ID: 338164
Sample Name: New Order 54380 pdf.exe
Cookbook: default.jbs
Time: 18:48:15
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

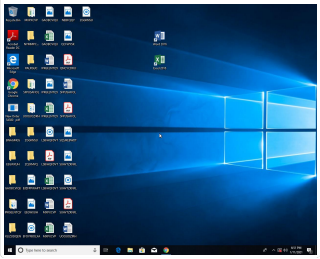
Analysis Report New Order 54380 pdf.exe

Overview

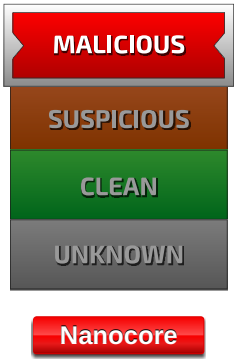
General Information

Sample Name:	New Order 54380 pdf.exe
Analysis ID:	338164
MD5:	e7192b48a761bb..
SHA1:	b4e6b76ebfe6b04.
SHA256:	db51bcbfe40ce22..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

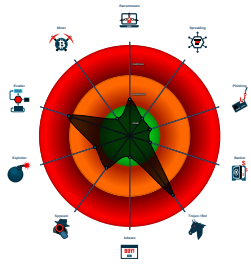


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected Nanocore RAT
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Contains capabilities to detect virtua…
- Contains long sleeps (>= 3 min)
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Creates a start menu entry (Start Me…
- Creates processes with suspicious n…

Classification



Startup

- **System is w10x64**
- New Order 54380 pdf.exe (PID: 6344 cmdline: 'C:\Users\user\Desktop\New Order 54380 pdf.exe' MD5: E7192B48A761BBC49DA028723E08889C)
  - a.exe (PID: 6740 cmdline: 'C:\Users\user\AppData\Roaming\a.exe' MD5: E7192B48A761BBC49DA028723E08889C)
- a.exe (PID: 6808 cmdline: 'C:\Users\user\AppData\Roaming\a.exe' MD5: E7192B48A761BBC49DA028723E08889C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

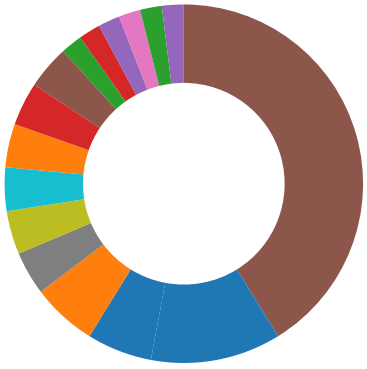
Source	Rule	Description	Author	Strings
00000000.00000002.270686743.000000000474 4000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x43787:$x1: NanoCore.ClientPluginHost • 0x76347:$x1: NanoCore.ClientPluginHost • 0xa8ef7:$x1: NanoCore.ClientPluginHost • 0x437c4:$x2: IClientNetworkHost • 0x76384:$x2: IClientNetworkHost • 0xa8f34:$x2: IClientNetworkHost • 0x472f7:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x79eb7:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xaca67:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.270686743.000000000474 4000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.270686743.000000000474 4000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x434ef:$a: NanoCore • 0x434ff:$a: NanoCore • 0x43733:$a: NanoCore • 0x43747:$a: NanoCore • 0x43787:$a: NanoCore • 0x760af:$a: NanoCore • 0x760bf:$a: NanoCore • 0x762f3:$a: NanoCore • 0x76307:$a: NanoCore • 0x76347:$a: NanoCore • 0xa8c5f:$a: NanoCore • 0xa8c6f:$a: NanoCore • 0xa8ea3:$a: NanoCore • 0xa8eb7:$a: NanoCore • 0xa8ef7:$a: NanoCore • 0x4354e:$b: ClientPlugin • 0x43750:$b: ClientPlugin • 0x43790:$b: ClientPlugin • 0x7610e:$b: ClientPlugin • 0x76310:$b: ClientPlugin • 0x76350:$b: ClientPlugin
00000000.00000002.270957926.000000000484 2000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10637:$x1: NanoCore.ClientPluginHost • 0x431e5:$x1: NanoCore.ClientPluginHost • 0x10674:$x2: IClientNetworkHost • 0x43222:$x2: IClientNetworkHost • 0x141a7:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x46d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.270957926.000000000484 2000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

