ID: 431780
Sample Name:
DHL#DOCUMENTS001010.PDF.exe
Cookbook: default.jbs
Time: 09:52:20
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

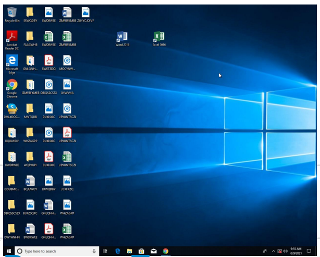
Analysis Report DHL#DOCUMENTS001010.PDF.exe

Overview

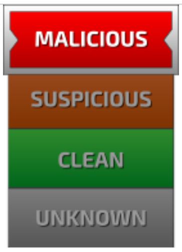
General Information

Sample Name:	DHL#DOCUMENTS001010.PDF.exe
Analysis ID:	431780
MD5:	b7fece0a9529306.
SHA1:	767fcf70a98dd70..
SHA256:	f9284667090735e.
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection



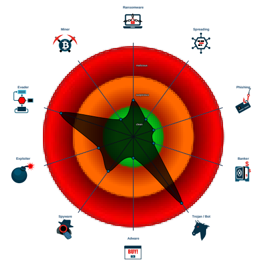
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- DHL#DOCUMENTS001010.PDF.exe (PID: 6964 cmdline: 'C:\Users\user\Desktop\DHL#DOCUMENTS001010.PDF.exe' MD5: B7FECE0A9529306A2644CE102FE2D86A)
  - RegAsm.exe (PID: 7020 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe hjhjkfk MD5: 6FD7592411112729BF6B1F2F6C34899F)
- bhjhjkek.exe (PID: 6868 cmdline: 'C:\Users\user\AppData\Local\bhjhjkek.exe' MD5: B7FECE0A9529306A2644CE102FE2D86A)
  - RegAsm.exe (PID: 5868 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe hjhjkfk MD5: 6FD7592411112729BF6B1F2F6C34899F)
- bhjhjkek.exe (PID: 5456 cmdline: 'C:\Users\user\AppData\Local\bhjhjkek.exe' MD5: B7FECE0A9529306A2644CE102FE2D86A)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ba5f434c-3370-4fb7-bec8-4c7f593d",
  "Group": "Grace",
  "Domain1": "23.105.131.142",
  "Domain2": "startedhere.ddns.net",
  "Port": 2092,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
DHL#DOCUMENTS001010.PDF.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\bhjhjkek.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.767317369.00000000030F1000.00000004.00000001.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000E.00000002.910382533.00000000007C2000.00000002.00020000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000B.00000002.919456791.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000002.919456791.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.919456791.0000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Click to see the 112 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DHL#DOCUMENTS001010.PDF.exe.43789c8.10.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.DHL#DOCUMENTS001010.PDF.exe.43789c8.10.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.DHL#DOCUMENTS001010.PDF.exe.43789c8.10.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.DHL#DOCUMENTS001010.PDF.exe.43789c8.10.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
11.2.RegAsm.exe.68d0000.22.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
Click to see the 242 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration
Multi AV Scanner detection for domain / URL
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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
C2 URLs / IPs found in malware configuration

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

Data Obfuscation:

.NET source code contains potential unpacker
Yara detected Costura Assembly Loader

