ID: 320240
Sample Name: invoice & packing.pdf.exe
Cookbook: default.jbs
Time: 07:46:27
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

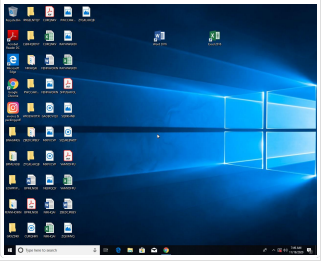
Analysis Report invoice & packing.pdf.exe

Overview

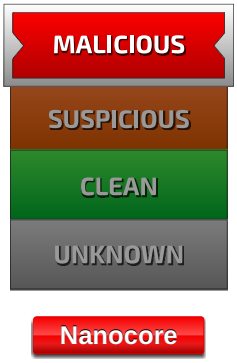
General Information

Sample Name:	invoice & packing.pdf.exe
Analysis ID:	320240
MD5:	ac3668260346d5..
SHA1:	479c7e0b3696f17.
SHA256:	3f746fa6f84b842...
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

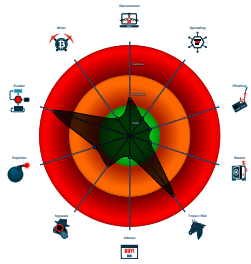


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through ...
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file...
- Sigma detected: Suspicious Double ...
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- 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...
- Tries to detect sandboxes and other

Classification



Startup

- **System is w10x64**
- invoice & packing.pdf.exe (PID: 7160 cmdline: 'C:\Users\user\Desktop\invoice & packing.pdf.exe' MD5: AC3668260346D59F25905579AA8EAF94)
  - schtasks.exe (PID: 1560 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NKzWuwUvFAvUo' /XML 'C:\Users\user\AppData\Local\Temp\tmpEBB4.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1420 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - invoice & packing.pdf.exe (PID: 4624 cmdline: C:\Users\user\Desktop\invoice & packing.pdf.exe MD5: AC3668260346D59F25905579AA8EAF94)
  - invoice & packing.pdf.exe (PID: 4668 cmdline: C:\Users\user\Desktop\invoice & packing.pdf.exe MD5: AC3668260346D59F25905579AA8EAF94)
  - invoice & packing.pdf.exe (PID: 4696 cmdline: C:\Users\user\Desktop\invoice & packing.pdf.exe MD5: AC3668260346D59F25905579AA8EAF94)
  - invoice & packing.pdf.exe (PID: 6040 cmdline: C:\Users\user\Desktop\invoice & packing.pdf.exe MD5: AC3668260346D59F25905579AA8EAF94)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.348394866.0000000003E84000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10d64d:$x1: NanoCore.ClientPluginHost • 0x13fe6d:$x1: NanoCore.ClientPluginHost • 0x10d68a:$x2: IClientNetworkHost • 0x13feaa:$x2: IClientNetworkHost • 0x1111bd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x1439dd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.348394866.0000000003E84000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.348394866.0000000003E8 4000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10d3b5:$a: NanoCore • 0x10d3c5:$a: NanoCore • 0x10d5f9:$a: NanoCore • 0x10d60d:$a: NanoCore • 0x10d64d:$a: NanoCore • 0x13fbd5:$a: NanoCore • 0x13fbe5:$a: NanoCore • 0x13fe19:$a: NanoCore • 0x13fe2d:$a: NanoCore • 0x13fe6d:$a: NanoCore • 0x10d414:$b: ClientPlugin • 0x10d616:$b: ClientPlugin • 0x10d656:$b: ClientPlugin • 0x13fc34:$b: ClientPlugin • 0x13fe36:$b: ClientPlugin • 0x13fe76:$b: ClientPlugin • 0x10d53b:$c: ProjectData • 0x13fd5b:$c: ProjectData • 0x10df42:$d: DESCrypto • 0x140762:$d: DESCrypto • 0x11590e:$e: KeepAlive
00000000.00000002.348069175.0000000002E8 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000006.00000003.361188308.00000000045C 4000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x13c2:$a: NanoCore • 0x13e7:$a: NanoCore • 0x1440:$a: NanoCore • 0x115dd:$a: NanoCore • 0x11603:$a: NanoCore • 0x1165f:$a: NanoCore • 0x1e4b4:$a: NanoCore • 0x1e50d:$a: NanoCore • 0x1e540:$a: NanoCore • 0x1e76c:$a: NanoCore • 0x1e7e8:$a: NanoCore • 0x1ee01:$a: NanoCore • 0x1ef4a:$a: NanoCore • 0x1f41e:$a: NanoCore • 0x1f705:$a: NanoCore • 0x1f71c:$a: NanoCore • 0x24cba:$a: NanoCore • 0x24d34:$a: NanoCore • 0x298d1:$a: NanoCore • 0x2ac8b:$a: NanoCore • 0x2acd5:$a: NanoCore
Click to see the 3 entries				

