ID: 345061
Sample Name: Dintec Order PDF.exe
Cookbook: default.jbs
Time: 16:43:19
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

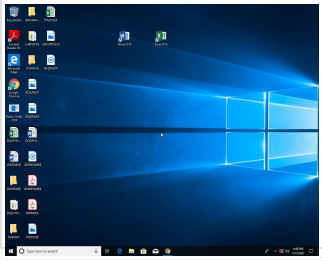
Analysis Report Dintec Order PDF.exe

Overview

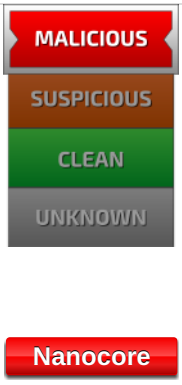
General Information

Sample Name:	Dintec Order PDF.exe
Analysis ID:	345061
MD5:	98e3c2ac1efdd99..
SHA1:	d3ce076af7b45e1.
SHA256:	d09ed1437134f7e.
Tags:	exe NanoCore

Most interesting Screenshot:



Detection



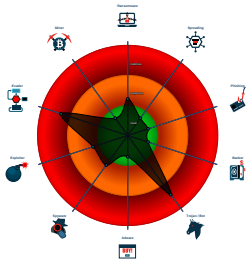
Nanocore

Score:	100
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 AntiVM_3
- Yara detected Nanocore RAT
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Contains capabilities to detect virtua…
- Contains long sleeps (>= 3 min)

Classification



Startup

- **System is w10x64**
- Dintec Order PDF.exe (PID: 3480 cmdline: 'C:\Users\user\Desktop\Dintec Order PDF.exe' MD5: 98E3C2AC1EFDD997B05A1FEE872630EC)
  - a.exe (PID: 984 cmdline: 'C:\Users\user\AppData\Roaming\a.exe' MD5: 98E3C2AC1EFDD997B05A1FEE872630EC)
- a.exe (PID: 6648 cmdline: 'C:\Users\user\AppData\Roaming\a.exe' MD5: 98E3C2AC1EFDD997B05A1FEE872630EC)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

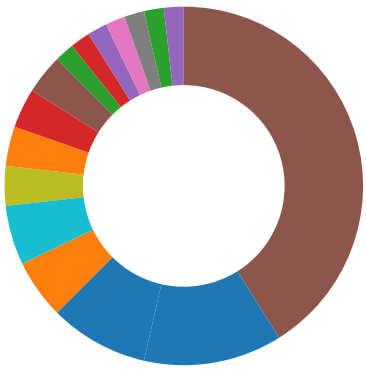
Source	Rule	Description	Author	Strings
00000001.00000002.681613074.000000000403 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x109b7:$x1: NanoCore.ClientPluginHost • 0x4359d:$x1: NanoCore.ClientPluginHost • 0x109f4:$x2: IClientNetworkHost • 0x435da:$x2: IClientNetworkHost • 0x14527:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4710d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.681613074.000000000403 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.681613074.000000000403 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1071f:$a: NanoCore • 0x1072f:$a: NanoCore • 0x10963:$a: NanoCore • 0x10977:$a: NanoCore • 0x109b7:$a: NanoCore • 0x43305:$a: NanoCore • 0x43315:$a: NanoCore • 0x43549:$a: NanoCore • 0x4355d:$a: NanoCore • 0x4359d:$a: NanoCore • 0x1077e:$b: ClientPlugin • 0x10980:$b: ClientPlugin • 0x109c0:$b: ClientPlugin • 0x43364:$b: ClientPlugin • 0x43566:$b: ClientPlugin • 0x435a6:$b: ClientPlugin • 0x108a5:$c: ProjectData • 0x4348b:$c: ProjectData • 0x112ac:$d: DESCrypto • 0x43e92:$d: DESCrypto • 0x18c78:$e: KeepAlive
00000001.00000002.681348992.0000000003E9 B000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xdba07:$x1: NanoCore.ClientPluginHost • 0x10e607:$x1: NanoCore.ClientPluginHost • 0x1411f7:$x1: NanoCore.ClientPluginHost • 0xdba44:$x2: IClientNetworkHost • 0x10e644:$x2: IClientNetworkHost • 0x141234:$x2: IClientNetworkHost • 0xdf577:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x112177:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x144d67:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.681348992.0000000003E9 B000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- 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

