ID: 321077
Sample Name: Quotation ATB-PR28500KINH.exe
Cookbook: default.jbs
Time: 10:50:48
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

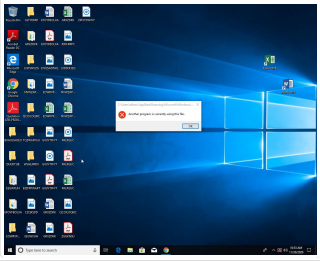
Analysis Report Quotation ATB-PR28500KINH.exe

Overview

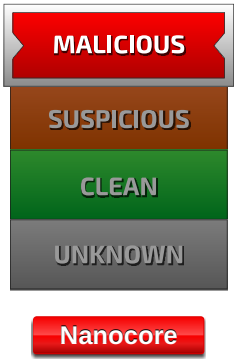
General Information

Sample Name:	Quotation ATB-PR28500KINH.exe
Analysis ID:	321077
MD5:	5a6b8a02021146..
SHA1:	7dc888c1f8a38a4..
SHA256:	7fa804f096ed67a..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

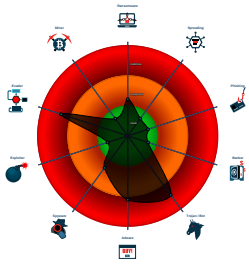


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Drops PE files to the startup folder
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …

Classification



Startup

- **System is w10x64**
- Quotation ATB-PR28500KINH.exe (PID: 6620 cmdline: 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe' MD5: 5A6B8A02021146DBE686B9A5EB628D9A)
  - RegAsm.exe (PID: 6880 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 6916 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - schtasks.exe (PID: 7012 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp21A1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Quotation ATB-PR28500KINH.exe (PID: 6988 cmdline: 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe' MD5: 5A6B8A02021146DBE686B9A5EB628D9A)
    - RegAsm.exe (PID: 7048 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- RegAsm.exe (PID: 7088 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe 0 MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - conhost.exe (PID: 7132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.315767298.0000000002F81000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000012.00000002.315767298.0000000002F81000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x6b44f:$a: NanoCore • 0x6b4a8:$a: NanoCore • 0x6b4e5:$a: NanoCore • 0x6b55e:$a: NanoCore • 0x6b4b1:$b: ClientPlugin • 0x6b4ee:$b: ClientPlugin • 0x6bdec:$b: ClientPlugin • 0x6bdf9:$b: ClientPlugin • 0x615ba:$e: KeepAlive • 0x6b939:$g: LogClientMessage • 0x6b8b9:$i: get_Connected • 0x5b885:$j: #=q • 0x5b8b5:$j: #=q • 0x5b8f1:$j: #=q • 0x5b919:$j: #=q • 0x5b949:$j: #=q • 0x5b979:$j: #=q • 0x5b9a9:$j: #=q • 0x5b9d9:$j: #=q • 0x5b9f5:$j: #=q • 0x5ba25:$j: #=q
00000000.00000002.512937029.00000000059E2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.512937029.00000000059E2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.512937029.00000000059E2000.00000040.00000001.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 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.RegAsm.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
4.2.RegAsm.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
4.2.RegAsm.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
4.2.RegAsm.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
0.2.Quotation ATB-PR28500KINH.exe.59e0000.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 19 entries				

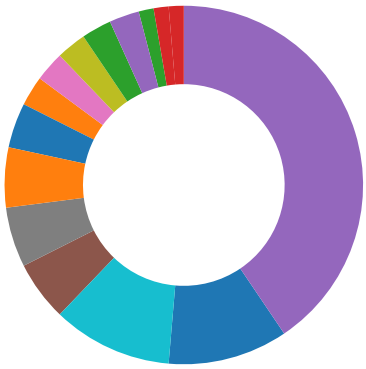
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

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

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

Boot Survival:

Drops PE files to the startup folder

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

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

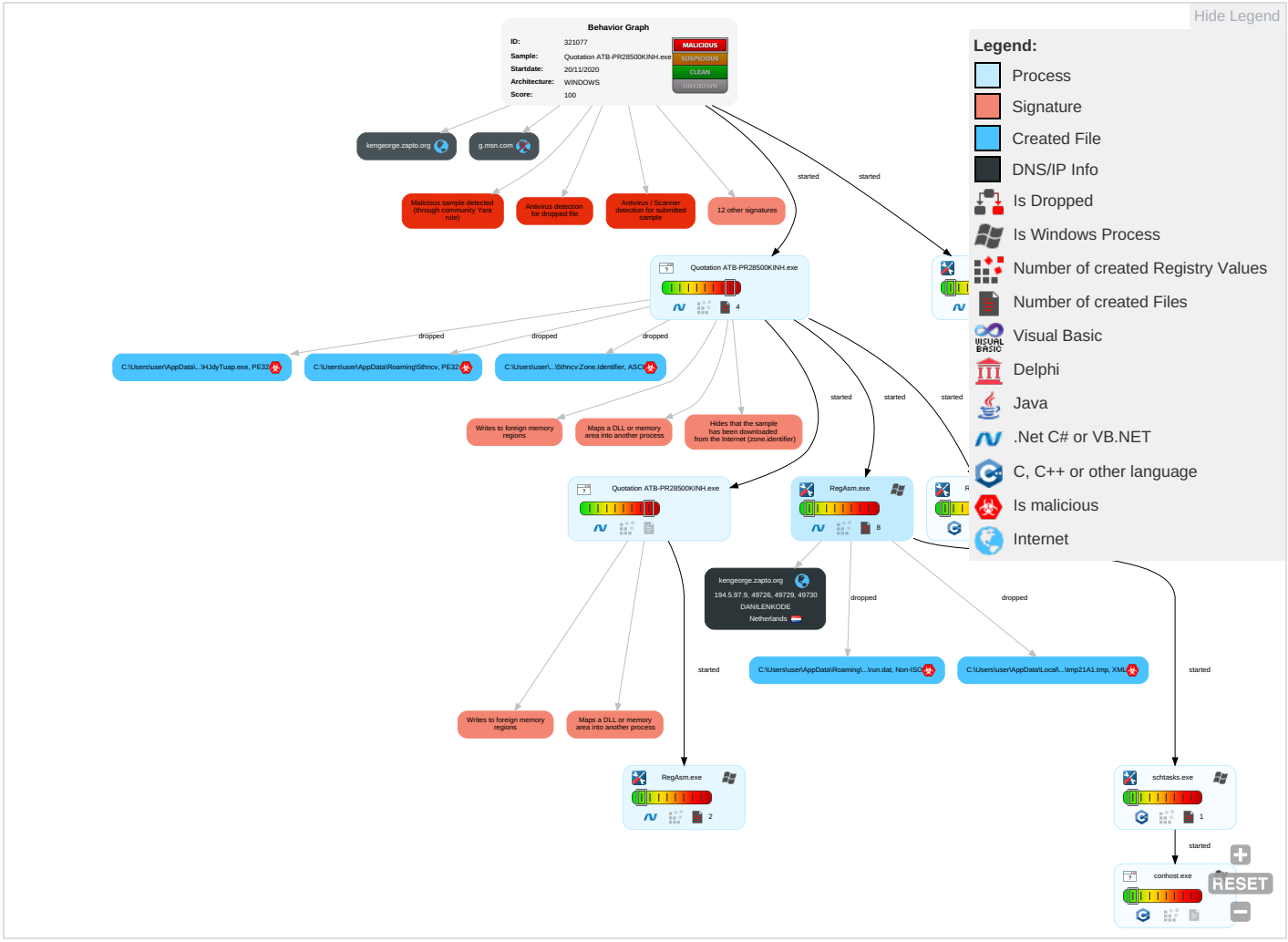
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Startup Items 1	Startup Items 1	Masquerading 1 1	Input Capture 1 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Scheduled Task/Job 1	Process Injection 2 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 1 2	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1 2	Process Injection 2 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Cloud Accounts	Cron	Network Logon Script	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