Sigma Overview

System Summary:

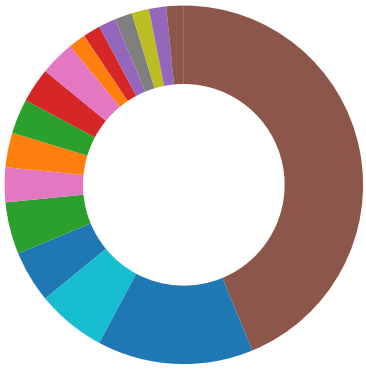
Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Suspicious Double Extension

Signature Overview

- AV Detection
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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



Click to jump to signature section

AV Detection:

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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)

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

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:

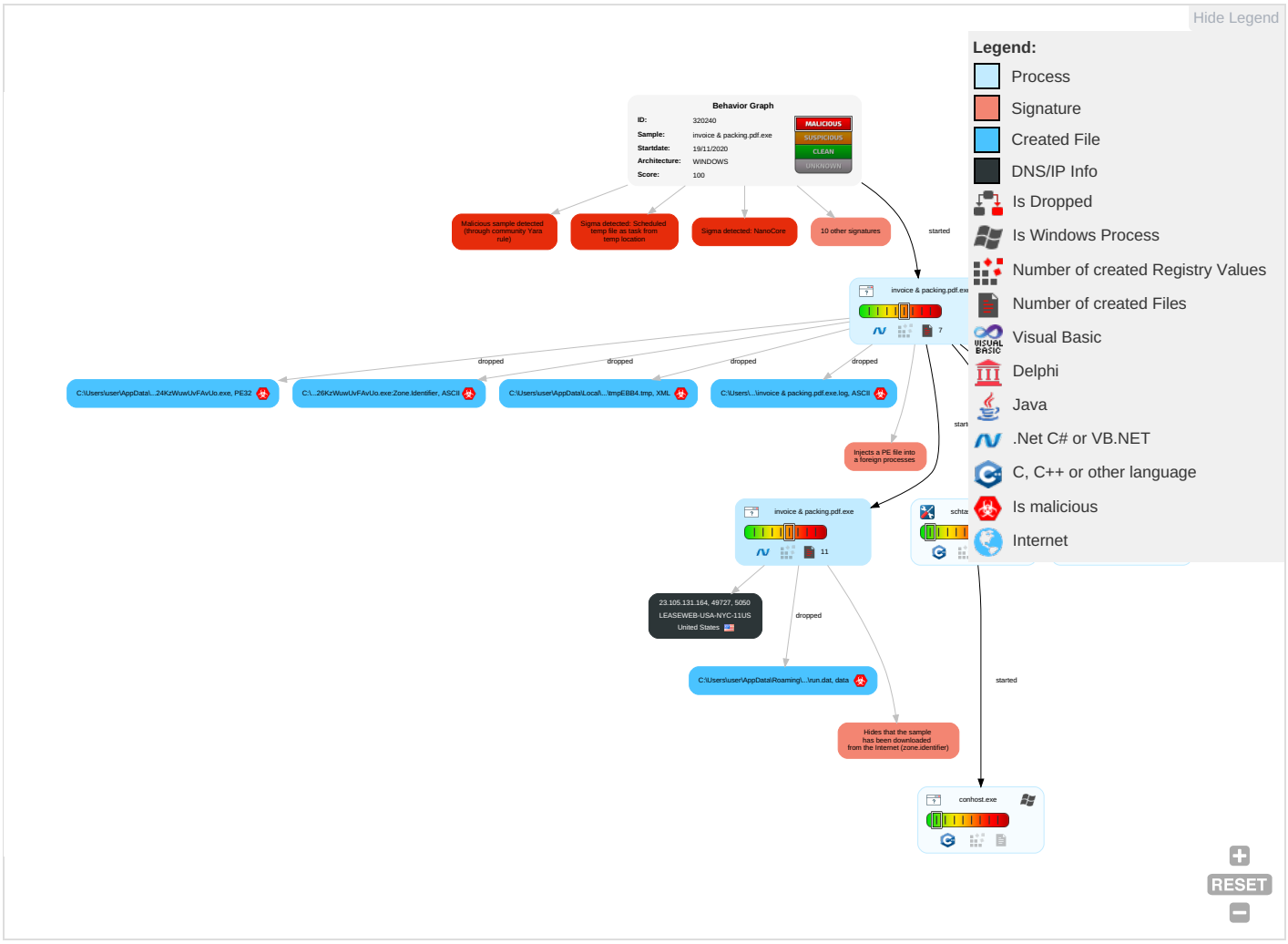
Detected Nanocore Rat

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 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comi