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

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)

Malware Analysis System Evasion:

Yara detected AntiVM_3

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

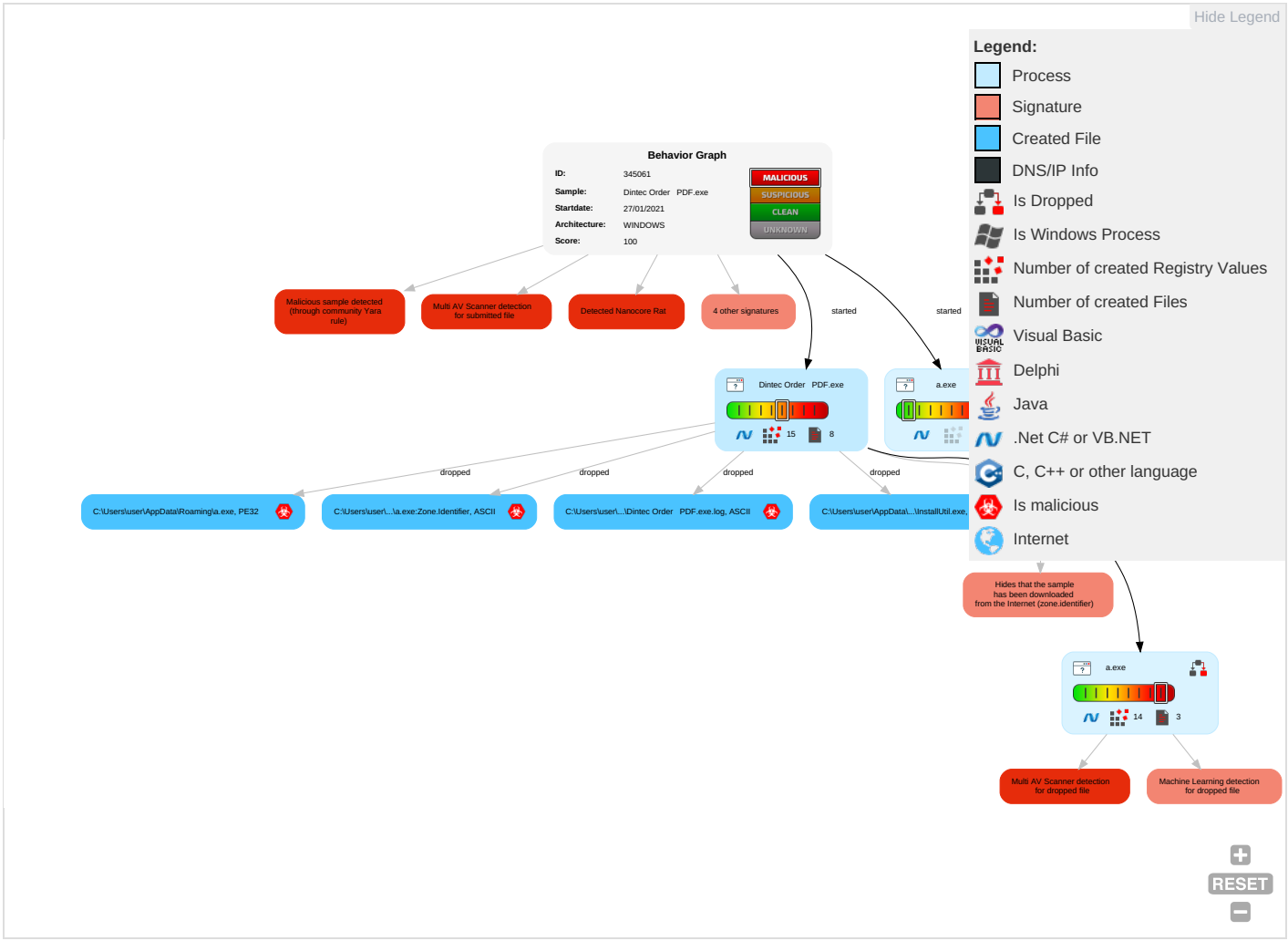
Yara detected Nanocore RAT

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	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 2	Process Injection 1 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Data from Removable Media	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	Virtualization/Sandbox Evasion 3	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	Process 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	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

