ID: 412361
Sample Name:
QuotationOrder.pdf.exe
Cookbook: default.jbs
Time: 16:37:08
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

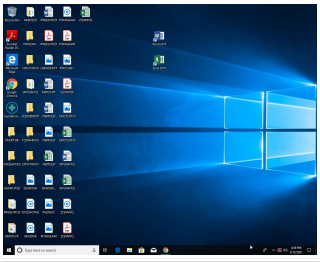
Analysis Report QuotationOrder.pdf.exe

Overview

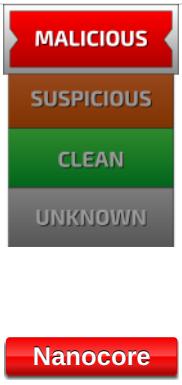
General Information

Sample Name:	QuotationOrder.pdf.exe
Analysis ID:	412361
MD5:	14e431bcb3fdb77.
SHA1:	717c23d8bd639b..
SHA256:	378932d5fc866bf..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



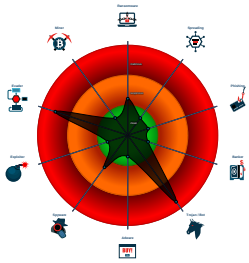
Nanocore

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 dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- QuotationOrder.pdf.exe (PID: 6248 cmdline: 'C:\Users\user\Desktop\QuotationOrder.pdf.exe' MD5: 14E431BCB3FDB77CD13912A5CBEF9E40)
  - schtasks.exe (PID: 6348 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RLaczhWDn' /XML 'C:\Users\user\AppData\Local\Temp\tmpAF14.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 6400 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7d9d1b37-9225-4679-a6f4-60db74de",
  "Group": "TBOSS1",
  "Domain1": "194.5.98.19",
  "Domain2": "tboss1.ddns.net",
  "Port": 53795,
  "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"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.243826185.00000000043B9000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xc5065:$x1: NanoCore.ClientPluginHost • 0xc50a2:$x2: IClientNetworkHost • 0xc8bd5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.243826185.00000000043B9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.243826185.00000000043B9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xc4dcd:$a: NanoCore • 0xc4ddd:$a: NanoCore • 0xc5011:$a: NanoCore • 0xc5025:$a: NanoCore • 0xc5065:$a: NanoCore • 0xc4e2c:$b: ClientPlugin • 0xc502e:$b: ClientPlugin • 0xc506e:$b: ClientPlugin • 0xc4f53:$c: ProjectData • 0xc595a:$d: DESCrypto • 0xcd326:$e: KeepAlive • 0xcb314:$g: LogClientMessage • 0xc750f:$i: get_Connected • 0xc5c90:$j: #=q • 0xc5cc0:$j: #=q • 0xc5cdc:$j: #=q • 0xc5d0c:$j: #=q • 0xc5d28:$j: #=q • 0xc5d44:$j: #=q • 0xc5d74:$j: #=q • 0xc5d90:$j: #=q
00000000.00000002.243971939.000000004508000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x14844d:$x1: NanoCore.ClientPluginHost • 0x14848a:$x2: IClientNetworkHost • 0x14bfbd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.243971939.000000004508000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.QuotationOrder.pdf.exe.446ded8.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
0.2.QuotationOrder.pdf.exe.446ded8.3.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:$s5: IClientLoggingHost
0.2.QuotationOrder.pdf.exe.446ded8.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.QuotationOrder.pdf.exe.446ded8.3.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$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
0.2.QuotationOrder.pdf.exe.446ded8.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 3 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:

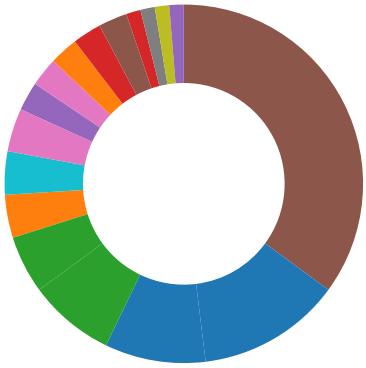
Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior



- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- 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:

- 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

Boot Survival:

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

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:

- Yara detected AntiVM3
- 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:

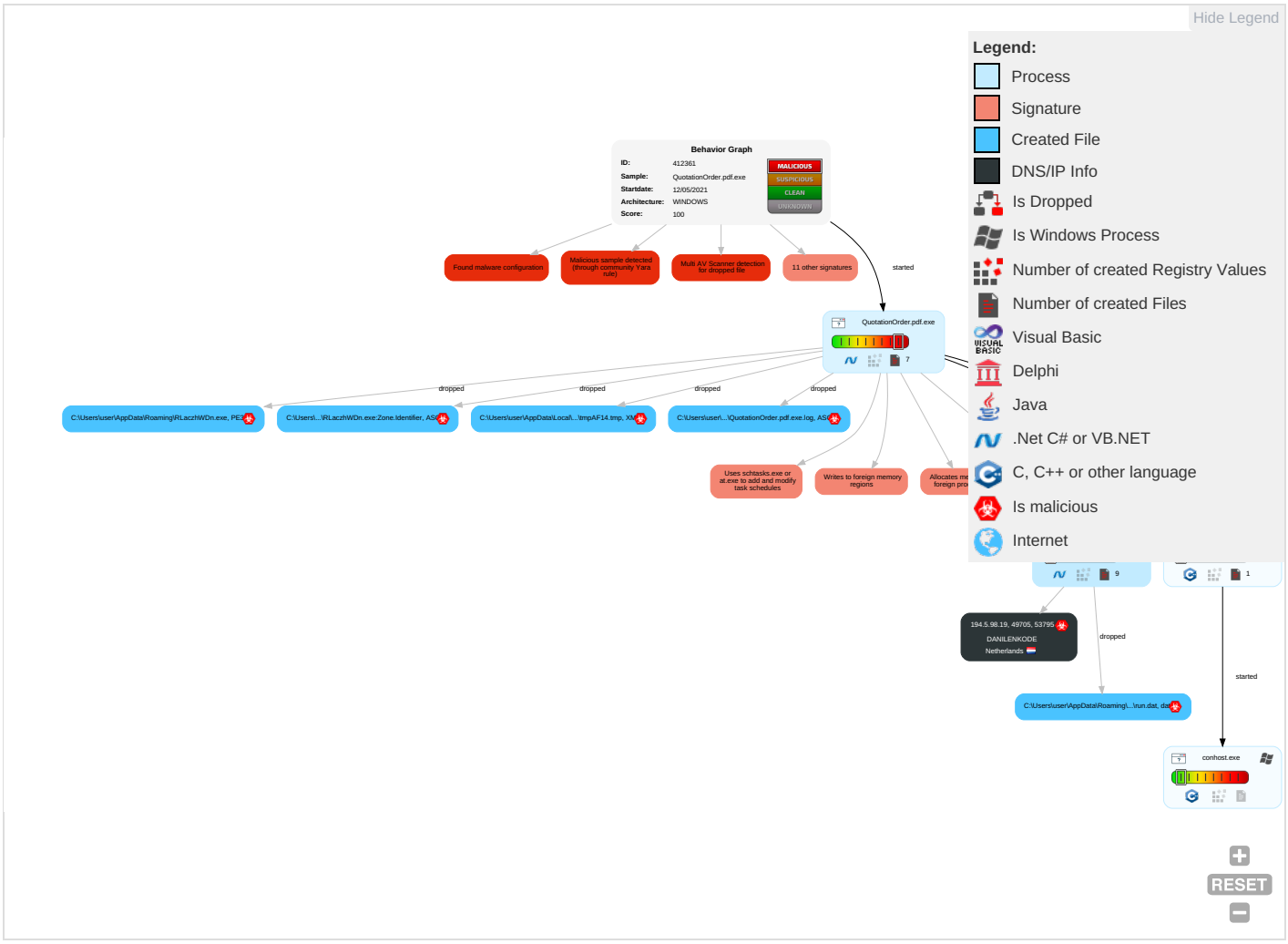
Detected Nanocore Rat

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	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 3 1 1	Masquerading 1 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Networ Commu
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial 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 Access