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

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

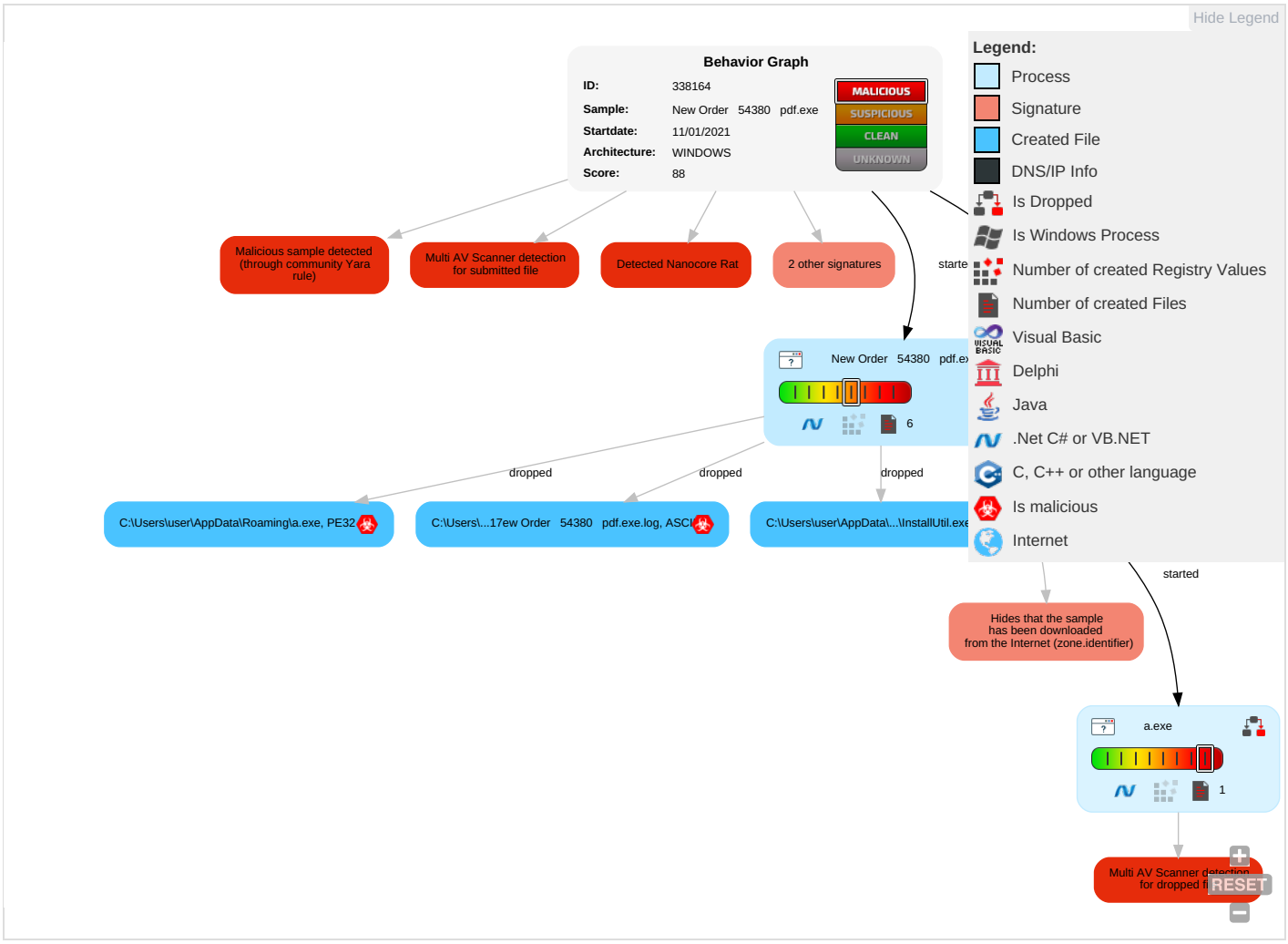
Detected Nanocore Rat

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	Network Effects
Valid Accounts	Windows Management Instrumentation	Startup Items 1	Startup Items 1	Masquerading 1	Input Capture 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 2	Process Injection 1 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 2	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
New Order 54380 pdf.exe	28%	Virustotal		Browse
New Order 54380 pdf.exe	17%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\a.exe	28%	Virustotal		Browse
C:\Users\user\AppData\Roaming\a.exe	17%	ReversingLabs	Win32.Trojan.Generic	

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

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338164
Start date:	11.01.2021
Start time:	18:48:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Order 54380 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:	25
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:	mal88.troj.evad.winEXE@4/6@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 1.3%) • Quality average: 66.6% • Quality standard deviation: 28.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • 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. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:49:12	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.lnk