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

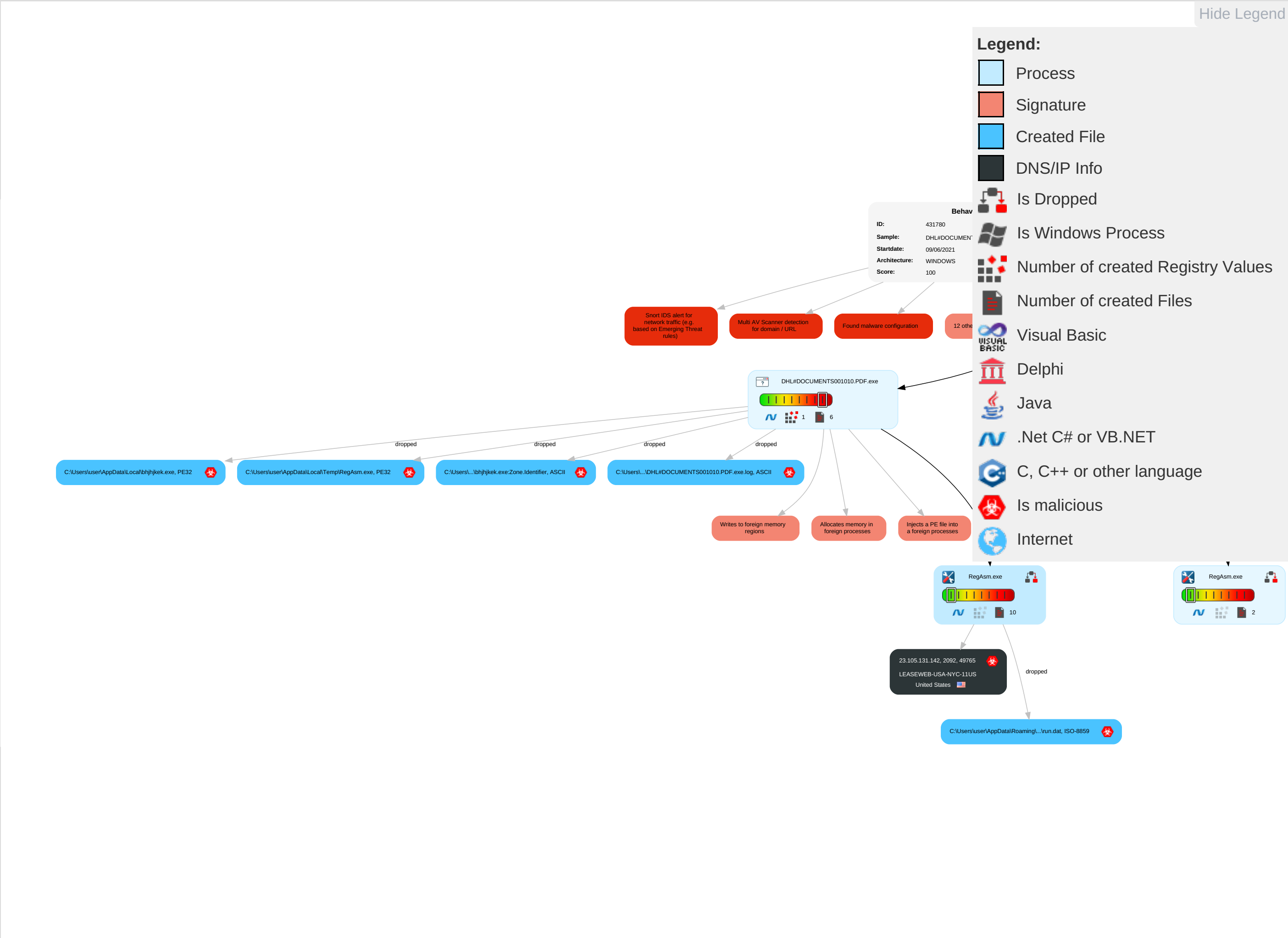
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Registry Run Keys / Startup Folder 1	Process Injection 3 1 2	Masquerading 1 1	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