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
Dintec Order PDF.exe	42%	Virustotal		Browse
Dintec Order PDF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\a.exe	100%	Joe Sandbox ML		
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	42%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.adb	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adb	Dintec Order PDF.exe, 00000001.00000003.647767848.00000008201000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	Dintec Order PDF.exe, 00000001.00000002.680577443.00000025AA000.00000004.00000001.sdmp, a.exe, 00000002.00000002.685914222.0000000000A0E000.00000004.00000020.sdmp, a.exe, 00000003.00000002.687185207.00000000025DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	Dintec Order PDF.exe, 00000001.00000002.685200737.00000008212000.00000004.00000001.sdmp, Dintec Order PDF.exe, 00000001.00000003.647767848.000000008201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pki.goog/gsr2/gsr2.crl0?	Dintec Order PDF.exe, 00000001.00000002.680271086.00000000 00951000.00000004.00000020.sdmp, a.exe, 00000002.00000002.685914222.0000000000A0E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	Dintec Order PDF.exe, 00000001.00000002.680271086.00000000 00951000.00000004.00000020.sdmp, a.exe, 00000002.00000002.685914222.0000000000A0E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	Dintec Order PDF.exe, 00000001.00000002.680271086.00000000 00951000.00000004.00000020.sdmp, a.exe, 00000002.00000002.685914222.0000000000A0E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	Dintec Order PDF.exe, 00000001.00000002.685200737.00000000 08212000.00000004.00000001.sdmp, Dintec Order PDF.exe, 00000001.00000003.647767848.000000000820100 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	Dintec Order PDF.exe, 00000001.00000002.680577443.00000000 025AA000.00000004.00000001.sdmp, a.exe, 00000002.00000002.685914222.0000000000A0E000.00000004.00000020.sdmp, a.exe, 00000003.00000002.687185207.00000000025DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Dintec Order PDF.exe, 00000001.00000002.680463344.00000000 02541000.00000004.00000001.sdmp, a.exe, 00000002.00000002.686284355.00000000025BB000.00000004.00000001.sdmp, a.exe, 00000003.00000002.686878655.000000000257B000.00000004.00000001.sdmp	false		high
http://schema.org/WebPage	a.exe, 00000002.00000002.686386684.000000000261A000.00000004.00000001.sdmp, a.exe, 00000003.00000002.687185207.00000000025DA000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	Dintec Order PDF.exe, 00000001.00000002.680577443.00000000 025AA000.00000004.00000001.sdmp, a.exe, 00000002.00000002.685914222.0000000000A0E000.00000004.00000020.sdmp, a.exe, 00000003.00000002.687185207.00000000025DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1	Dintec Order PDF.exe, 00000001.00000002.685200737.00000000 08212000.00000004.00000001.sdmp, Dintec Order PDF.exe, 00000001.00000003.647767848.000000000820100 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345061
Start date:	27.01.2021
Start time:	16:43:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	Dintec Order 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:	19
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@4/6@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.2% (good quality ratio 2.3%) • Quality average: 29.9% • Quality standard deviation: 33.7%
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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.147.198.201, 172.217.23.68, 172.217.23.36, 51.11.168.160, 92.123.180.163, 92.123.180.153, 52.155.217.156, 20.54.26.129, 67.26.81.254, 8.241.11.254, 8.241.11.126, 67.27.158.126, 8.248.141.254, 51.104.144.132 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • 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
16:44:12	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.lnk
16:44:21	API Interceptor	1x Sleep call for process: Dintec Order PDF.exe modified

Time	Type	Description
16:44:24	API Interceptor	2x Sleep call for process: a.exe modified

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	IMG-47901.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	
	Ewqm21lwdh.exe	Get hash	malicious	Browse	
	a4iz7zkilq.exe	Get hash	malicious	Browse	
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	
	nMn5eAMhBy.exe	Get hash	malicious	Browse	
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	
	vK6VPijMoq.exe	Get hash	malicious	Browse	
	8gom3VEZLS.exe	Get hash	malicious	Browse	
	y4Gpxq7eWg.exe	Get hash	malicious	Browse	
	DHL-#AWB130501923096PDF.exe	Get hash	malicious	Browse	
	IMG_1677.EXE	Get hash	malicious	Browse	
	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	IMG_5371.EXE	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	IMG_9501.EXE	Get hash	malicious	Browse	
	IMG_04017.pdf.exe	Get hash	malicious	Browse	
	GFS_03781.xls.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Dintec Order PDF.exe.log

