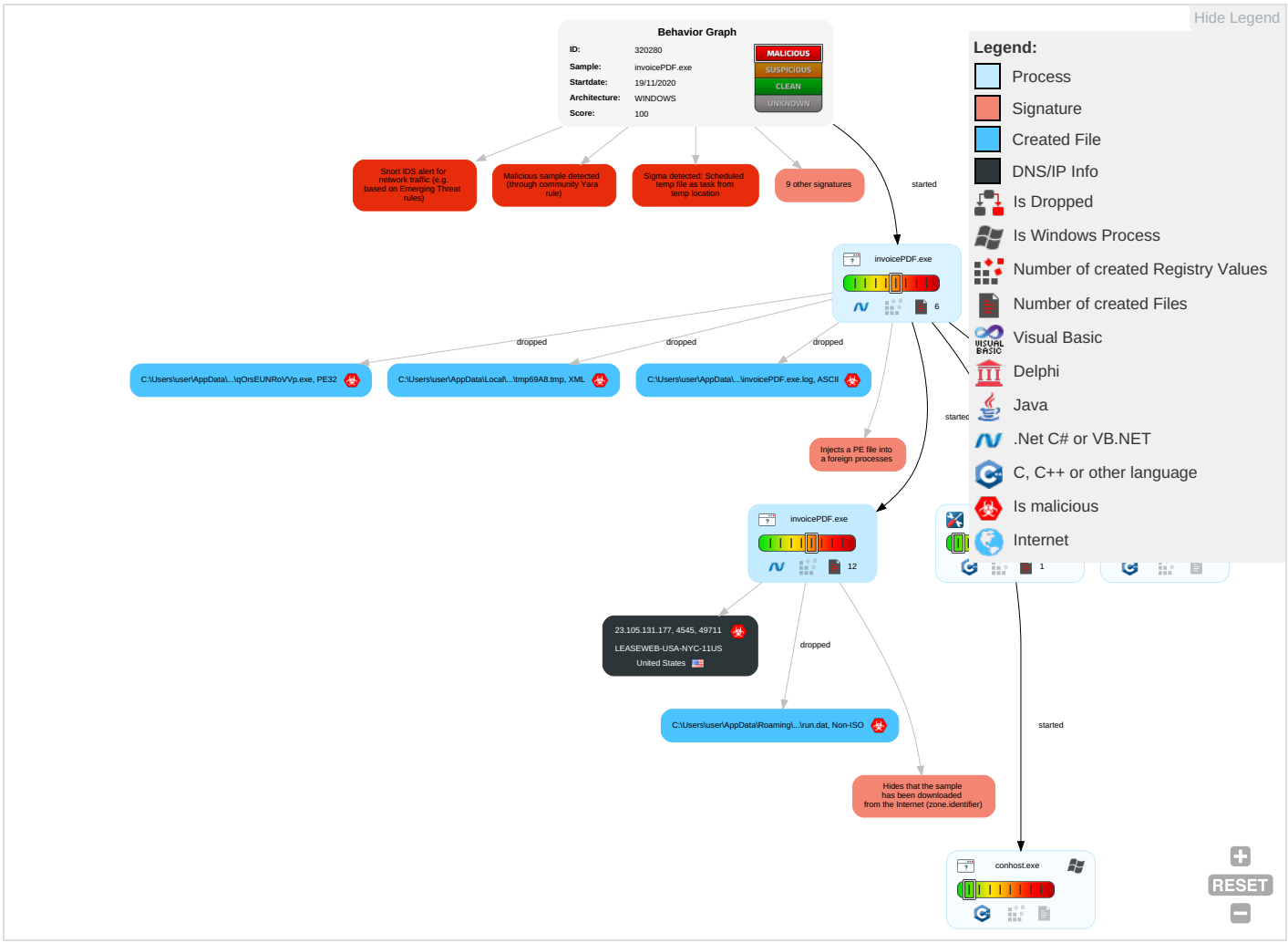
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