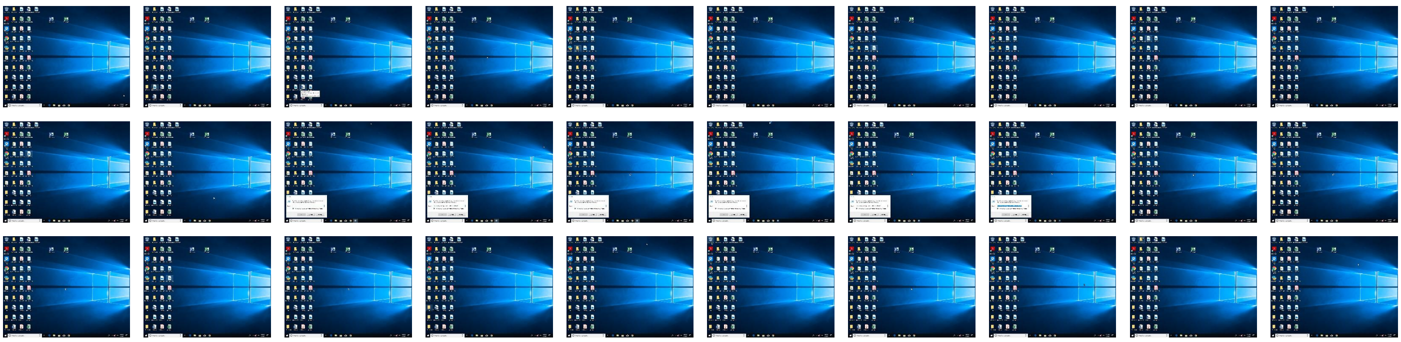
Behavior Graph



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
DHL#DOCUMENTS001010.PDF.exe	44%	Virustotal		Browse
DHL#DOCUMENTS001010.PDF.exe	31%	Metadefender		Browse
DHL#DOCUMENTS001010.PDF.exe	32%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
DHL#DOCUMENTS001010.PDF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\bhjhjkek.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\bhjhjkek.exe	44%	Virustotal		Browse
C:\Users\user\AppData\Local\bhjhjkek.exe	31%	Metadefender		Browse
C:\Users\user\AppData\Local\bhjhjkek.exe	32%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.RegAsm.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.RegAsm.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.RegAsm.exe.5dd0000.19.unpack	100%	Avira	TR/NanoCore.fadte		Download File
19.0.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
startedhere.ddns.net	9%	Virustotal		Browse
startedhere.ddns.net	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
23.105.131.142	5%	Virustotal		Browse
23.105.131.142	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
startedhere.ddns.net	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
23.105.131.142	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431780
Start date:	09.06.2021
Start time:	09:52:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 31s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	DHL#DOCUMENTS001010.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:	20
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@7/10@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.4%) • Quality average: 34.9% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 90% • 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

Simulations

Behavior and APIs

Time	Type	Description
09:54:05	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run bhjhjkek "C:\Users\user\AppData\Local\bhjhjkek.exe"
09:54:13	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run bhjhjkek "C:\Users\user\AppData\Local\bhjhjkek.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.105.131.142	RFQ27559404D4E5A.PDF.exe	Get hash	malicious	Browse	
	RFQ#21040590409448.pdf.exe	Get hash	malicious	Browse	
	DHL#DOCUMENTS02010910.PDF.exe	Get hash	malicious	Browse	
	QOUTATION#2300003590.PDF.exe	Get hash	malicious	Browse	
	ORDER#INQUIRY000111.PDF.exe	Get hash	malicious	Browse	
	RFQ#QQO2103060.PDF.exe	Get hash	malicious	Browse	
	RFQ#QQO2103060.PDF.exe	Get hash	malicious	Browse	
	AWBSHIPMENT20210000900.PDF.exe	Get hash	malicious	Browse	
	Order#PPO040963RG02.PDF.exe	Get hash	malicious	Browse	
	iOI0kJwm97.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	2lt24JqVH4.exe	Get hash	malicious	Browse	• 23.105.131.207
	RFQ27559404D4E5A.PDF.exe	Get hash	malicious	Browse	• 23.105.131.142
	XVIdVNjoHI.exe	Get hash	malicious	Browse	• 23.105.131.173
	cKWxEAbeX7.exe	Get hash	malicious	Browse	• 23.105.131.251
	apWkH5Vq75.exe	Get hash	malicious	Browse	• 23.105.131.141
	RFQ#21040590409448.pdf.exe	Get hash	malicious	Browse	• 23.105.131.142
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 23.105.131.132
	DHL#DOCUMENTS02010910.PDF.exe	Get hash	malicious	Browse	• 23.105.131.142
	QOUTATION#2300003590.PDF.exe	Get hash	malicious	Browse	• 23.105.131.142
	Purchase Order.exe	Get hash	malicious	Browse	• 23.105.131.158
	Scanned Documents.exe	Get hash	malicious	Browse	• 23.105.131.158
	ORDER#INQUIRY000111.PDF.exe	Get hash	malicious	Browse	• 23.105.131.142
	URGENT ORDER 2T6U545267,pdf.exe	Get hash	malicious	Browse	• 23.105.131.132
	9849858 PO.exe	Get hash	malicious	Browse	• 23.105.131.166
	Yeni sipari_ WJO-001, pdf.exe	Get hash	malicious	Browse	• 23.105.131.132
	061195d6_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.105.131.158
	URGENT ORDER 2T6U545267,pdf.exe	Get hash	malicious	Browse	• 23.105.131.132
	ORDER QUOTE CBM787563788265542,pdf.exe	Get hash	malicious	Browse	• 23.105.131.132
	PO ____-34002174,pdf.exe	Get hash	malicious	Browse	• 23.105.131.141
	RECHNUNGSKAUF Bestellung-46509008.pdf.exe	Get hash	malicious	Browse	• 23.105.131.132