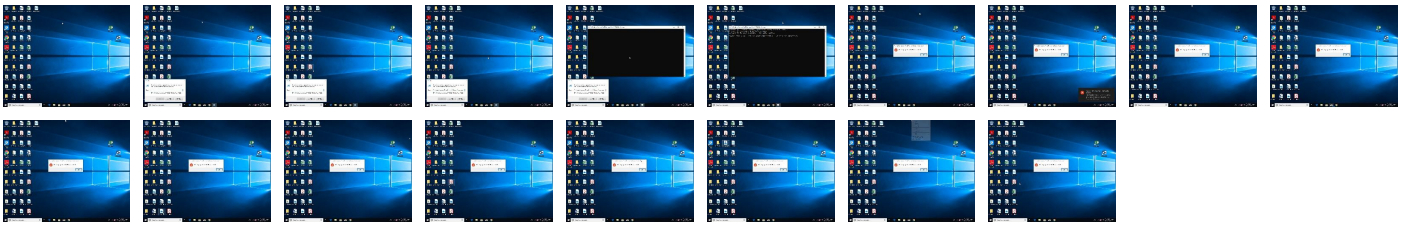
Behavior Graph



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
Quotation ATB-PR28500KINH.exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
Quotation ATB-PR28500KINH.exe	100%	Avira	TR/AD.Nanocore.bbyez	
Quotation ATB-PR28500KINH.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe	100%	Avira	TR/AD.Nanocore.bbyez	
C:\Users\user\AppData\Roaming\5thncv	100%	Avira	TR/AD.Nanocore.bbyez	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\5thncv	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\5thncv	27%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Quotation ATB-PR28500KINH.exe.5a80000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
18.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.Quotation ATB-PR28500KINH.exe.59e0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.RegAsm.exe.68a0000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kengeorge.zapto.org	194.5.97.9	true	false		unknown
g.msn.com	unknown	unknown	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.9	unknown	Netherlands		208476	DANILENKODE	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321077
Start date:	20.11.2020
Start time:	10:50:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation ATB-PR28500KINH.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.adwa.evad.winEXE@14/8@21/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 12.7% • Quality standard deviation: 9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.255.188.83, 23.210.248.85, 51.104.139.180, 51.103.5.159, 8.241.9.254, 8.253.204.120, 8.248.119.254, 8.248.113.254, 8.241.11.254, 8.241.11.126, 8.248.125.254, 8.248.117.254, 67.26.137.254, 52.155.217.156, 20.54.26.129, 52.142.114.176, 95.101.22.125, 95.101.22.134, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/321077/sample/Quotation ATB-PR28500KINH.exe

Simulations

Behavior and APIs

Time	Type	Description
10:51:51	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe
10:51:57	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" s>$(Arg0)
10:51:57	API Interceptor	917x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
kengeorge.zapto.org	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 185.140.53.139

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	19112020778IMG78487784.exe	Get hash	malicious	Browse	• 194.5.97.249
	PaymentConformation.exe	Get hash	malicious	Browse	• 194.5.97.202
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 194.5.98.122
	IMAGE-18112020.exe	Get hash	malicious	Browse	• 194.5.97.17
	Covid-19 relief.exe	Get hash	malicious	Browse	• 194.5.97.21
	tax-relief.exe	Get hash	malicious	Browse	• 194.5.97.166
	Ref-BID PRICE.exe	Get hash	malicious	Browse	• 194.5.98.252
	1ttmgYD97B.exe	Get hash	malicious	Browse	• 194.5.99.163
	2mtUEXin7W.exe	Get hash	malicious	Browse	• 194.5.99.163
	wk59hOo880.exe	Get hash	malicious	Browse	• 194.5.99.163
	BCVaSYrgmG.exe	Get hash	malicious	Browse	• 194.5.99.163
	30203490666.exe	Get hash	malicious	Browse	• 194.5.98.199
	InSppuoN2s.exe	Get hash	malicious	Browse	• 194.5.98.196
	Av01vC7kS1.exe	Get hash	malicious	Browse	• 194.5.97.155
	yb1rlaFJuO.exe	Get hash	malicious	Browse	• 194.5.99.163
	1MwYrZqjEy.exe	Get hash	malicious	Browse	• 194.5.99.163
	IRS-RELIEF.exe	Get hash	malicious	Browse	• 194.5.97.21
	Jvdivmn_Signed_.exe	Get hash	malicious	Browse	• 194.5.97.38
	myupsfile.exe	Get hash	malicious	Browse	• 194.5.97.38
	dO50wcBKmS.exe	Get hash	malicious	Browse	• 194.5.97.155

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177C E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Temp\tmp21A1.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1319
Entropy (8bit):	5.134254141338449
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mxz5xtn:cbk4oL600QydbQxIYODOLedq3Zxz5j