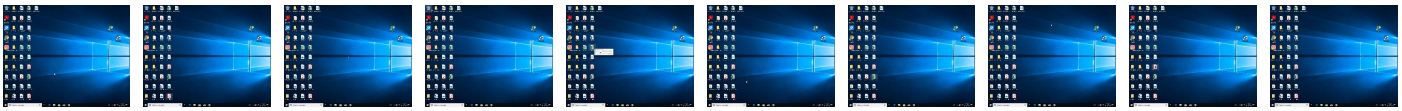
Behavior Graph



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
invoicePDF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\qOrsEUNRoVVp.exe	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-e	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.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr$	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.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.fonts.comic	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krV	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cny	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnt	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.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/-u	0%	Avira URL Cloud	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.founder.com.cn/cn/h	0%	Avira URL Cloud	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.founder.com.cn/cnt-i	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comx	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comu=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/E	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.tiro.comtn	0%	Avira URL Cloud	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.tiro.comcom	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnm=o	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comcomma	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/a-e	invoicePDF.exe, 00000000.00000003.236978150.0000000007764000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false		high
http://www.tiro.com	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp, invoicePDF.exe, 00000000.00000003.233995308.000000000777B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.kr$	invoicePDF.exe, 00000000.00000003.234807091.0000000007766000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersP	invoicePDF.exe, 00000000.00000003.238816781.0000000007769000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	invoicePDF.exe, 00000000.00000003.233717553.000000000777B000.00000004.00000001.sdmp, invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic	invoicePDF.exe, 00000000.00000003.233861149.000000000777B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krV	invoicePDF.exe, 00000000.00000003.234807091.0000000007766000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cny	invoicePDF.exe, 00000000.00000003.235433616.000000000779D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnt	invoicePDF.exe, 00000000.00000003.235832918.0000000007764000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	invoicePDF.exe, 00000000.00000003.236978150.0000000007764000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/-u	invoicePDF.exe, 00000000.00000003.235832918.0000000007764000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	invoicePDF.exe, 00000000.00000003.233823605.000000000777B000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	invoicePDF.exe, 00000000.00000003.234807091.0000000007766000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/h	invoicePDF.exe, 00000000.00000003.235832918.0000000007764000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnt-i	invoicePDF.exe, 00000000.00000003.235433616.000000000779D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comx	invoicePDF.exe, 00000000.00000003.233823605.000000000777B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/X	invoicePDF.exe, 00000000.00000003.236978150.0000000007764000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/S	invoicePDF.exe, 00000000.00000003.236978150.0000000007764000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comu=	invoicePDF.exe, 00000000.00000003.233717553.000000000777B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/E	invoicePDF.exe, 00000000.00000003.236978150.0000000007764000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	invoicePDF.exe, 00000000.00000003.236978150.0000000007764000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comtn	invoicePDF.exe, 00000000.00000003.234011048.000000000777B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.come.com	invoicePDF.exe, 00000000.00000002.256205653.0000000007760000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comcom	invoicePDF.exe, 00000000.00000003.234026172.000000000777B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	invoicePDF.exe, 00000000.00000003.235909054.000000000776B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnm=o	invoicePDF.exe, 00000000.00000003.235433616.000000000779D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma7	invoicePDF.exe, 00000000.00000002.256205653.0000000007760000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	invoicePDF.exe, 00000000.00000003.236978150.0000000007764000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	invoicePDF.exe, 00000000.00000003.239254455.000000000776D000.00000004.00000001.sdmp, invoicePDF.exe, 00000000.00000002.256342214.00000000078D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comcomma	invoicePDF.exe, 00000000.00000002.256205653.0000000007760000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.105.131.177	unknown	United States		396362	LEASEWEB-USA-NYC-11US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320280
Start date:	19.11.2020
Start time:	08:30:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoicePDF.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/8@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.8% (good quality ratio 9%) • Quality average: 49.5% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 94% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • 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
08:31:18	API Interceptor	1001x Sleep call for process: invoicePDF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.105.131.177	TDToxqrclL.exe	Get hash	malicious	Browse	
	ORDER INQUIRY.pdf.exe	Get hash	malicious	Browse	
	Purchase Order 4500033557.pdf.exe	Get hash	malicious	Browse	
	SHIPPING DOCUMENTS.pdf.exe	Get hash	malicious	Browse	
	SHIPPING INVOICE.pdf.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	invoice & packing.pdf.exe	Get hash	malicious	Browse	• 23.105.131.164
	NXKfWP9SPF0XHRu.exe	Get hash	malicious	Browse	• 23.105.131.214
	DOC.exe	Get hash	malicious	Browse	• 23.105.131.162
	Shipping_Details.exe	Get hash	malicious	Browse	• 23.105.131.165
	2AyWKsCvVF.exe	Get hash	malicious	Browse	• 192.253.246.143
	tn9jVPvlMSqAUX5.exe	Get hash	malicious	Browse	• 23.105.131.229
	HLiw2LPA8i.rtf	Get hash	malicious	Browse	• 192.253.246.143
	TDToxqrclL.exe	Get hash	malicious	Browse	• 23.105.131.177
	Ziiq5tI3CT.exe	Get hash	malicious	Browse	• 23.105.131.239
	f3wo2FuLN6.exe	Get hash	malicious	Browse	• 192.253.246.143
	ORDER INQUIRY.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Purchase Order 4500033557.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	SecuriteInfo.com.Trojan.DownLoader35.34609.25775.exe	Get hash	malicious	Browse	• 192.253.246.138
	Proof_of_payment.xlsm	Get hash	malicious	Browse	• 23.105.131.217
	invoice tax.xlsm	Get hash	malicious	Browse	• 23.105.131.217
	SHIPPING DOCUMENTS.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Payment_Order_20201111.xlsx	Get hash	malicious	Browse	• 192.253.246.138
	TLpMnhJmg7.exe	Get hash	malicious	Browse	• 192.253.246.143
	HDyADDoI3I.exe	Get hash	malicious	Browse	• 192.253.246.143
	11.exe	Get hash	malicious	Browse	• 173.234.155.145