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\RegAsm.exe	kylfnzzg3E.exe	Get hash	malicious	Browse	
	flyZab7hHk.exe	Get hash	malicious	Browse	
	AedJpyQ9lM.exe	Get hash	malicious	Browse	
	UPDATED SOA.exe	Get hash	malicious	Browse	
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	
	RFQ27559404D4E5A.PDF.exe	Get hash	malicious	Browse	
	Receiptn.exe	Get hash	malicious	Browse	
	PURCHASE LIST.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.783.10804.exe	Get hash	malicious	Browse	
	Y6k2VgaGck.exe	Get hash	malicious	Browse	
	Bank swift.exe	Get hash	malicious	Browse	
	tT1XWdxOYv.exe	Get hash	malicious	Browse	
	363IN050790620 BOOKING.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	RFQ#21040590409448.pdf.exe	Get hash	malicious	Browse	
	DHL#DOCUMENTS02010910.PDF.exe	Get hash	malicious	Browse	
	QOUTATION#2300003590.PDF.exe	Get hash	malicious	Browse	
	1p037oXV3S.exe	Get hash	malicious	Browse	
	BaU9m8mMFx.exe	Get hash	malicious	Browse	
	yl77tM4JDg.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL#DOCUMENTS001010.PDF.exe.log

Process:	C:\Users\user\Desktop\DHL#DOCUMENTS001010.PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL#DOCUMENTS001010.PDF.exe.log	
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD: D
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,"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..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bhjhjkek.exe.log	
Process:	C:\Users\user\AppData\Local\bhjhjkek.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD: D
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,"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..

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Process:	C:\Users\user\Desktop\DHL#DOCUMENTS001010.PDF.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	64616
Entropy (8bit):	6.037264560032456
Encrypted:	false
SSDEEP:	768:J8XcJiMjm2ieHlPyCsSuJbn8dBhFVBSMQ6Iq8TSYDKpgLaDViRLNdr:9YMaNylPYSAb8dBnTHv8DKKaDVkX
MD5:	6FD7592411112729BF6B1F2F6C34899F
SHA1:	5E5C839726D6A43C478AB0B95DBF52136679F5EA
SHA-256:	FFE4480CCC81B061F725C54587E9D1BA96547D27FE28083305D75796F2EB3E74
SHA-512:	21EFCC9DEE3960F1A64C6D8A44871742558666BB792D77ACE91236C7DBF42A6CA77086918F363C4391D9C00904C55A952E2C18BE5FA1A67A509827BFC630070I
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: kylfnzzg3E.exe, Detection: malicious, Browse • Filename: flyZab7hHk.exe, Detection: malicious, Browse • Filename: AedJpyQ9lM.exe, Detection: malicious, Browse • Filename: UPDATED SOA.exe, Detection: malicious, Browse • Filename: qdFDmi3Bhy.exe, Detection: malicious, Browse • Filename: RFQ27559404D4E5A.PDF.exe, Detection: malicious, Browse • Filename: Receiptn.exe, Detection: malicious, Browse • Filename: PURCHASE LIST.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.783.10804.exe, Detection: malicious, Browse • Filename: Y6k2VgaGck.exe, Detection: malicious, Browse • Filename: Bank swift.exe, Detection: malicious, Browse • Filename: tT1XWdxOYv.exe, Detection: malicious, Browse • Filename: 363IN050790620 BOOKING.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: RFQ#21040590409448.pdf.exe, Detection: malicious, Browse • Filename: DHL#DOCUMENTS02010910.PDF.exe, Detection: malicious, Browse • Filename: QOUTATION#2300003590.PDF.exe, Detection: malicious, Browse • Filename: 1p037oXV3S.exe, Detection: malicious, Browse • Filename: BaU9m8mMFx.exe, Detection: malicious, Browse • Filename: yl77tM4JDg.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\RegAsm.exe

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...xX.Z.............0............^.... ....@.. ....`....................................O.......8...............h>.......................................................... ............... ..H...........text...d.... ...................... ..`.rsrc...8..........................@..@.reloc........ ....@..B................@.......H........A...p..........T..~P...-.r...p.....(....(....s.....P...*..0..".......(......-.r...p.rl..p(....s....z.*...0..........(....~P.....o..... .*..(....*n(.....(..........%...(....*~(.....(..........%...%...(....*.(.....(..........%...%...%...(....*V.(......}Q.....}R...*..{Q...*..{R...*...0...........(.......i.=...}S......i.@...}T......i.@...}U.....+m...(....o .....r]..p.o!...,..{T.......{U........o"....+(.ra..p.o!...,..{T.......