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Archive Collected Data 1	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	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Process 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	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devic Comi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Account Discovery 1	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 1 3	DCSync	System Owner/User Discovery 1	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	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 2	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

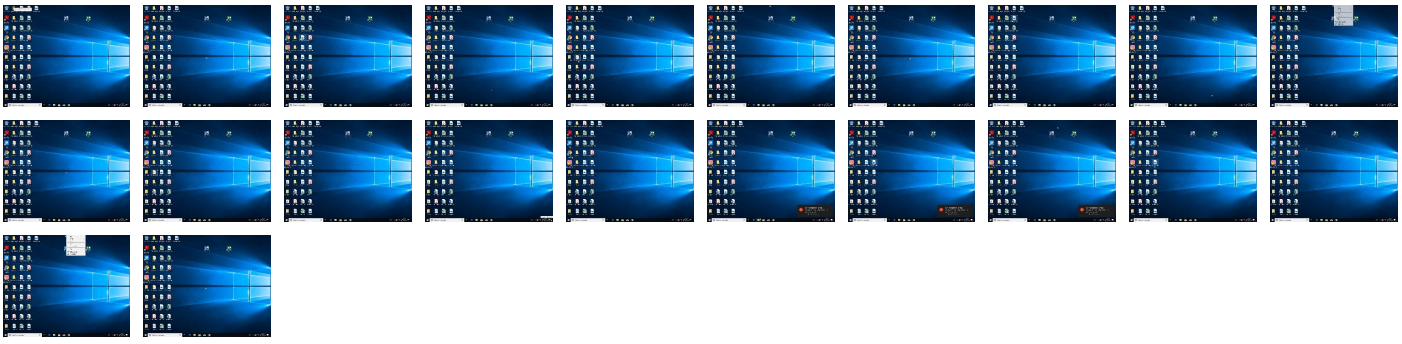
Behavior Graph



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 & packing.pdf.exe	8%	ReversingLabs		
invoice & packing.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NKzWuwUvFAvUo.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\NKzWuwUvFAvUo.exe	8%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