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	6hE7zSMErZ.exe	Get hash	malicious	Browse	
	Invoice - Payment_Advice_pdf.exe	Get hash	malicious	Browse	
	DSj7ak0N6l.exe	Get hash	malicious	Browse	
	QWP-0716.xls.exe	Get hash	malicious	Browse	
	QPI-01458.exe	Get hash	malicious	Browse	
	01gVXUhwxO.exe	Get hash	malicious	Browse	
	Payment Copy.exe	Get hash	malicious	Browse	
	AWBDQfjfh8.exe	Get hash	malicious	Browse	
	iuu4DJ67MC.exe	Get hash	malicious	Browse	
	ORDER-02044.exe	Get hash	malicious	Browse	
	New Order pdf.exe	Get hash	malicious	Browse	
	NEW SC #ORDER.exe	Get hash	malicious	Browse	
	New Order 7320 PDF.exe	Get hash	malicious	Browse	
	PAYMENT COPY.exe	Get hash	malicious	Browse	
	Request.exe	Get hash	malicious	Browse	
	a2PdLccwuz.exe	Get hash	malicious	Browse	
	PO456789.exe	Get hash	malicious	Browse	
	31.exe	Get hash	malicious	Browse	
	ORDER FORM DENK.exe	Get hash	malicious	Browse	
	niMONOdcTZ.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order 54380 pdf.exe.log	
Process:	C:\Users\user\Desktop\New Order 54380 pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order 54380 pdf.exe.log	
Size (bytes):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895E ABB
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	
Process:	C:\Users\user\AppData\Roaming\a.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1362
Entropy (8bit):	5.343186145897752
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovj
MD5:	1249251E90A1C28AB8F7235F30056DEB
SHA1:	166BA6B64E9B0D9BA7B856334F7D7EC027030BA1
SHA-256:	B5D65BF3581136CD5368BC47FA3972E06F526EED407BC6571D11D9CD4B5C4D83
SHA-512:	FD880C5B12B22241F67139ABD09B99ACE7A4DD24635FC6B340A3E7C463E2AEF3FA68EF647352132934BC1F8CA134F46064049449ACB67954BEDDEA9AA967088
Malicious:	false
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\New Order 54380 pdf.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Joe Sandbox View:	• Filename: 6hE7zSMErZ.exe, Detection: malicious, Browse • Filename: Invoice - Payment_Advice_pdf.exe, Detection: malicious, Browse • Filename: DSj7ak0N6I.exe, Detection: malicious, Browse • Filename: QWP-0716.xls.exe, Detection: malicious, Browse • Filename: QPI-01458.exe, Detection: malicious, Browse • Filename: 01gVXUhwxO.exe, Detection: malicious, Browse • Filename: Payment Copy.exe, Detection: malicious, Browse • Filename: AWBDQfjfh8.exe, Detection: malicious, Browse • Filename: iuu4DJ67MC.exe, Detection: malicious, Browse • Filename: ORDER-02044.exe, Detection: malicious, Browse • Filename: New Order pdf.exe, Detection: malicious, Browse • Filename: NEW SC #ORDER.exe, Detection: malicious, Browse • Filename: New Order 7320 PDF.exe, Detection: malicious, Browse • Filename: PAYMENT COPY.exe, Detection: malicious, Browse • Filename: Request.exe, Detection: malicious, Browse • Filename: a2PdLccwuz.exe, Detection: malicious, Browse • Filename: PO456789.exe, Detection: malicious, Browse • Filename: 31.exe, Detection: malicious, Browse • Filename: ORDER FORM DENK.exe, Detection: malicious, Browse • Filename: niMONOdcTZ.