C:\Users\user\AppData\Local\Temp\tmp21A1.tmp	
MD5:	48EF7FA9033389AD7929D7A6B9D10298
SHA1:	9DB6CB7325C8BDF66A15F7B5F34703709A45AEB6
SHA-256:	0C1B5F67EEB276D1D4205B138CE32BC6149924E02281A2DB8E4623A700E88F15
SHA-512:	AC8BD104ECBACC9BCCCE9E087F67E5B18072D59367CCD31D4E66132B6BAAEA520CBA5B9B59464483D86ABF74826B382C402F12E9A586C99BDA8C78A0DE339 44E
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\5thncv	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1020928
Entropy (8bit):	6.7450135182284585
Encrypted:	false
SSDEEP:	12288:95B/zCKY12RnzFAsKibDzxr3Cz2GG3tjNl91JgE8ltd4Y0pnx1ld8C:dbC+z8i/zxrSz2FO91JgE8a4TFxH
MD5:	5A6B8A02021146DBE686B9A5EB628D9A
SHA1:	7DC888C1F8A38A4A7385F666FCEE60BAB258A869
SHA-256:	7FA804F096ED67A239A1FA164BA4A63F06B6FD52F3163C82F096CC12082ACCA9
SHA-512:	DD30026FEF52A4A5700144980C7805D1710E0A5EA504A167FDBC59129A781BE6CEA3DD565D95B2EAFE4D57A8991FEC00D121FD5ACFBB316690BCDB60719CFF 9F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...p._..... ... .@.. .....$H... .@.....t...W.... ..N..... ....H.....text..... ....`.rsrc...N.... .....@..@.reloc..... .....@..B.....H.....d.....q.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D.E.F.G.H.I.J .K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(.....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r9..p.....*6..{b... (^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

C:\Users\user\AppData\Roaming\5thncv:Zone.Identifier	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	Non-ISO extended-ASCII text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:F3t:F3t
MD5:	D137D5B6421522A3D19236A56ACCFF51
SHA1:	AE22E7372035E11079F2D03F1ADA51F98E2DA19E
SHA-256:	EF685074F06CB6D1AA010756AF124480A2621EBF53E542036F5A267BB2FEC86A
SHA-512:	405D130E38D0275E57DF0CAF6032923A5CA1C2D3E7D846B46AE04EC831C96D1CACDBBCC071F5C7F4D1AC46540CC6C26CE1EA7729680A8E979918650E5DF47 22

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Malicious:	**true**
Preview:	.D.Z...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	56
Entropy (8bit):	4.823079645651109
Encrypted:	false
SSDEEP:	3:oMty8WddSWAnPL4A:oMLW6WAnPL4A
MD5:	743A1D76D284D8E42E19061A3F13A723
SHA1:	D6BBE641CBAC7B46C0922F32DCC89F8F5B87F98C
SHA-256:	86093BF03032ACFCEF934A0D8363B66AAF4ADEE58015DA0172E13635B1DD1FE8
SHA-512:	DF687DCD985D1F6127624220083DFD93A39FEBCE02A869F4126787DF3724890ECC10FF18077BFDEF02FCC802440F3F83545E4DA4BD826DC84E59B26A105F656
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1024000
Entropy (8bit):	6.738941723536787
Encrypted:	false
SSDEEP:	12288:95B/zCKY12RnzFAsKibDzxr3Cz2GG3tjNI91JgE8Itd4Y0pnx1ld8C:dbC+z8i/zxrSz2FO91JgE8a4TFxH
MD5:	5F6F43FE7C5BDB4D77EFF131C8536E9B
SHA1:	3ED423034972EDF3518B97AFC64632FD4DC8419B
SHA-256:	82660B3E8BA370C6FAA0BF5ACB7C425F9C2D8CACC4194A0E9EE35F68D76D3239
SHA-512:	F61EF23DB4DAC90155D772E22E638CFE7D2C15BF37CE7DB7B0A79468F2489F921CD9E5E7281C96C5FB56A37B34631DCF745E4FF8B35BD9FF0F11FF009ADFDC1
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...p._..... ... .@.. .....$H... .@.....t...W.... ..N..... ....H.....text..... ....`.rsrc...N.... .....@..@.reloc..... .....@..B.....H.....d.....q.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D.E.F.G.H.I.J .K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r9..p.....*6..{b...(^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	275
Entropy (8bit):	4.839531074781769
Encrypted:	false
SSDEEP:	6:z30qJ5tUI+30qobtUmYRZBXVNYL0dxKaRFfnYJin:z30mc30b4BFNY4xNYU
MD5:	1B648D405C15ECA8CF1B9B0469B5627E
SHA1:	C6BBAEDE7AE2353E15271F1FBAA18588BEF0E922
SHA-256:	52FF7329D9E47BF7366892E79338FEE702C60D1F3ADB2EDDB601DFAEC8F170A0
SHA-512:	086EC3F608C80CDB6DC844366CFBBA5237ABCEB5306C0EF7C91600003F1A169CD94EB07D3680E943C9AC498CBA3845857756C5D745A66999BE78C263E5C440
Malicious:	false
Preview:	Microsoft .NET Framework Assembly Registration Utility version 4.7.3056.0..for Microsoft .NET Framework version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....RegAsm : error RA0000 : Unable to locate input assembly '0' or one of its dependencies...