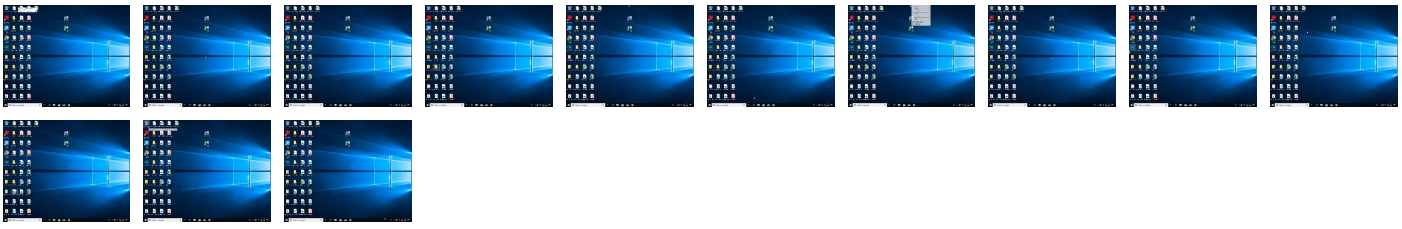
Behavior Graph



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
QuotationOrder.pdf.exe	13%	ReversingLabs	Win32.Trojan.Wacatac	
QuotationOrder.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\RLaczhWDn.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\RLaczhWDn.exe	13%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
tboss1.ddns.net	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
194.5.98.19	0%	Virustotal		Browse
194.5.98.19	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
tboss1.ddns.net	true	• Avira URL Cloud: safe	unknown
194.5.98.19	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	QuotationOrder.pdf.exe, 00000000.00000002.243492551.00000000033B1000.00000004.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	QuotationOrder.pdf.exe, 00000000.00000002.243530638.00000000033F4000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.19	unknown	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412361
Start date:	12.05.2021
Start time:	16:37:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QuotationOrder.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:	30
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@6/8@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 20.82.209.183, 104.43.139.144, 40.88.32.150, 92.122.145.220, 184.30.20.56, 2.20.143.16, 2.20.142.209, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:37:58	API Interceptor	2x Sleep call for process: QuotationOrder.pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.19	http://saggepaylive.co/Receipt of BACS payment 20092018.jar	Get hash	malicious	Browse	
	http://https://fellasconstrltd.co.uk	Get hash	malicious	Browse	
	http://https://www.aeroart.com.au/wp-admin/remittance.jar	Get hash	malicious	Browse	
	remittance.jar	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	Quotation.jar	Get hash	malicious	Browse	• 194.5.98.38
	Quotation.jar	Get hash	malicious	Browse	• 194.5.98.38
	47755769_by_Libranalysis.exe	Get hash	malicious	Browse	• 194.5.98.210
	Contract_kyrgyzstan_pdf.exe	Get hash	malicious	Browse	• 194.5.98.203
	y3t4g48gj6_PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.75
	y3t4g48gj6_PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.75
	Quotation.jar	Get hash	malicious	Browse	• 194.5.98.38
	5lQuLT5Zu8.exe	Get hash	malicious	Browse	• 194.5.97.116
	IPUt7Nr2CH.exe	Get hash	malicious	Browse	• 194.5.97.75
	Passport_ID_jpg.jar	Get hash	malicious	Browse	• 194.5.98.228
	Vd80r7R7K5.exe	Get hash	malicious	Browse	• 194.5.98.208
	noVPhNP46G.exe	Get hash	malicious	Browse	• 194.5.98.208
	LQ0dDP64uk.exe	Get hash	malicious	Browse	• 194.5.98.208
	SCAN_DOCX-36673672.exe	Get hash	malicious	Browse	• 194.5.97.11
	4b092c1e_by_Libranalysis.docx	Get hash	malicious	Browse	• 194.5.98.208
	QW8lWJDpU8.exe	Get hash	malicious	Browse	• 194.5.98.5
	2a8f04dd_by_Libranalysis.docm	Get hash	malicious	Browse	• 194.5.98.210
	Invoice_orderYscFwfO1peuGl0w.exe	Get hash	malicious	Browse	• 194.5.98.250
	Quotation.jar	Get hash	malicious	Browse	• 194.5.97.87
	Quotation.jar	Get hash	malicious	Browse	• 194.5.97.87