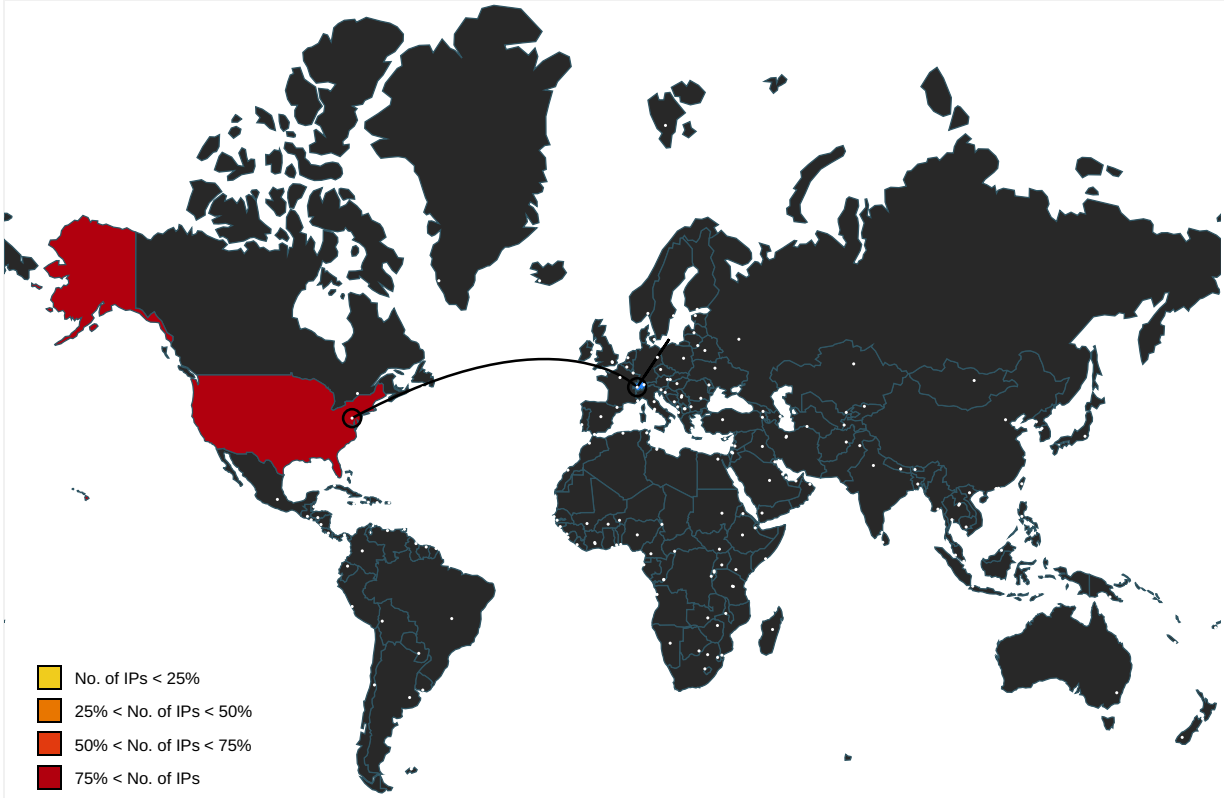
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320240
Start date:	19.11.2020
Start time:	07:46:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoice & packing.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:	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@12/8@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.2% (good quality ratio 0.8%) • Quality average: 44.3% • Quality standard deviation: 33.7%
HCA Information:	• Successful, ratio: 98% • 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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:47:23	API Interceptor	966x Sleep call for process: invoice & packing.pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TDToxqrclL.exe	Get hash	malicious	Browse	• 23.105.131.177
	Ziiq5tl3CT.exe	Get hash	malicious	Browse	• 23.105.131.239
	f3wo2FuLN6.exe	Get hash	malicious	Browse	• 192.253.24 6.143
	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	• 192.253.24 6.138
	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	• 192.253.24 6.138
	TLpMnhJmg7.exe	Get hash	malicious	Browse	• 192.253.24 6.143
	HDyADDol3I.exe	Get hash	malicious	Browse	• 192.253.24 6.143
	11.exe	Get hash	malicious	Browse	• 173.234.15 5.145
	53C29QAJnd.exe	Get hash	malicious	Browse	• 173.234.15 5.145

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\invoice & packing.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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..