Static File Info

General

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

General

Entropy (8bit):	6.7450135182284585
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:	Quotation ATB-PR28500KINH.exe
File size:	1020928
MD5:	5a6b8a02021146dbe686b9a5eb628d9a
SHA1:	7dc888c1f8a38a4a7385f666fcee60bab258a869
SHA256:	7fa804f096ed67a239a1fa164ba4a63f06b6fd52f3163c82f096cc12082acca9
SHA512:	dd30026fef52a4a5700144980c7805d1710e0a5ea504a167fdbc59129a781be6cea3dd565d95b2eafe4d57a8991fec00d121fd5acfbb316690bcdb60719cff9f
SSDEEP:	12288:95B/zCKY12RnzFAsKibDzxr3Cz2GG3tjNl91JgE8ltd4Y0pnx1ld8C:dbC+z8i/zxrSz2FO91JgE8a4TFxH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...p..._..... ... .@.. .....$H...@.....

File Icon

Icon Hash:	905ada12e9cc368b

Static PE Info

General

Entrypoint:	0x4a04ce
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:	0x5FB6F070 [Thu Nov 19 22:23:44 2020 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
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa0474	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x5a94e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xfe000	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	0x9e4d4	0x9e600	False	0.921844169298	data	7.86217054502	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x5a94e	0x5aa00	False	0.0372737068966	data	2.71520754372	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfe000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa21d8	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xe4200	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xe4668	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 2699173413, next used block 2699173413	English	United States
RT_ICON	0xe6c10	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 3236110116, next used block 3236110116	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe7cb8	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xf84e0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 2162368036, next used block 2162368036	English	United States
RT_GROUP_ICON	0xfc708	0x5a	data	English	United States
RT_MANIFEST	0xfc764	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 93