Process:	C:\Users\user\Desktop\Dintec Order PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1873
Entropy (8bit):	5.355036985457214
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjovitHoxHhAHKzvr1qHj:iqXeqm00YqhQnouRqjoKtIxHeqzTwD
MD5:	CDA95282F22F47DA2FDDC9E912B67FEF
SHA1:	67A40582A092B5DF40C3EB61A361A2D336FC69E0
SHA-256:	179E50F31095D0CFA13DCBB9CED6DEE424DFE8CEF8E05BDE1F840273F45E5F49

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Dintec Order PDF.exe.log	
SHA-512:	1D151D92AE982D2149C2255826C2FFB89A475A1EB9B9FE93DC3706F3016CD6B309743B36A4D7F6D68F48CE25391FDA7A2BAE42061535EEA7862460424A3A2036
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):	1784
Entropy (8bit):	5.35306750074546
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjovitHoxHhAHKzva:iqXeqm00YqhQnouRqjoKtlxHeqzC
MD5:	4D3278A4C9BE931A3AFCEACB561B87DB
SHA1:	E828DC80D92A261CA30E7333E7C2C3205C05AD7E
SHA-256:	A45DF0DB57887914E4C1D5A8F8053E669561A9177B333BE50AE3CB1EA4770EEB
SHA-512:	567CACB27FC7888FA3ABF924D64356780464DA20BDDB4A4719D15AD006522C0B1B75876A57E61CFC96A3A0C8C79F1D825F0D82C404AF0E53309A73CAF88519F
Malicious:	false
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\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\Dintec Order 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:ZBMs2SqdD86Iq8gZZFyViML3an
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%
Joe Sandbox View:	• Filename: IMG-47901.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Packed2.42783.27799.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Packed2.42783.24703.exe, Detection: malicious, Browse • Filename: Ewqm21Iwdh.exe, Detection: malicious, Browse • Filename: a4iz7zkilq.exe, Detection: malicious, Browse • Filename: Vcg9GH4CWw.exe, Detection: malicious, Browse • Filename: nMn5eAMhBy.exe, Detection: malicious, Browse • Filename: sSPHg0Y2cZ.exe, Detection: malicious, Browse • Filename: vK6VPijMoq.exe, Detection: malicious, Browse • Filename: 8gom3VEZLS.exe, Detection: malicious, Browse • Filename: y4Gpxq7eWg.exe, Detection: malicious, Browse • Filename: DHL-#AWB130501923096PDF.exe, Detection: malicious, Browse • Filename: IMG_1677.EXE, Detection: malicious, Browse • Filename: PO#4018-308875.pdf.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: IMG_5371.EXE, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: IMG_9501.EXE, Detection: malicious, Browse • Filename: IMG_04017.pdf.exe, Detection: malicious, Browse • Filename: GFS_03781.xls.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
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\Dintec Order 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):	854
Entropy (8bit):	3.0159112944533297
Encrypted:	false
SSDEEP:	12:8wl0RsXowAOcQ/tz0/CSLm9RKMJkHgTCNfBT/v4t2Y+xIBjK:8iLDWLYr+Vpd7aB
MD5:	CDE31B0A7CA104AEE6CB2FF9ABFED71F
SHA1:	B92338857A61560D0E667E6E3EB5B9CCF22CE260
SHA-256:	A835B03B57A7941B592CCF6825F308CDA3158A53B4B798B0E14C51D3E9DB1AB1
SHA-512:	AF3C36C759A831D5366F2493A4AAF7BA2A97181D098C4E2D2394F06BC379A3D947A8D2BFCFDA2ADE9C3D6AC44B0895C0E4470AA8AECF1D960C7424E2E6FAE9D
Malicious:	false
Reputation:	low
Preview:	L.....F.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<..... .....j.o.n.e.s.....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.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.a...e.x.e.....y.....>.e.L.: ..er.=y.....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\Dintec Order PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	643584
Entropy (8bit):	5.320790042456682
Encrypted:	false
SSDEEP:	6144:0OplH55fOUxVcMpvWt56GyM0cwlnRvCSyiof5d+mxiqNdmwvg03:hHfNbxpvWtQMRwlnASyv71xiqZF
MD5:	98E3C2AC1EFDD997B05A1FEE872630EC
SHA1:	D3CE076AF7B45E1F11AAC5E3A1C984951C7B92BA
SHA-256:	D09ED1437134F7E5C71EE4877E6D030C2750B6E1873FE6AFB0F82B988C591B44
SHA-512:	F0C9CC82F29D547216672FC78C19CAAA23D432C63760433A17C86A4D484A49B879733659CEA68AE19FEEB1841A803C8BEE04CD96064C1CB3AE273E7299BE7E47
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 42%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.....P..... .....@.. .....@..... ..`.....S.....B..... ..... ..... ..H.....text...$.... ..... ..`.rsrc...B.....@..@.reloc..... .....@..B.....H.....&.....>...La...[.....&..(.....*.s.....s.....s.....s .....*&.....*".....*Vs....(3...t.....*..(4...*..(....*..(8...*. .~....r...po5...tE...t....o8....*..(V...*..0..F.....(@...u1.....(@...u..... .K.M(B...t2... ..U.\(B...t..... 4..... ....(B...t.....(B...t....(....t2...(B...t2...(B...t.....(B...t1...(@...u.....(B...t....&..