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\invoicePDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	5.271473536084351
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoicePDF.exe.log	
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70U2u7x5I6Hi0Ug+9Yz9tv:MLF20NaL329hJ5g522rW2I3rOz2T
MD5:	C3EC08CD6BEA8576070D5A52B4B6D7D0
SHA1:	40B95253F98B3CC5953100C0E71DAC7915094A5A
SHA-256:	28B314C3E5651414FD36B2A65B644A2A55F007A34A536BE17514E12CEE5A091B
SHA-512:	5B0E6398A092F08240DC6765425E16DB52F32542FF7250E87403C407E54B3660EF93E0EAD17BA2CEF6B666951ACF66FA0EAD61FB52E80867DDD398E8258DED2
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\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.Web\d05d469d89b319a068f2123e7e6f8621\System.Web.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp69A8.tmp	
Process:	C:\Users\user\Desktop\invoicePDF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1649
Entropy (8bit):	5.177706223059003
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBqOtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3j
MD5:	EAAC4199D1BA170974F111BD475BC456
SHA1:	394B659987331043A4A866A6E751512D370FB057
SHA-256:	4BEBBAEA5EC94A4F0C4686E242E9D175CAEB5B37A1452C446629FA5F1DE27DED
SHA-512:	447D27747C7B95969CA5E638F23CC03020B2E5A6FB2410659EED02FF066F97D6DF99A3DBD697F3891F60040BADB52E0715166067F0C3EFA0AF5EAE8DE7138CF
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\invoicePDF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\invoicePDF.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:fpNpP:f9
MD5:	930EF7F1A5AAFEEA4FBB4409AD08C590
SHA1:	B3AA518D3C65611A6666E73C606ED7239BF984FA
SHA-256:	576ADCB3BBA6BFBFD3B550456E0EEC05258204E2ED46934A206EDED08FB24CD2
SHA-512:	C013A4684EB497B988ACA0798BB5A6987694FEF9E9E4A32D019463211B453975BCF602E7469C02DFFBBB3AF93F83808DB4D898C5076DD6B65A271F92F806A548
Malicious:	**true**

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Reputation:	low
Preview:	.X...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\invoicePDF.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.584962500721156
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBn:RzWDqTB
MD5:	3FCC766D28BFD974C68B38C27D0D7A9A
SHA1:	45ED19A78D9B79E46EDBFC3E3CA58E90423A676B
SHA-256:	39A25F1AB5099005A74CF04F3C61C3253CD9BDA73B85228B58B45AAA4E838641
SHA-512:	C7D47BDAABEEBB8C9D9B31CC4CE968EAF291771762FA022A2F55F9BA4838E71FDBD3F83792709E47509C5D94629D6D274CC933371DC01560D13016D944012D5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.....l.d