- 53 (DNS)
- 6184 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:52:02.466367960 CET	49726	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:02.496193886 CET	6184	49726	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:03.184657097 CET	49726	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:03.214612007 CET	6184	49726	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:03.784126043 CET	49726	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:03.813864946 CET	6184	49726	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:08.033576965 CET	49729	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:08.064066887 CET	6184	49729	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:08.723309994 CET	49729	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:08.753233910 CET	6184	49729	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:09.410831928 CET	49729	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:09.441014051 CET	6184	49729	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:13.485429049 CET	49730	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:13.515448093 CET	6184	49730	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:14.020757914 CET	49730	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:14.050601959 CET	6184	49730	194.5.97.9	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:52:14.551795959 CET	49730	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:14.581655025 CET	6184	49730	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:18.705220938 CET	49731	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:18.735104084 CET	6184	49731	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:19.239630938 CET	49731	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:19.269522905 CET	6184	49731	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:19.770930052 CET	49731	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:19.800921917 CET	6184	49731	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:23.858556032 CET	49732	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:23.888431072 CET	6184	49732	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:24.396251917 CET	49732	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:24.426213026 CET	6184	49732	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:24.927702904 CET	49732	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:24.957645893 CET	6184	49732	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:29.029927015 CET	49736	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:29.059813023 CET	6184	49736	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:29.568558931 CET	49736	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:29.598489046 CET	6184	49736	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:30.099837065 CET	49736	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:30.129645109 CET	6184	49736	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:34.375207901 CET	49743	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:34.405150890 CET	6184	49743	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:35.007620096 CET	49743	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:35.037687063 CET	6184	49743	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:35.620990038 CET	49743	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:35.650985956 CET	6184	49743	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:39.703183889 CET	49749	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:39.733134031 CET	6184	49749	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:40.241233110 CET	49749	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:40.271064997 CET	6184	49749	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:40.772504091 CET	49749	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:40.802356958 CET	6184	49749	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:44.845530033 CET	49756	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:47.851152897 CET	49756	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:53.867326021 CET	49756	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:54.051198959 CET	6184	49756	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:58.141248941 CET	49757	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:58.330878973 CET	6184	49757	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:58.836340904 CET	49757	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:59.020982981 CET	6184	49757	194.5.97.9	192.168.2.5
Nov 20, 2020 10:52:59.523906946 CET	49757	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:52:59.709059000 CET	6184	49757	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:03.754981995 CET	49760	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:03.946958065 CET	6184	49760	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:04.461786985 CET	49760	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:04.668989897 CET	6184	49760	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:05.180625916 CET	49760	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:05.370690107 CET	6184	49760	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:09.424768925 CET	49761	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:09.610785961 CET	6184	49761	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:10.119046926 CET	49761	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:10.300734997 CET	6184	49761	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:10.806098938 CET	49761	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:10.990715027 CET	6184	49761	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:15.088957071 CET	49762	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:15.280740976 CET	6184	49762	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:15.790833950 CET	49762	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:15.998838902 CET	6184	49762	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:16.509627104 CET	49762	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:16.690829992 CET	6184	49762	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:20.757941008 CET	49763	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:20.940715075 CET	6184	49763	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:21.447537899 CET	49763	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:21.640497923 CET	6184	49763	194.5.97.9	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:53:22.150638103 CET	49763	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:22.350904942 CET	6184	49763	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:26.629566908 CET	49764	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:26.818627119 CET	6184	49764	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:27.447866917 CET	49764	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:27.648524046 CET	6184	49764	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:28.151122093 CET	49764	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:28.350675106 CET	6184	49764	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:32.552192926 CET	49765	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:32.748727083 CET	6184	49765	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:33.260946035 CET	49765	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:33.460822105 CET	6184	49765	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:33.964111090 CET	49765	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:34.140450001 CET	6184	49765	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:38.247296095 CET	49766	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:38.430479050 CET	6184	49766	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:38.933101892 CET	49766	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:39.131073952 CET	6184	49766	194.5.97.9	192.168.2.5
Nov 20, 2020 10:53:39.636411905 CET	49766	6184	192.168.2.5	194.5.97.9
Nov 20, 2020 10:53:39.820441008 CET	6184	49766	194.5.97.9	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:51:38.788116932 CET	49992	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:51:38.815205097 CET	53	49992	8.8.8.8	192.168.2.5
Nov 20, 2020 10:51:39.880928993 CET	60075	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:51:39.908036947 CET	53	60075	8.8.8.8	192.168.2.5
Nov 20, 2020 10:51:55.739993095 CET	55016	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:51:55.777512074 CET	53	55016	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:02.374857903 CET	64345	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:02.412364006 CET	53	64345	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:06.545293093 CET	57128	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:06.572278976 CET	53	57128	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:07.995281935 CET	54791	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:08.032438040 CET	53	54791	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:13.445796967 CET	50463	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:13.483804941 CET	53	50463	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:18.668350935 CET	50394	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:18.703979015 CET	53	50394	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:23.822185040 CET	58530	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:23.857530117 CET	53	58530	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:25.016227961 CET	53813	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:25.053634882 CET	53	53813	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:25.163535118 CET	63732	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:25.190555096 CET	53	63732	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:25.247749090 CET	57344	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:25.274890900 CET	53	57344	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:28.992866993 CET	54450	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:29.028661966 CET	53	54450	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:31.312700033 CET	59261	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:31.348434925 CET	53	59261	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:31.952512980 CET	57151	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:31.979826927 CET	53	57151	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:32.442549944 CET	59413	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:32.478214025 CET	53	59413	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:32.830388069 CET	60516	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:32.857480049 CET	53	60516	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:33.274805069 CET	51649	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:33.310241938 CET	53	51649	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:33.727365971 CET	65086	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:33.763178110 CET	53	65086	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:34.332396984 CET	56432	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:34.368335009 CET	53	56432	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:52:34.549232006 CET	52929	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:34.595470905 CET	53	52929	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:35.678245068 CET	64317	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:35.714148998 CET	53	64317	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:37.744891882 CET	61004	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:37.780716896 CET	53	61004	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:38.269572020 CET	56895	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:38.280118942 CET	62372	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:38.305378914 CET	53	56895	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:38.323765039 CET	53	62372	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:39.666395903 CET	61515	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:39.702186108 CET	53	61515	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:40.541301012 CET	56675	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:40.585426092 CET	53	56675	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:40.723639011 CET	57172	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:40.761017084 CET	53	57172	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:44.808027983 CET	55267	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:44.843740940 CET	53	55267	8.8.8.8	192.168.2.5
Nov 20, 2020 10:52:58.099848986 CET	50969	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:52:58.135505915 CET	53	50969	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:00.573663950 CET	64362	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:00.600734949 CET	53	64362	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:01.550841093 CET	54766	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:01.594623089 CET	53	54766	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:03.715306997 CET	61446	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:03.753169060 CET	53	61446	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:09.388045073 CET	57515	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:09.423793077 CET	53	57515	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:15.049813032 CET	58199	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:15.087260008 CET	53	58199	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:20.718812943 CET	65221	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:20.756669998 CET	53	65221	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:26.427288055 CET	61573	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:26.463021040 CET	53	61573	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:32.515227079 CET	56562	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:32.550981045 CET	53	56562	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:38.155330896 CET	53591	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:38.190993071 CET	53	53591	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:43.952354908 CET	59688	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:43.990181923 CET	53	59688	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:49.701139927 CET	56032	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:49.736870050 CET	53	56032	8.8.8.8	192.168.2.5
Nov 20, 2020 10:53:55.361381054 CET	61150	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:53:55.396862030 CET	53	61150	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 10:52:02.374857903 CET	192.168.2.5	8.8.8.8	0xc3a3	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:07.995281935 CET	192.168.2.5	8.8.8.8	0x1d8b	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:13.445796967 CET	192.168.2.5	8.8.8.8	0xc2aa	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:18.668350935 CET	192.168.2.5	8.8.8.8	0xd980	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:23.822185040 CET	192.168.2.5	8.8.8.8	0x638b	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:28.992866993 CET	192.168.2.5	8.8.8.8	0x7c40	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:34.332396984 CET	192.168.2.5	8.8.8.8	0x62fa	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:39.666395903 CET	192.168.2.5	8.8.8.8	0x6f9f	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:40.541301012 CET	192.168.2.5	8.8.8.8	0xb80a	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 10:52:44.808027983 CET	192.168.2.5	8.8.8.8	0x89cd	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:58.099848986 CET	192.168.2.5	8.8.8.8	0xb049	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:03.715306997 CET	192.168.2.5	8.8.8.8	0xab7c	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:09.388045073 CET	192.168.2.5	8.8.8.8	0x963b	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:15.049813032 CET	192.168.2.5	8.8.8.8	0x78b1	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:20.718812943 CET	192.168.2.5	8.8.8.8	0x9c6b	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:26.427288055 CET	192.168.2.5	8.8.8.8	0xbcfc	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:32.515227079 CET	192.168.2.5	8.8.8.8	0xa06b	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:38.155330896 CET	192.168.2.5	8.8.8.8	0xa01	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:43.952354908 CET	192.168.2.5	8.8.8.8	0x91fe	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:49.701139927 CET	192.168.2.5	8.8.8.8	0x4484	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:55.361381054 CET	192.168.2.5	8.8.8.8	0x3fce	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)