C:\Users\user\AppData\Local\bhjhjkek.exe

Process:	C:\Users\user\Desktop\DHL#DOCUMENTS001010.PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	607704
Entropy (8bit):	6.749029364545613
Encrypted:	false
SSDEEP:	12288:v3SBz/P5DgjDjNGPZk3Zg1Ke0lC8+lEvKlJfF05Ibmu9EgeIKxAtWO:v3IzJDgjDjNU2Jg1t0lCb3
MD5:	B7FECE0A9529306A2644CE102FE2D86A
SHA1:	767FCF70A98DD70D9035DFE4FCCA04E17CDEBFDE
SHA-256:	F9284667090735ECCB6110C4C9E33122890570B6F10798EF57370740C4D9DB6D
SHA-512:	04092525491ADD6E159FDD19E720CD0D38CFB4FA037907B1D08AAFF9AA3833A2F0387A1169026831C0F2FE388DBE2C6C0B47EE5814CE6C64680F27A3849D109
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\bhjhjkek.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 44%, Browse • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 32%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....`.....................p........... ........@.. ................................... .@...............................p...K.......tl..........*.......`... ....H...........text....... ....`.rsrc...tl.......n.................@..@.reloc.......`.. .....(.............@..B.......................H.......87..X.......'....e...q..9.....:....8....(....8....(....8....*..*..j...:....&(....8....&8....*..*..j...:....&(....8....&8....*..*...*..j...:....& (....8....&8....*..*...*...*...*...*...0..z.......s.....:P...&s.....:N...&s.....:L...&s.........~....r...pr...po....~....rO..pra..po....8.........8.........8.........8....*......:....&:....8....&8....r...p*...:....&o.. ..8....&8....*...0..........(....o.....:....&..:....&8f....8.....8..

C:\Users\user\AppData\Local\bhjhjkek.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\DHL#DOCUMENTS001010.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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356 A5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:uh:2
MD5:	290BBB2342B623C21C98E5B0AFF6126A
SHA1:	DFFF467E660EB007454A2E677B3C81D60296A296
SHA-256:	5BC0B7B765A4BA88635ED78FB9EF64DA054F77B354F5B6A0C9370AF18EF83694
SHA-512:	652B1A33D06529AAF40A063D737039799562D58BBFEB9AAA0744605A11DAC2FEC3598232BFC890A34785D1CC7AA1E27704DA5A27935A82E6FAD2FA804F803DF C
Malicious:	**true**
Reputation:	low
Preview:	.e=..+.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A 6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a........~.~.......3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i......~...|..fX_...Xf.p^......>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.......v."".v.......#..X.a....../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz......(...o......b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O..........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?............b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.......H...6$. ..d...|m...N..1.R..B.i..........$....$........CY}..$....r.....H...8...li.....7 P......?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.749029364545613
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DHL#DOCUMENTS001010.PDF.exe
File size:	607704
MD5:	b7fece0a9529306a2644ce102fe2d86a
SHA1:	767fcf70a98dd70d9035dfe4fcca04e17cdebfde
SHA256:	f9284667090735eccb6110c4c9e33122890570b6f10798ef57370740c4d9db6d
SHA512:	04092525491add6e159fdd19e720cd0d38cfb4fa037907b1d08aaff9aa3833a2f0387a1169026831c0f2fe388dbe2c6c0b47ee5814ce6c64680f27a3849d1099
SSDEEP:	12288:v3SBz/P5DgjDjNGPZk3Zg1Ke0lC8+lEvKlJfF05Ibmu9EgeIKxAtWO:v3IzJDgjDjNU2Jg1t0lCb3
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......`.....................p........... ....@.. ....@................................

File Icon

Icon Hash:	74f2dbb284c2e2ee

Static PE Info

General

Entrypoint:	0x44d7be
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60BFE88A [Tue Jun 8 22:00:42 2021 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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert SHA2 Assured ID Code Signing CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 8/25/2016 2:00:00 AM 10/9/2019 2:00:00 PM
Subject Chain	• CN="OpenVPN Technologies, Inc.", O="OpenVPN Technologies, Inc.", L=Pleasanton, S=California, C=US
Version:	3
Thumbprint MD5:	6146F700D6452042DC954108EBA73447
Thumbprint SHA-1:	21F94C255A8B20D21A323CA5ACB8EBF284E09037
Thumbprint SHA-256:	BAA11FF9D7FEDEC30BC343F6F0E85B3256EA8155573E862B17C15DCB2596C678
Serial:	03E49B29AE75DF4C50DC1662670776B9