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\invoicePDF.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.425704882778696
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBPcgY6oRDMjmPl:RzWDqTdRWDMCd
MD5:	CA214D2E41394F5ADA74FA4F2EA15CB5
SHA1:	32E3F863838177349F2AF70CA1CE695B3C184166
SHA-256:	B6E370AF3F5C1001C79BC19706D1A5B1803C59BC45AEFAB4BD18FC67034F47A1
SHA-512:	E9C268BCDE8872F4DD2964ACA6F9C51834E42E2AF7FF2E1C327573CEDC98127B0EDBBF8E76E456FFF82A28FC46A210D91EEEA2242ECED5368D107436B349214
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.....l.d9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\invoicePDF.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:....L.g<.....I..%4[.G^.~.l'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-.P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\qOrsEUNRoVVp.exe	
Process:	C:\Users\user\Desktop\invoicePDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	488448
Entropy (8bit):	7.843226468010816

C:\Users\user\AppData\Roaming\qOrsEUNRoVVp.exe	
Encrypted:	false
SSDEEP:	12288:CgRJEqCCYu5Poz1wgLZQ9P/wk6ESR2j8xN8r2THYps39BMTFo:CgjEfCYZdiA1RK8D8r2
MD5:	71FBB96E66805FFC1F477B3CD89E1A99
SHA1:	DEB4D9F604AC1502BC5CD601753E8B588A0EBA0B
SHA-256:	78323D67F56B427A363820B094A4081E652B7E740C75E715FA96FB7CCF96795F
SHA-512:	F6BDE7C29C8D5C42B8A4B39417E9D61FE9F37AA0A679B94F8D54797362C59DC6288FE25733F94CFC472606CC42BE3391A9EC7BE352E1FE691B82D3A9CEE115C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....,...F.....nJ... ...`....@.. ..... ..@.....J..S....`..HB..... ....H.....text...t*... ...,..... ..`.rsrc...HB...`...D.....@..@.rel oc.....r.....@..B.....PJ.....H.....xp.....\|....X..?0...P..s....K..d...X'....Aj.\|K."...I.q+dm...` .Z.....A...Sr.....WCF.O.r.m.+. k#...`%\|.#..@.{.*%...M. ...}..q.(}..Uv...L....0!..^..'..n.?Y...j:zl.....\|.2z..JeL...K..0<J.....s.[$....E.i..s.[.~Ms....n.....x....b"..... ..qbm...k.TI.Rh...qm.,A9....c..\OD..Q..+8.:..?|....cv..~x^A ...).J7..5.d?.....:.*N...Z3./c.o..r.Yc?.}.....Ug.....y.....u.....c3..~.... .N... .

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.843226468010816
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	invoicePDF.exe
File size:	488448
MD5:	71fbb96e66805ffc1f477b3cd89e1a99
SHA1:	deb4d9f604ac1502bc5cd601753e8b588a0eba0b
SHA256:	78323d67f56b427a363820b094a4081e652b7e740c75e715fa96fb7ccf96795f
SHA512:	f6bde7c29c8d5c42b8a4b39417e9d61fe9f37aa0a679b94f8d54797362c59dc6288fe25733f94cfc472606cc42be3391a9ec7be352e1fe691b82d3a9cee1155c
SSDEEP:	12288:CgRJEqCCYu5Poz1wgLZQ9P/wk6ESR2j8xN8r2THYps39BMTFo:CgjEfCYZdiA1RK8D8r2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....,...F.....nJ... ...`....@.. .....@.....

File Icon

Icon Hash:	f8c492aaaa92dcfe

Static PE Info

General

Entrypoint:	0x474a6e
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:	0x5FB5BEAB [Thu Nov 19 00:39:07 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727