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QuotationOrder.pdf.exe.log

Process:	C:\Users\user\Desktop\QuotationOrder.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpAF14.tmp

Process:	C:\Users\user\Desktop\QuotationOrder.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658

C:\Users\user\AppData\Local\Temp\tmpAF14.tmp	
Entropy (8bit):	5.172758791574188
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBIItn:cbhH7MlNQ8/rydbz9I3YODOLNdq3Cu
MD5:	B79D81932ABEC23FDC88F5174005E22B
SHA1:	8AD532699EFB3ABDB0C9C8CE6AB813D3A8E61A43
SHA-256:	AAD7A31CC58EE7586719F33F84442BC343F68268E17B57F9925819FE2C5C954D
SHA-512:	2D5FEB2DFB7A5F739781017063E37FC36FC1FA1B9CD0938B5207D7A4D2621F9DD14D2EC9A1EDB6FE106CC7309075621133C8DB4A49A8AA4B2E4497D61FD6C5A
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:f:f
MD5:	98FFEE1BE6A389DA995E26874A8902A7
SHA1:	6A9A6943232179F45B37AB51E3424DAB9F229281
SHA-256:	0D6B2577E2F9D323C9632D28ED41AC91DBBE5FC476A0FAAADEA9BDA4685EF368
SHA-512:	8ED324A779482DD98B6D35C4873D0C2421E034BC53A6E8AC7301ED35C27A3A49D6E5DCFF65EE966300E29F29FA55B1A778C44D6D2BE0F3388E308390EF5CF7
Malicious:	**true**
Reputation:	low
Preview:	.:.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false

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

Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.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
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....*. l..&<}....`|.B....3.....l..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\RLaczhWDn.exe

Process:	C:\Users\user\Desktop\QuotationOrder.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	850944
Entropy (8bit):	7.33046471356557
Encrypted:	false
SSDEEP:	24576:CHqaISNYHhszddtBr+8qqbGdxP9rm0JU0:2vZuAddtyi8P/
MD5:	14E431BCB3FDB77CD13912A5CBEF9E40
SHA1:	717C23D8BD639B9E22E2DE994EF8EF87F575B48C
SHA-256:	378932D5FC866BFE3AE59ABE125E21DA19AE9FD819976FD1FDD73F8FCE110B7E
SHA-512:	2E8A8B5117F1680C30A3F8234BA2944BE4543F94EA7753720087C839F45901296ACD2072A3EBBC18292882015ABF8790B86B000FEAECAFB3452E074713927671
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..L.....k... .....@.. .....`..... .@.....k..O.....<.....@..... ....H.....text....K... ...L..... ..`.rsrc...<.....N.....@..@.relo c.....@.....@..B.....k.....H.....8.....0...X.....0.....(...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(.. ..oS...((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<..... ..~.....(4.....,lr...p.....(5...o6...s7.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\RLaczhWDn.exe:Zone.Identifier

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.33046471356557
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:	QuotationOrder.pdf.exe
File size:	850944
MD5:	14e431bcb3fdb77cd13912a5cbef9e40
SHA1:	717c23d8bd639b9e22e2de994ef8ef87f575b48c
SHA256:	378932d5fc866bfe3ae59abe125e21da19ae9fd819976fd1fdd73f8fce110b7e
SHA512:	2e8a8b5117f1680c30a3f8234ba2944be4543f94ea7753720087c839f45901296acd2072a3ebbc18292882015abf8790b86b000feaecafb3452e074713927671
SSDEEP:	24576:CHqaISNYHhszddtBr+8qqbGdxP9rm0JU0:2vZuAddtyi8P/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..L.....k... .....@.. .....`.....@.....