C:\Users\user\AppData\Roaming\a.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Dintec Order 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**
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):	5.320790042456682
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:	Dintec Order PDF.exe
File size:	643584
MD5:	98e3c2ac1efdd997b05a1fee872630ec
SHA1:	d3ce076af7b45e1f11aac5e3a1c984951c7b92ba
SHA256:	d09ed1437134f7e5c71ee4877e6d030c2750b6e1873fe6a fb0f82b988c591b44
SHA512:	f0c9cc82f29d547216672fc78c19caaa23d432c63760433 a17c86a4d484a49b879733659cea68ae19feeb1841a803 c8bee04cd96064c1cb3ae273e7299be7ea7
SSDEEP:	6144:0OplH55fOUxVcMpvWt56GyM0cwlnRvCSyiof5d+ mxiqNdmwvg03:hHfNbxpvWtQMRwlnASyv71xiqZF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.....P..... .....@.. .....@..... ....` .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49e41e
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:	0x9D433DF [Mon Mar 24 14:04:15 1975 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0x9e3c8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa0000	0x642	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa2000	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	0x9c424	0x9c600	False	0.5252344999	data	5.32775062207	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa0000	0x642	0x800	False	0.35595703125	data	3.69283936063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa2000	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	0xa00a0	0x3b8	COM executable for DOS		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xa0458	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 1991 23F;HID;C92C>DJ
Assembly Version	1.0.0.0
InternalName	Dintec Order PDF.exe
FileVersion	9.13.17.22
CompanyName	23F;HID;C92C>DJ
Comments	77E5FH5@:B:;3GBH4G7
ProductName	D6:CEB?E58538D9<25FG
ProductVersion	9.13.17.22
FileDescription	D6:CEB?E58538D9<25FG
OriginalFilename	Dintec Order PDF.exe