C:\Users\user\AppData\Local\Temp\tmpEBB4.tmp

Process:	C:\Users\user\Desktop\invoice & packing.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.169644445225677
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3altn:cbha7JlNQV/rydbz9l3YODOLNdq39
MD5:	8C54517939B406C8DAE32AD5439E85E4
SHA1:	F9C0D812F35D6498238989DFD5BF7469059632F8
SHA-256:	3B9BA204CF8DC26B7BE6F46EEDCDCA0D9DF4E156B4A57DB3647D998528CB871E

C:\Users\user\AppData\Local\Temp\tmpEBB4.tmp	
SHA-512:	795C7DE27586546AF789B9FFD53F891E70586DE2A5DCAE66328A8A6185739F69CC2C5B9BAC7AA0D8823160BCF2572ADC9AA548E7D9415A44EE33BF3C91EBE95
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>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\invoice & packing.pdf.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\invoice & packing.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:UHh:m
MD5:	8F8822F0459769C3D4C8BBD6B94685D1
SHA1:	4403B5ABEB290502AA1CD8A297D7A22AEEFC618C
SHA-256:	9380CC30AE6D7AE544EEFBDD8929DD26AF5BB425CAA97E7688C313F069098687
SHA-512:	5305B6872A18CF0EC3350E702D14AF9C9D908CBCD57F9274AD0D08A5514AE08DE21DCFD61EEF854AEB494E579B40D4892EB09B2DDF3500196DA8284DD983DA9
Malicious:	**true**
Reputation:	low
Preview:	..*k...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\invoice & packing.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}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\invoice & packing.pdf.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..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=.....L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`'].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!.;.^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\NKzWuwUvFAvUo.exe	
Process:	C:\Users\user\Desktop\invoice & packing.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	590336
Entropy (8bit):	7.810863680136923
Encrypted:	false
SSDEEP:	12288:h5k/J+UIdk23WCfofAeGD2TmPsaMj7Yx960yBHXoauQ2YwhOTHo:hfUIdkSWCQfAebiPZY7Ye9ZXzKD8
MD5:	AC3668260346D59F25905579AA8EAF94
SHA1:	479C7E0B3696F174E13D59AE04353205B9A3203D
SHA-256:	3F746FA6F84B842F03679244794C7F16F4497FB2FB8EB770539A7BBD3110E9E9
SHA-512:	1F7B0571BDD36F119EE7CC7A2D578C337E6BB9D092EA29E15C4C10A49BB6A0C95BEDBACF4F460815307585ECA9D02F249D9738B645F5BA8CBC4A9F502C7A8 55
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 8%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....D....."... .....@.. .....`..... .@.....O.....pA.....@..... ..... ..H.....text...(.... ..... ..`.rsrc...pA.....B.....@..@.relo c.....@.....@..B.....H.....x{..X_.....0.....(....(.....(.....o....*.....(.....(.....(!.....("....(#....*N..(....oD... ($....*&..(%....*.s&.....s'.....s(.....s).....s*.....*....0.....~....o+....+..*.0.....~....o,...+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0..<.....~..... (0.....,!r...p.....(1...o2...s3.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\NKzWuwUvFAvUo.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\invoice & packing.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

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

General

Entropy (8bit):	7.810863680136923
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 & packing.pdf.exe
File size:	590336
MD5:	ac3668260346d59f25905579aa8eaf94
SHA1:	479c7e0b3696f174e13d59ae04353205b9a3203d
SHA256:	3f746fa6f84b842f03679244794c7f16f4497fb2fb8eb770539a7bbd3110e9e9
SHA512:	1f7b0571bdd36f119ee7cc7a2d578c337e6bb9d092ea29e15c4c10a49bb6a0c95bedbacf4f460815307585eca9d02f249d9738b645f5ba8cbc4a9f502c7a8b55
SSDEEP:	12288:h5k/J+UIdk23WCfofAeGD2TmPsaMj7Yx960yBHXoauQ2YwhOTHo:hfUIdkSWCQfAebiPZY7Ye9ZXzKD8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ._.....P.....D....."... .....@.. .....`.....@.....