File Icon

Icon Hash:	cc92316d713396e8

Static PE Info

General

Entrypoint:	0x4b6bda
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609BD296 [Wed May 12 13:05:26 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

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb6b88	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x1ab3c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd4000	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	0xb4be0	0xb4c00	False	0.811643650588	data	7.65733353837	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x1ab3c	0x1ac00	False	0.145973276869	data	3.15479172029	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb8220	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xb8688	0x162a	PNG image data, 256 x 256, 8-bit colormap, non-interlaced		
RT_ICON	0xb9cb4	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xbc25c	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbd304	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xcdb2c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xd1d54	0x5a	data		
RT_VERSION	0xd1db0	0x35c	data		
RT_MANIFEST	0xd210c	0xa2e	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

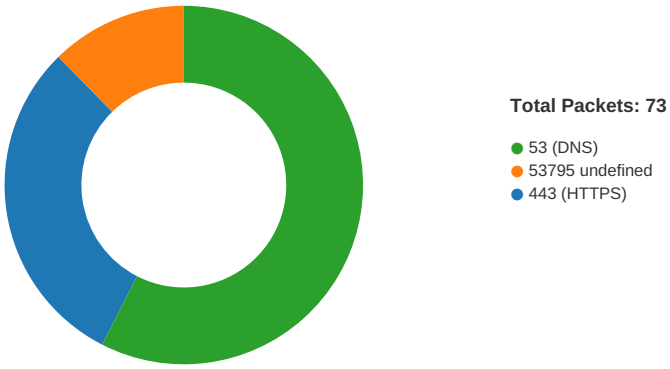
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	WaitHandle.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	LibraryManagementSystem
ProductVersion	1.0.0.0
FileDescription	LibraryManagementSystem
OriginalFilename	WaitHandle.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:37:49.402602911 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.402625084 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.402640104 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.402653933 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.402666092 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.402678967 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.402692080 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.402704954 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.402720928 CEST	443	49683	20.190.160.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:37:49.402798891 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.406750917 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.406775951 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.437081099 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.437128067 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.446013927 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.484226942 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.484262943 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.558038950 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.558084965 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.558279991 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.572079897 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.572144985 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.626034021 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.628714085 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.637880087 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.637937069 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.637986898 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.638031960 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.638073921 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.638114929 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.638154030 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.638170004 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.638189077 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.638194084 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.638233900 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.638350010 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.638359070 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.793132067 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.793154955 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.793168068 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.793185949 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.793205976 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.793225050 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.793241024 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.793256998 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.793276072 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.793291092 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.793385983 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.859034061 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.859078884 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.860367060 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.860460043 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:49.906537056 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.906565905 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.913742065 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.913774014 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:49.948044062 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.065779924 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.065824986 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.065845013 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.065871000 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.065895081 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.065918922 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.065943003 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.065967083 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.065989971 CEST	443	49683	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.066137075 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:50.066188097 CEST	49683	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:50.069802999 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.069839001 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.069864988 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.069890022 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.069915056 CEST	443	49686	20.190.160.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:37:50.069942951 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.069960117 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:50.069969893 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.069998026 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.070005894 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:50.070022106 CEST	443	49686	20.190.160.8	192.168.2.7
May 12, 2021 16:37:50.070054054 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:37:50.125252962 CEST	49686	443	192.168.2.7	20.190.160.8
May 12, 2021 16:38:04.338349104 CEST	49705	53795	192.168.2.7	194.5.98.19
May 12, 2021 16:38:04.625350952 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:04.626024008 CEST	49705	53795	192.168.2.7	194.5.98.19
May 12, 2021 16:38:04.663634062 CEST	49705	53795	192.168.2.7	194.5.98.19
May 12, 2021 16:38:05.025593996 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:05.025703907 CEST	49705	53795	192.168.2.7	194.5.98.19
May 12, 2021 16:38:05.673342943 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:05.673434973 CEST	49705	53795	192.168.2.7	194.5.98.19
May 12, 2021 16:38:06.131752968 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:06.208240986 CEST	49705	53795	192.168.2.7	194.5.98.19
May 12, 2021 16:38:06.847779989 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:06.854868889 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:06.857724905 CEST	49705	53795	192.168.2.7	194.5.98.19
May 12, 2021 16:38:07.400722980 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:07.450665951 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:07.450900078 CEST	49705	53795	192.168.2.7	194.5.98.19
May 12, 2021 16:38:07.463649035 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:07.492629051 CEST	53795	49705	194.5.98.19	192.168.2.7
May 12, 2021 16:38:07.493413925 CEST	49705	53795	192.168.2.7	194.5.98.19