General

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74a18	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x76000	0x4248	.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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x72a74	0x72c00	False	0.902945857162	data	7.86853683687	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x4248	0x4400	False	0.493106617647	data	5.4056455766	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_ICON	0x761c0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x76628	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4275388049, next used block 4258479509		
RT_ICON	0x776d0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 3771611807, next used block 3167566498		
RT_GROUP_ICON	0x79c78	0x30	data		
RT_GROUP_ICON	0x79ca8	0x14	data		
RT_VERSION	0x79cbc	0x39e	data		
RT_MANIFEST	0x7a05c	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	Les loups-garous de Thiercelieux 1998
Assembly Version	27.0.0.0
InternalName	.exe
FileVersion	11.0.0.0
CompanyName	Les loups-garous de Thiercelieux
LegalTrademarks	
Comments	Jeu de la barbichette
ProductName	Ptanque
ProductVersion	11.0.0.0
FileDescription	Ptanque
OriginalFilename	.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/19/20-08:31:23.859506	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	4545	192.168.2.5	23.105.131.177

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 08:31:23.388092041 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:23.710218906 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:23.710346937 CET	49711	4545	192.168.2.5	23.105.131.177

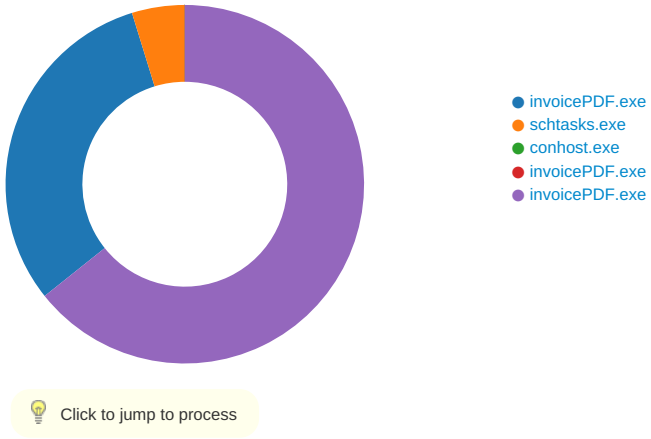
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 08:31:23.859505892 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:24.194200039 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:24.217653036 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:24.550395966 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:24.567853928 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:24.967032909 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:24.967221022 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:24.974666119 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:24.975167990 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:24.992713928 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:24.993043900 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:24.998570919 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:24.998682976 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.002340078 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.002448082 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.004663944 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.004724026 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.004842997 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.008321047 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.008595943 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.012352943 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.012531996 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.018557072 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.018641949 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.022696972 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.022792101 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.322532892 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.344458103 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.344587088 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.352382898 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.360383987 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.361558914 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.367640018 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.370583057 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.370760918 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.374444008 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.378453016 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.378622055 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.382503986 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.387371063 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.387499094 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.390377998 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.394130945 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.394372940 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.398411036 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.402563095 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.402790070 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.406306982 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.410427094 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.410614014 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.428561926 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.428623915 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.428806067 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.438710928 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.438771009 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.438927889 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.700515032 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.720784903 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.720875978 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.730659962 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.740634918 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.740714073 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.749887943 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.752598047 CET	4545	49711	23.105.131.177	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 08:31:25.752691984 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.762777090 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.772658110 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.772689104 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.772706985 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.772865057 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.777041912 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.780257940 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.780433893 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.785446882 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.788806915 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.788897038 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.806674004 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.806706905 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.806762934 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.806778908 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.806843996 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.806896925 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.810286045 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.828433037 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.828470945 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.828507900 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.838854074 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.838886976 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.838911057 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.838924885 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.838959932 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.839046001 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.856554031 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.856626034 CET	49711	4545	192.168.2.5	23.105.131.177
Nov 19, 2020 08:31:25.856770992 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.856797934 CET	4545	49711	23.105.131.177	192.168.2.5
Nov 19, 2020 08:31:25.856822968 CET	4545	49711	23.105.131.177	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: invoicePDF.exe PID: 5548 Parent PID: 5744

General

Start time:	08:31:12
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\invoicePDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\invoicePDF.exe'
Imagebase:	0x9c0000
File size:	488448 bytes
MD5 hash:	71FBB96E66805FFC1F477B3CD89E1A99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.255600273.0000000006D61000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.255600273.0000000006D61000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.255600273.0000000006D61000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.252586380.0000000003122000.00000004.00000001.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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\qOrsEUNRoVVp.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	77307D7	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp69A8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	120B2B8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoicePDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp69A8.tmp	success or wait	1	773144E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\qOrsEUNRoVVp.exe	unknown	488448	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 ab be b5 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 2c 07 00 00 46 00 00 00 00 00 00 6e 4a 07 00 00 20 00 00 00 60 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 e0 07 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....._..... .....,...F.....nJ... ...`....@.. ....@.....	success or wait	1	7730A5F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp69A8.tmp	unknown	1649	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	7730A5F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoicePDF.exe.log	unknown	641	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 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	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\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	72E5A33A	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Users\user\Desktop\invoicePDF.exe	unknown	488448	success or wait	1	7730A5F	ReadFile