DNS Answers

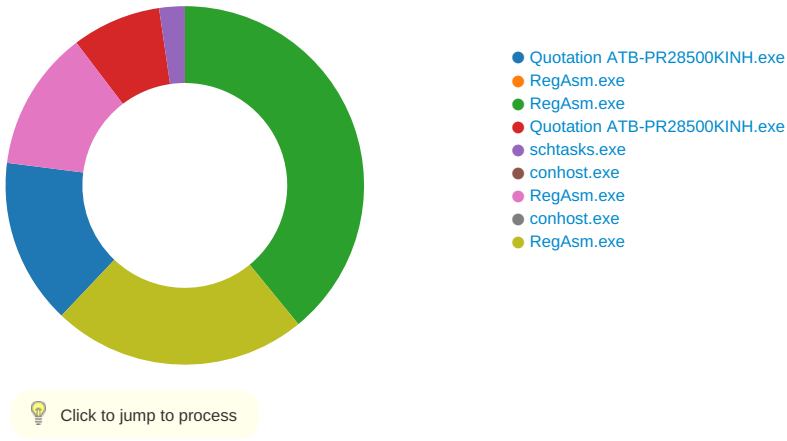
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 10:52:02.412364006 CET	8.8.8.8	192.168.2.5	0xc3a3	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:08.032438040 CET	8.8.8.8	192.168.2.5	0x1d8b	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:13.483804941 CET	8.8.8.8	192.168.2.5	0xc2aa	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:18.703979015 CET	8.8.8.8	192.168.2.5	0xd980	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:23.857530117 CET	8.8.8.8	192.168.2.5	0x638b	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:29.028661966 CET	8.8.8.8	192.168.2.5	0x7c40	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:34.368335009 CET	8.8.8.8	192.168.2.5	0x62fa	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:39.702186108 CET	8.8.8.8	192.168.2.5	0x6f9f	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:40.585426092 CET	8.8.8.8	192.168.2.5	0xb80a	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 10:52:44.843740940 CET	8.8.8.8	192.168.2.5	0x89cd	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:52:58.135505915 CET	8.8.8.8	192.168.2.5	0xb049	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:03.753169060 CET	8.8.8.8	192.168.2.5	0xab7c	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:09.423793077 CET	8.8.8.8	192.168.2.5	0x963b	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:15.087260008 CET	8.8.8.8	192.168.2.5	0x78b1	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:20.756669998 CET	8.8.8.8	192.168.2.5	0x9c6b	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:26.463021040 CET	8.8.8.8	192.168.2.5	0xbcfc	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 10:53:32.550981045 CET	8.8.8.8	192.168.2.5	0xa06b	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:38.190993071 CET	8.8.8.8	192.168.2.5	0xa01	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:43.990181923 CET	8.8.8.8	192.168.2.5	0x91fe	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:49.736870050 CET	8.8.8.8	192.168.2.5	0x4484	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:55.396862030 CET	8.8.8.8	192.168.2.5	0x3fce	No error (0)	kengeorge.zapto.org		194.5.97.9	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Quotation ATB-PR28500KINH.exe PID: 6620 Parent PID: 5672