UDP Packets

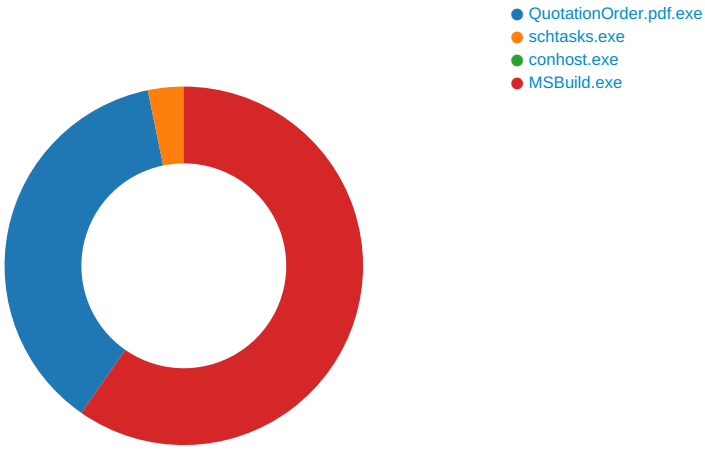
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:37:50.136571884 CEST	57820	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:50.197191000 CEST	53	57820	8.8.8.8	192.168.2.7
May 12, 2021 16:37:50.305509090 CEST	50848	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:50.364871979 CEST	53	50848	8.8.8.8	192.168.2.7
May 12, 2021 16:37:50.436470032 CEST	61242	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:50.496620893 CEST	53	61242	8.8.8.8	192.168.2.7
May 12, 2021 16:37:51.380249977 CEST	58562	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:51.430921078 CEST	53	58562	8.8.8.8	192.168.2.7
May 12, 2021 16:37:52.520164967 CEST	56590	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:52.578984022 CEST	53	56590	8.8.8.8	192.168.2.7
May 12, 2021 16:37:53.069900036 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:53.121454954 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 16:37:55.749366999 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:55.802941084 CEST	53	53775	8.8.8.8	192.168.2.7
May 12, 2021 16:37:56.546875954 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:56.598454952 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 16:37:57.524034977 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:57.572818995 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 16:37:59.112962961 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 16:37:59.161858082 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 16:38:00.298413992 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:00.347196102 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 16:38:01.534859896 CEST	58739	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:01.586709976 CEST	53	58739	8.8.8.8	192.168.2.7
May 12, 2021 16:38:02.570036888 CEST	60338	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:02.620176077 CEST	53	60338	8.8.8.8	192.168.2.7
May 12, 2021 16:38:03.501022100 CEST	58717	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:03.550889015 CEST	53	58717	8.8.8.8	192.168.2.7
May 12, 2021 16:38:04.529175997 CEST	59762	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:04.580795050 CEST	53	59762	8.8.8.8	192.168.2.7
May 12, 2021 16:38:05.407155037 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:05.456099987 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 16:38:06.186273098 CEST	58052	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:38:06.237843037 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 16:38:07.044519901 CEST	54008	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:07.093291998 CEST	53	54008	8.8.8.8	192.168.2.7
May 12, 2021 16:38:07.847956896 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:07.896676064 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 16:38:08.874038935 CEST	52914	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:08.923909903 CEST	53	52914	8.8.8.8	192.168.2.7
May 12, 2021 16:38:09.832998991 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:09.881685972 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 16:38:10.754215002 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:10.803047895 CEST	53	52816	8.8.8.8	192.168.2.7
May 12, 2021 16:38:13.429421902 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:13.478338003 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 16:38:15.326056004 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:15.375394106 CEST	53	54230	8.8.8.8	192.168.2.7
May 12, 2021 16:38:15.911966085 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:15.971407890 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 16:38:34.968208075 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:35.025798082 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 16:38:46.392949104 CEST	50860	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:46.450272083 CEST	53	50860	8.8.8.8	192.168.2.7
May 12, 2021 16:38:46.549272060 CEST	50452	53	192.168.2.7	8.8.8.8
May 12, 2021 16:38:46.606832027 CEST	53	50452	8.8.8.8	192.168.2.7
May 12, 2021 16:39:01.538760900 CEST	59730	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:01.595906973 CEST	53	59730	8.8.8.8	192.168.2.7
May 12, 2021 16:39:02.271943092 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:02.332194090 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 16:39:02.778215885 CEST	51919	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:02.851145029 CEST	53	51919	8.8.8.8	192.168.2.7
May 12, 2021 16:39:02.960926056 CEST	64296	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:03.020271063 CEST	53	64296	8.8.8.8	192.168.2.7
May 12, 2021 16:39:03.496707916 CEST	56680	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:03.546567917 CEST	53	56680	8.8.8.8	192.168.2.7
May 12, 2021 16:39:04.136363029 CEST	58820	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:04.196341991 CEST	53	58820	8.8.8.8	192.168.2.7
May 12, 2021 16:39:05.036043882 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:05.084620953 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 16:39:05.593821049 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:05.642579079 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 16:39:06.537549973 CEST	52286	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:06.597774029 CEST	53	52286	8.8.8.8	192.168.2.7
May 12, 2021 16:39:07.591264963 CEST	56064	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:07.644853115 CEST	53	56064	8.8.8.8	192.168.2.7
May 12, 2021 16:39:08.113748074 CEST	63744	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:08.174438953 CEST	53	63744	8.8.8.8	192.168.2.7
May 12, 2021 16:39:19.232753038 CEST	61457	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:19.293617964 CEST	53	61457	8.8.8.8	192.168.2.7
May 12, 2021 16:39:47.435106039 CEST	58367	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:47.515708923 CEST	53	58367	8.8.8.8	192.168.2.7
May 12, 2021 16:39:48.874694109 CEST	60599	53	192.168.2.7	8.8.8.8
May 12, 2021 16:39:48.931833029 CEST	53	60599	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: QuotationOrder.pdf.exe PID: 6248 Parent PID: 5856