Analysis Process: schtasks.exe PID: 4392 Parent PID: 5548

General

Start time:	08:31:19
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\qOrsEUNRoVVp' /XML 'C:\Users\user\AppData\Local\Temp\tmp69A8.tmp'
Imagebase:	0xde0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp69A8.tmp	unknown	2	success or wait	1	DEAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp69A8.tmp	unknown	1650	success or wait	1	DEABD9	ReadFile

Analysis Process: conhost.exe PID: 340 Parent PID: 4392

General

Start time:	08:31:19
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: invoicePDF.exe PID: 4532 Parent PID: 5548

General

Start time:	08:31:20
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\invoicePDF.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0xf0000
File size:	488448 bytes
MD5 hash:	71FBB96E66805FFC1F477B3CD89E1A99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: invoicePDF.exe PID: 3440 Parent PID: 5548

General

Start time:	08:31:20
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\invoicePDF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x540000
File size:	488448 bytes
MD5 hash:	71FBB96E66805FFC1F477B3CD89E1A99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4EC07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4EC089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4EC07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4EC07A1	CreateDirectoryW
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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4EC089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4EC089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4EC089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	4EC36BC	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\invoicePDF.exe:Zone.Identifier	success or wait	1	4EC0B41	DeleteFileA
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	72167D95	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	c3 58 e1 8c a8 8c d8 48	.X.....H	success or wait	1	4EC0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	4EC0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	426840	c1 e9 67 26 6a 6f 1f 01 d5 49 50 67 08 81 cd a2 47 4d d1 a4 d4 0d a7 52 3e 69 e1 fc 09 6f 8c b1 04 49 e1 3e e3 bb b0 26 9f 72 7b d6 fa a5 93 38 a9 d3 a5 93 7d ff da 89 8a 45 03 7f ea e6 96 76 cf 21 37 95 75 33 65 bc fc 20 fb c0 05 b7 f7 64 62 bd 90 15 7d b2 c7 1d 02 02 ab e8 22 c2 74 28 06 78 43 39 b8 63 70 15 42 e6 e0 91 e1 37 82 0f 1b 27 bd 93 ad a1 d3 7f c2 25 bd 09 b2 06 eb c7 77 86 5e ac c1 5f 13 c4 d2 02 d8 9d d4 b4 f1 42 b7 57 25 fd 3c ce a6 d9 a4 69 e1 30 d1 7b 39 bb 78 53 fc ab fb 35 c5 d8 c7 29 05 ef 77 ca 0f 24 14 92 43 87 80 3f 60 46 d7 8f da 75 a8 35 db 92 54 b6 58 ab 77 27 53 69 f4 f0 7a b2 6e 7b 8f ef b9 ea 9f 84 59 21 6d d8 d3 1c 52 41 f8 b9 e3 78 67 d3 d0 ba 03 e9 5b 37 8a 18 89 7a b7 9f 39 40 02 4b ca 2d 9a fe 88 54 95 8d 2b d8 41 43 65	..g&jo...IPg....GM.....R>i...o ...I.>...&.r{....8....}....E.. ...v.!7.u3e.. .....db...}..... ..".t(.xC9.cp.B....7...'..... .%......w.^._.........B.W%.<. ...i.0.{9.xS...5...)..w..$..C..? `F...u.5..T.X.w'Si..z.n{.... ..Y!m...RA...xg..... [7...z..9@.K.-...T..+.ACe	success or wait	1	4EC0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d db 87 b1 98 c9 6c f6 64	9iH....}Z..4..f.....l.d	success or wait	2	4EC0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d db 87 b1 98 c9 6c f6 64	9iH....}Z..4..f.....l.d	success or wait	1	4EC36BC	CopyFileW

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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Users\user\Desktop\invoicePDF.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Users\user\Desktop\invoicePDF.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4EC0A53	ReadFile

Disassembly

Code Analysis