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x4b7c4	0x4b800	False	0.979075046565	data	7.98213921813	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4e000	0x46c74	0x46e00	False	0.197964891975	data	4.61492882254	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x96000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-09:54:09.372256	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	2092	192.168.2.4	23.105.131.142

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DHL#DOCUMENTS001010.PDF.exe PID: 6964 Parent PID: 6008

General

Start time:	09:53:09
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\DHL#DOCUMENTS001010.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL#DOCUMENTS001010.PDF.exe'
Imagebase:	0xca0000
File size:	607704 bytes
MD5 hash:	B7FECE0A9529306A2644CE102FE2D86A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.767317369.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000000.644449963.0000000000CA2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.768500563.000000000424A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.768500563.000000000424A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.768500563.000000000424A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.768627185.0000000004329000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.768627185.0000000004329000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.768627185.0000000004329000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.766443926.0000000000CA2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.767390433.0000000003140000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.767390433.0000000003140000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.768765358.00000000043C8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.768765358.00000000043C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.768765358.00000000043C8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: RegAsm.exe PID: 7020 Parent PID: 6964

General

Start time:	09:54:05
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe hjhjkfk
Imagebase:	0x9a0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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: 0000000B.00000002.919456791.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.919456791.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.919456791.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.928006695.0000000006AA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.928006695.0000000006AA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.927086659.0000000005DD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.927086659.0000000005DD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.927086659.0000000005DD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.927717545.00000000068D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.927717545.00000000068D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.927972563.0000000006A90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.927972563.0000000006A90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.928481566.0000000006B30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.928481566.0000000006B30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.927934540.0000000006A80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.927934540.0000000006A80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.923206884.0000000003E7F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.928049608.0000000006AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.928049608.0000000006AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.921992403.0000000002E21000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.921992403.0000000002E21000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.765891937.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.765891937.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.765891937.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.927902201.0000000006A70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.927902201.0000000006A70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.923629464.000000000410E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.928268197.0000000006AF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.928268197.0000000006AF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.928208155.0000000006AE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.928208155.0000000006AE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.927748989.00000000068E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.927748989.00000000068E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.765519849.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.765519849.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.765519849.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.926591236.00000000054A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.926591236.00000000054A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.927857463.0000000006A50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.927857463.0000000006A50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.928087795.0000000006AC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.928087795.0000000006AC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.923284531.0000000003EF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.923284531.0000000003EF0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: bhjhjkek.exe PID: 6868 Parent PID: 3424

General

Start time:	09:54:13
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Local\bhjhjkek.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\bhjhjkek.exe'
Imagebase:	0x7c0000
File size:	607704 bytes
MD5 hash:	B7FECE0A9529306A2644CE102FE2D86A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000E.00000002.910382533.00000000007C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000E.00000002.913423269.0000000002D31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000E.00000000.782814633.00000000007C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.916788361.0000000003E8A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.916788361.0000000003E8A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.916788361.0000000003E8A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.917015051.0000000003F69000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.917015051.0000000003F69000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.917015051.0000000003F69000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.917166768.0000000004008000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.917166768.0000000004008000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.917166768.0000000004008000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.914492634.0000000002E66000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.914492634.0000000002E66000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\bhjhjkek.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 44%, Virustotal, Browse • Detection: 31%, Metadefender, Browse • Detection: 32%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: bhjhjkek.exe PID: 5456 Parent PID: 3424

General

Start time:	09:54:22
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Local\bhjhjkek.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\bhjhjkek.exe'
Imagebase:	0x290000
File size:	607704 bytes
MD5 hash:	B7FECE0A9529306A2644CE102FE2D86A
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: 00000011.00000002.923323005.00000000038C8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.923323005.00000000038C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.923323005.00000000038C8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.923195254.0000000003829000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.923195254.0000000003829000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.923195254.0000000003829000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.919434619.0000000000292000.00000002.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.922180168.00000000027EC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.922180168.00000000027EC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000000.801027556.0000000000292000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.921745591.00000000025F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.923041905.000000000374A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.923041905.000000000374A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.923041905.000000000374A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: RegAsm.exe PID: 5868 Parent PID: 6868

General

Start time:	09:55:09
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe hjhjkfk
Imagebase:	0xb50000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.921730326.0000000003ED9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.921730326.0000000003ED9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.902721900.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.902721900.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.902721900.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.903322514.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.903322514.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.903322514.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.921433877.0000000002ED1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.921433877.0000000002ED1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.919456275.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.919456275.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.919456275.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 32.0.0 Black Diamond