General

Start time:	16:37:56
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\QuotationOrder.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QuotationOrder.pdf.exe'
Imagebase:	0xf20000
File size:	850944 bytes
MD5 hash:	14E431BCB3FDB77CD13912A5CBEF9E40
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.243826185.00000000043B9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.243826185.00000000043B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.243826185.00000000043B9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.243971939.0000000004508000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.243971939.0000000004508000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.243971939.0000000004508000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.243530638.00000000033F4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D4FCF06	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	6D4FCF06	unknown
C:\Users\user\AppData\Roaming\RLaczhWDn.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	6C34DD66	CopyFileW
C:\Users\user\AppData\Roaming\RLaczhWDn.exe\:Zone.Identifier :$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C34DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpAF14.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C347038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ QuotationOrder.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D80C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAF14.tmp	success or wait	1	6C346A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RLaczhWDn.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 96 d2 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 4c 0b 00 00 ae 01 00 00 00 00 00 da 6b 0b 00 00 20 00 00 00 80 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....P..L...........k... ........@.. ......................` ....@.................	success or wait	4	6C34DD66	CopyFileW
C:\Users\user\AppData\Roaming\ RLaczhWDn.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	6C34DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAF14.tmp	unknown	1658	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	6C341B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QuotationOrder.pdf.exe.log	unknown	1314	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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D80C907	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	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D4D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D4DCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C341B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C341B4F	ReadFile

Analysis Process: schtasks.exe PID: 6348 Parent PID: 6248

General

Start time:	16:38:00
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RLaczhWDn' /XML 'C:\Users\user\AppData\Local\Temp\tmpAF14.tmp'
Imagebase:	0xef0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAF14.tmp	unknown	2	success or wait	1	EFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpAF14.tmp	unknown	1659	success or wait	1	EFABD9	ReadFile

Analysis Process: conhost.exe PID: 6356 Parent PID: 6348

General

Start time:	16:38:00
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 6400 Parent PID: 6248

General

Start time:	16:38:01
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0xd20000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

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	6D4FCF06	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	6D4FCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C34BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C341E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C34BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C34BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C341E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C341E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C341E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	c4 3a 1a fc 9e 15 d9 48	.:.....H	success or wait	1	6C341B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	6C341B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wp K .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.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C341B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6C341B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D4D5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D4D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D4DCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D4DCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D4DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C341B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C341B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	success or wait	1	6C341B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	end of file	1	6C341B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	4096	success or wait	1	6D4BD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	512	success or wait	1	6D4BD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D4D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D4D5705	unknown

Disassembly

Code Analysis