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".J.....lm.....o.....2~.....o...*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... ....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.lnk	
Process:	C:\Users\user\Desktop\New Order 54380 pdf.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	874
Entropy (8bit):	3.0690696428127464
Encrypted:	false
SSDEEP:	12:8wl0tsXMlykXG/tz0/CSLmWqkXg1MJkHg/CNfBn/v4t2Y+xIBjK:8erxWLhqo+M2Fd7aB
MD5:	0312823243A664EEA0071DDF9C7B403C
SHA1:	DC983848A10950AC95DDB5350D981A8A6BCBAF3B
SHA-256:	D714BF9FD71CFCD5E9D6D9C132972821882FADA03A1BFBB66AB5654287ED2B10
SHA-512:	AB0B09CD0F34B09DA800634D0396F964E265F15B20E458215DA236BE4918A6AF3244A564B70CA9F0D3728BD2BFF319487FD2B1CD213E923C4842BF1D360C607
Malicious:	false
Reputation:	low
Preview:	L.....F.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....\.1.....user.D..... .....f.r.o.n.t.d.e.s.k.....V.1.....AppData.@.....A.p.p.D.a.t.a.....V.1.....Roaming.@.....R.o.a.m.i.n.g.....P. 2.....a.exe.<.....a...e.x.e.....\.....\.....\.....\.....\.a...e.x.e.(.C.:.\.U.s.e.r.s.\.f.r.o.n.t.d.e.s.k.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.a...e.x.e. .....>.e.L.:...er.=.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Roaming\a.exe	
Process:	C:\Users\user\Desktop\New Order 54380 pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	902144
Entropy (8bit):	5.721140644960939
Encrypted:	false
SSDEEP:	12288:/ljnDvY0D720EcNj6usUEfTvc8ol7uwtCEWY:/pDvY0vpEcNjJEfTk3PWY
MD5:	E7192B48A761BBC49DA028723E08889C
SHA1:	B4E6B76EBFE6B0497AA456C7CAC2B31FE54D3B8C
SHA-256:	DB51BCBFE40CE228CAE597A42C2DD1906BC04FAE69A1BBE75653F6FEEB923E41
SHA-512:	842B0EF943A56113154964F41A8B30A7A4771E3EC9F5D70298539190FBA7D3F092A928765F52399A9D2E1864EAB2FEC96C83885EBC1F0A4ED2A4EA8B2B60F049
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 28%, Browse • Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. ....`.....S..... ..... ..H.....text...$.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....@....*.....V....I..&c.....&..(.....*.s.....s.....s.....s .....*&.....*"".....*Vs/...(2...t.....*..(3...*..(....*....(I.. ..*^.....(C...t....o^....*..(D...*....0...../.....-t..(0...t....(0...t.....&.....@..... .hR.....(9...t.....-.....(0...t.....(0...t/...-..... ....(9...t....&+.....-...!&..... ...J %...(

C:\Users\user\AppData\Roaming\a.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\New Order 54380 pdf.exe