File Icon

Icon Hash:	f8c492aaaa92dcfe

Static PE Info

General

Entrypoint:	0x48db22
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:	0x5FB5CEE5 [Thu Nov 19 01:48:21 2020 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

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
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	0x8dad0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8e000	0x4170	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x94000	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	0x8bb28	0x8bc00	False	0.877744507491	data	7.83069798608	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8e000	0x4170	0x4200	False	0.503255208333	data	5.47730162147	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x94000	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	0x8e190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x8e5f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4275388049, next used block 4258479509		
RT_ICON	0x8f6a0	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	0x91c48	0x30	data		
RT_VERSION	0x91c78	0x30c	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x91f84	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 2014
Assembly Version	1.0.0.0
InternalName	gSqi.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Blackjack
ProductVersion	1.0.0.0
FileDescription	Blackjack
OriginalFilename	gSqi.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 07:47:30.474591970 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:30.792576075 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:30.792745113 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:30.823401928 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:31.155839920 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:31.167666912 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:31.486973047 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:31.489686012 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:31.849564075 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:31.849776030 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.215687990 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.234042883 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.240955114 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.241173983 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.246521950 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.252232075 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.252499104 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.260375977 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.265594006 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.265743971 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.270591974 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.274962902 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.275067091 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.283077002 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.289684057 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.289827108 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.577071905 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.581955910 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.582199097 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.586194992 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.591187954 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.591351032 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.598623991 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.602005005 CET	5050	49727	23.105.131.164	192.168.2.6

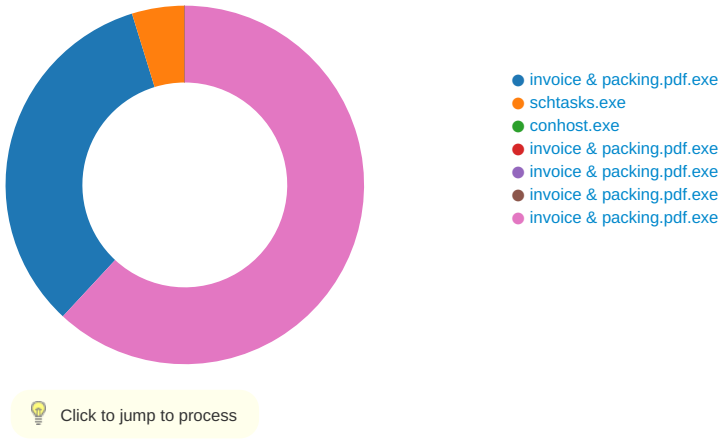
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 07:47:32.602191925 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.605751038 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.612010956 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.612185955 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.618050098 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.623076916 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.623183966 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.627986908 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.633099079 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.633234024 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.637991905 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.642129898 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.642303944 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.646337032 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.658047915 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.658168077 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.658176899 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.660998106 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.661154032 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.664242983 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.670133114 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.670347929 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.903955936 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.908914089 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.909184933 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.915057898 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.918975115 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.919220924 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.925088882 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.930382013 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.930627108 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.936024904 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.941917896 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.942300081 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.947257042 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.952514887 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.952651978 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.956017971 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.960462093 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.960736036 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.964013100 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.970436096 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.970541000 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.974679947 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.977952957 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.978094101 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.981884003 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.985008955 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.985115051 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.987893105 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.990993977 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.991130114 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.992677927 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.996151924 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:32.996345997 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:32.999043941 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:33.002943993 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:33.003117085 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:33.005810976 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:33.009715080 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:33.009891033 CET	49727	5050	192.168.2.6	23.105.131.164
Nov 19, 2020 07:47:33.013971090 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:33.017862082 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:33.018131971 CET	49727	5050	192.168.2.6	23.105.131.164

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 07:47:33.021931887 CET	5050	49727	23.105.131.164	192.168.2.6
Nov 19, 2020 07:47:33.025867939 CET	5050	49727	23.105.131.164	192.168.2.6

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: invoice & packing.pdf.exe PID: 7160 Parent PID: 5952