Network Behavior

UDP Packets

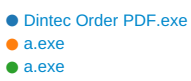
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:44:00.369968891 CET	49257	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:00.420526028 CET	53	49257	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:02.034677029 CET	62389	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:02.096035004 CET	53	62389	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:03.912905931 CET	49910	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:03.960730076 CET	53	49910	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:05.790050030 CET	55854	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:05.846998930 CET	53	55854	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:09.958733082 CET	64549	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:10.006597042 CET	53	64549	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:11.314935923 CET	63153	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:11.371381998 CET	53	63153	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:17.520215988 CET	52991	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:17.569350958 CET	53	52991	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:18.648869038 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:18.699317932 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:19.893682003 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:19.941685915 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:22.173286915 CET	56794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:22.221118927 CET	53	56794	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:23.031732082 CET	56534	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:23.087929964 CET	53	56534	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:23.151201010 CET	56627	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:23.176327944 CET	56621	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:23.216319084 CET	53	56627	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:23.227221012 CET	53	56621	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:24.032463074 CET	63116	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:24.080446959 CET	53	63116	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:25.059024096 CET	64078	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:25.085433960 CET	64801	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:25.109750986 CET	53	64078	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:25.136379957 CET	53	64801	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:26.191709995 CET	61721	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:26.242696047 CET	53	61721	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:27.431175947 CET	51255	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:44:27.481992960 CET	53	51255	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:28.297048092 CET	61522	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:28.350481033 CET	53	61522	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:29.657900095 CET	52337	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:29.718781948 CET	53	52337	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:42.962939024 CET	55046	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:43.022135019 CET	53	55046	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:43.544616938 CET	49612	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:43.607117891 CET	53	49612	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:44.167186022 CET	49285	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:44.223592997 CET	53	49285	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:44.378401995 CET	50601	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:44.450712919 CET	53	50601	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:44.659657001 CET	60875	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:44.711767912 CET	53	60875	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:45.163724899 CET	56448	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:45.213849068 CET	53	56448	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:45.748568058 CET	59172	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:45.810645103 CET	53	59172	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:46.401335001 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:46.458602905 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:47.273775101 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:47.330384016 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:48.324867964 CET	50183	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:48.381885052 CET	53	50183	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:48.881405115 CET	61531	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:48.942864895 CET	53	61531	8.8.8.8	192.168.2.4
Jan 27, 2021 16:44:49.295454979 CET	49228	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:44:49.355367899 CET	53	49228	8.8.8.8	192.168.2.4
Jan 27, 2021 16:45:00.754601955 CET	59794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:45:00.802643061 CET	53	59794	8.8.8.8	192.168.2.4
Jan 27, 2021 16:45:00.874398947 CET	55916	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:45:00.945894957 CET	53	55916	8.8.8.8	192.168.2.4
Jan 27, 2021 16:45:02.516755104 CET	52752	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:45:02.580696106 CET	53	52752	8.8.8.8	192.168.2.4
Jan 27, 2021 16:45:35.890669107 CET	60542	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:45:35.943331003 CET	53	60542	8.8.8.8	192.168.2.4
Jan 27, 2021 16:45:37.506793976 CET	60689	53	192.168.2.4	8.8.8.8
Jan 27, 2021 16:45:37.563329935 CET	53	60689	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Dintec Order PDF.exe PID: 3480 Parent PID: 5932

General

Start time:	16:44:04
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\Dintec Order PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Dintec Order PDF.exe'
Imagebase:	0x1b0000
File size:	643584 bytes
MD5 hash:	98E3C2AC1EFDD997B05A1FEE872630EC
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: 00000001.00000002.681613074.0000000004031000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.681613074.0000000004031000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.681613074.0000000004031000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.681348992.0000000003E9B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.681348992.0000000003E9B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.681348992.0000000003E9B000.00000004.00000001.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	6D1CCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D1CCF06	unknown
C:\Users\user\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	4CCD20B	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	4CCD20B	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	4CCD20B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Dintec Order PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	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 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	4CCD20B	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 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 df 33 d4 09 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 c6 09 00 00 0a 00 00 00 00 00 00 1e e4 09 00 00 20 00 00 00 00 0a 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 40 0a 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....3........... ....P................. ....@.. ....@ ....`................	success or wait	3	4CCD20B	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	4CCD20B	CopyFileExW
C:\Users\user\AppData\Local\Mi crosoft\CLR_v4.0_32\UsageLogs\Dintec Order PDF.exe.log	unknown	1873	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,"Win RT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, Pub licKeyToken=b77a5c5619 34e089", "C:\Windows\assembly\Nat iveIma ges_v4.0.30319_32\Syste m\4f0a7 eefa3cd3e0ba98b5ebddbb c72e6\Sy stem.ni.dll",0..3,"Presentati onCore, Version=	success or wait	1	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	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	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: a.exe PID: 984 Parent PID: 3480

General

Start time:	16:44:21
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\a.exe'
Imagebase:	0x250000
File size:	643584 bytes
MD5 hash:	98E3C2AC1EFDD997B05A1FEE872630EC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 42%, Virustotal, Browse
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	6D1CCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D1CCF06	unknown
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	6D4DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	unknown	1784	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	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: a.exe PID: 6648 Parent PID: 3424

General

Start time:	16:44:21
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\a.exe'
Imagebase:	0x110000
File size:	643584 bytes
MD5 hash:	98E3C2AC1EFDD997B05A1FEE872630EC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D1003DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Disassembly

Code Analysis