C:\Users\user\AppData\Roaming\a.exe:Zone.Identifier	
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:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.721140644960939
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	New Order 54380 pdf.exe
File size:	902144
MD5:	e7192b48a761bbc49da028723e08889c
SHA1:	b4e6b76ebfe6b0497aa456c7cac2b31fe54d3b8c
SHA256:	db51bcbfe40ce228cae597a42c2dd1906bc04fae69a1bbe75653f6feeb923e41
SHA512:	842b0ef943a56113154964f41a8b30a7a4771e3ec9f5d70298539190fba7d3f092a928765f52399a9d2e1864eab2fec96c83885ebc1f0a4ed2a4ea8b2b60f049
SSDEEP:	12288:/ljnDvY0D720EcNj6usUEfTvc8ol7uwtCEWY:/pDvY0vpEcNjJEfTk3PWY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. ....` .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4dd71e
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, HIGH_ENTROPY_VA
Time Stamp:	0xF8B858C [Fri Apr 7 12:58:52 1978 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

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	0xdd6c8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xde000	0x68a	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe0000	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	0xdb724	0xdb800	False	0.504631442198	data	5.72644571098	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xde000	0x68a	0x800	False	0.3681640625	data	3.82080882615	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xde0a0	0x400	data		
RT_MANIFEST	0xde4a0	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 2017 F;:E48:5?@C8>HHB54ACD@GA
Assembly Version	1.0.0.0
InternalName	New Order 54380 pdf.exe
FileVersion	9.14.18.23
CompanyName	F;:E48:5?@C8>HHB54ACD@GA
Comments	A24FH=7>CH9B8>6@C<@=
ProductName	G63@F<BB:9@:FAGF?5;7J5EI
ProductVersion	9.14.18.23
FileDescription	G63@F<BB:9@:FAGF?5;7J5EI
OriginalFilename	New Order 54380 pdf.exe

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

● New Order 54380 pdf.exe
● a.exe

System Behavior

Analysis Process: New Order 54380 pdf.exe PID: 6344 Parent PID: 5692

General

Start time:	18:49:05
Start date:	11/01/2021
Path:	C:\Users\user\Desktop\New Order 54380 pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New Order 54380 pdf.exe'
Imagebase:	0x8f0000
File size:	902144 bytes
MD5 hash:	E7192B48A761BBC49DA028723E08889C
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: 00000000.00000002.270686743.0000000004744000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.270686743.0000000004744000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.270686743.0000000004744000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.270957926.0000000004842000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.270957926.0000000004842000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.270957926.0000000004842000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\InstallUtil.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	2D7C423	CopyFileExW
C:\Users\user\AppData\Roaming\a.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	2D7C423	CopyFileExW
C:\Users\user\AppData\Roaming\a.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2D7C423	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order 54380 pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0	41064	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 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 07 5a 8e 5a 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 86 72 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 9a 80 01 00 03 00 60 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....Z.Z.......... ....0..T...........r... ....@.. ....`................	success or wait	1	2D7C423	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\a.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 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 8c 85 8b 0f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 b8 0d 00 00 0a 00 00 00 00 00 00 1e d7 0d 00 00 20 00 00 00 e0 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 0e 00 00 02 00 00 00 00 00 00 02 00 60 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................. ....@.. ....`................	success or wait	4	2D7C423	CopyFileExW
C:\Users\user\AppData\Roaming\a.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	2D7C423	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order 54380 pdf.exe.log	unknown	1451	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=	success or wait	1	6D6AC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D375705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D37CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D2D03DE	ReadFile

Analysis Process: a.exe PID: 6740 Parent PID: 6344

General

Start time:	18:49:19
Start date:	11/01/2021
Path:	C:\Users\user\AppData\Roaming\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\a.exe'
Imagebase:	0x930000
File size:	902144 bytes
MD5 hash:	E7192B48A761BBC49DA028723E08889C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 28%, Virustotal, Browse • Detection: 17%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6AC78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	unknown	1362	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=	success or wait	1	6D6AC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D375705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D37CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D2D03DE	ReadFile

Analysis Process: a.exe PID: 6808 Parent PID: 3292

General

Start time:	18:49:21
Start date:	11/01/2021
Path:	C:\Users\user\AppData\Roaming\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\a.exe'
Imagebase:	0x2c0000
File size:	902144 bytes
MD5 hash:	E7192B48A761BBC49DA028723E08889C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D375705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D37CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D2D03DE	ReadFile

Disassembly

Code Analysis