General

Start time:	07:47:22
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\invoice & packing.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\invoice & packing.pdf.exe'
Imagebase:	0x790000
File size:	590336 bytes
MD5 hash:	AC3668260346D59F25905579AA8EAF94
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: 00000000.00000002.348394866.0000000003E84000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.348394866.0000000003E84000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.348394866.0000000003E84000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.348069175.0000000002E81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.348133021.0000000002ED7000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\NKzWuwUvFAvUo.exe	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	DFBEE8	CopyFileW
C:\Users\user\AppData\Roaming\NKzWuwUvFAvUo.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	DFBEE8	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEBB4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	55A07D8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoice & packing.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEBB4.tmp	success or wait	1	55A0DAA	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\NKzWuwUvFAvUo.exe	0	262144	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 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 e5 ce b5 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 bc 08 00 00 44 00 00 00 00 00 00 22 db 08 00 00 20 00 00 00 e0 08 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 60 09 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....P......D......".... ....@.. ....` ....@................	success or wait	3	DFBEE8	CopyFileW
C:\Users\user\AppData\Roaming\NKzWuwUvFAvUo.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	DFBEE8	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEBB4.tmp	unknown	1658	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 65 6e 67 69 6e 65 65 72 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	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registratio	success or wait	1	55A0A67	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoice & packing.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 69 63 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	7328A33A	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: schtasks.exe PID: 1560 Parent PID: 7160

General

Start time:	07:47:24
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NKzWuwUvFAvUo' /XML 'C:\Users\user\AppData\Local\Temp\tmpEBB4.tmp'
Imagebase:	0xa70000
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\tmpEBB4.tmp	unknown	2	success or wait	1	A7AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpEBB4.tmp	unknown	1659	success or wait	1	A7ABD9	ReadFile

Analysis Process: conhost.exe PID: 1420 Parent PID: 1560

General

Start time:	07:47:25
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: invoice & packing.pdf.exe PID: 4624 Parent PID: 7160

General

Start time:	07:47:25
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\invoice & packing.pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\invoice & packing.pdf.exe
Imagebase:	0x370000
File size:	590336 bytes
MD5 hash:	AC3668260346D59F25905579AA8EAF94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: invoice & packing.pdf.exe PID: 4668 Parent PID: 7160

General

Start time:	07:47:25
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\invoice & packing.pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\invoice & packing.pdf.exe
Imagebase:	0x3d0000
File size:	590336 bytes
MD5 hash:	AC3668260346D59F25905579AA8EAF94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: invoice & packing.pdf.exe PID: 4696 Parent PID: 7160

General

Start time:	07:47:26
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\invoice & packing.pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\invoice & packing.pdf.exe
Imagebase:	0x20000
File size:	590336 bytes
MD5 hash:	AC3668260346D59F25905579AA8EAF94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: invoice & packing.pdf.exe PID: 6040 Parent PID: 7160

General

Start time:	07:47:26
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\invoice & packing.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\invoice & packing.pdf.exe
Imagebase:	0xa30000
File size:	590336 bytes
MD5 hash:	AC3668260346D59F25905579AA8EAF94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000006.00000003.361188308.00000000045C4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.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	72FB60AC	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	72FB60AC	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	52D07A1	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	52D089B	CreateFileW

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	72FB60AC	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	72FB60AC	unknown
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	52D07A1	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	52D07A1	CreateDirectoryW
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	52D089B	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	52D089B	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	52D089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\invoice & packing.pdf.exe:Zone.Identifier	success or wait	1	52D0D41	DeleteFileA

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	cb 7f 2a 6b a2 8c d8 48	..*k...H	success or wait	1	52D0A53	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	52D0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	52D0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 85 16 f4 a5 20 38 a2 6a 80 a4 a3 f3 7c 88 26 58 b6 ca 65 a6 46 b8 2a 80	9iH....}Z..4..f..... 8.j....|. &X..e.F.*.	success or wait	1	52D0A53	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	52D0A53	ReadFile
C:\Users\user\Desktop\invoice & packing.pdf.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\invoice & packing.pdf.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	52D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	52D0A53	ReadFile

Disassembly

Code Analysis