General

Start time:	10:51:43
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe'
Imagebase:	0xf90000
File size:	1020928 bytes
MD5 hash:	5A6B8A02021146DBE686B9A5EB628D9A
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: 00000000.00000002.512937029.00000000059E2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.512937029.00000000059E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.512937029.00000000059E2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.511212576.0000000004381000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.511212576.0000000004381000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.511212576.0000000004381000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.513612076.0000000005D3C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.513612076.0000000005D3C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.513612076.0000000005D3C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\5thncv	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	6CB4DD66	CopyFileW
C:\Users\user\AppData\Roaming\5thncv\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CB4DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe	write data or add file | append data or add subdirectory or create pipe instance | write ea | write attributes | read control | synchronize	device	non directory file	success or wait	1	59C201B	NtCreateFile

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\5thncv:Zone.Identifier	success or wait	1	1799359	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\5thncv	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 70 f0 b6 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e6 09 00 00 ac 05 00 00 00 00 00 ce 04 0a 00 00 20 00 00 00 20 0a 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 00 10 00 00 02 00 00 24 48 10 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...p.._.......... ....@.. ....$H....@.................	success or wait	4	6CB4DD66	CopyFileW
C:\Users\user\AppData\Roaming\5thncv: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	6CB4DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe	0	1024000	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 70 f0 b6 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e6 09 00 00 ac 05 00 00 00 00 00 ce 04 0a 00 00 20 00 00 00 20 0a 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 00 10 00 00 02 00 00 24 48 10 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...p.._.......... ....@.. ....$H....@.................	pending	1	59C204E	NtWriteFile

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	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCD5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC303DE	ReadFile
C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	0	1024000	pending	1	59C1D6A	NtReadFile

Analysis Process: RegAsm.exe PID: 6880 Parent PID: 6620

General

Start time:	10:51:54
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x150000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: 6916 Parent PID: 6620

General

Start time:	10:51:55
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xf50000
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: 00000004.00000002.511598900.0000000004299000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.511598900.0000000004299000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.514616448.00000000068A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.514616448.00000000068A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.514616448.00000000068A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.504689843.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.504689843.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.504689843.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.513526465.0000000005940000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.513526465.0000000005940000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.507695159.0000000003291000.00000004.00000001.sdmp, Author: Joe Security
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	6DCFCF06	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	6DCFCF06	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	6CB4BEFF	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	6CB41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp21A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB47038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CB41E60	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	6CB4BEFF	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	6CB4BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp21A1.tmp	success or wait	1	6CB46A95	DeleteFileW

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	99 44 d5 5a 85 8d d8 48	.D.Z...H	success or wait	1	6CB41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp21A1.tmp	unknown	1319	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6CB41B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	56	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 52 65 67 41 73 6d 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	success or wait	1	6CB41B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DCDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC303DE	ReadFile

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	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6CB41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6CB41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	unknown	4096	success or wait	1	6DCBD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	unknown	512	success or wait	1	6DCBD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DCD5705	unknown

Analysis Process: Quotation ATB-PR28500KINH.exe PID: 6988 Parent PID: 6620

General

Start time:	10:51:56
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe'
Imagebase:	0xc50000
File size:	1020928 bytes
MD5 hash:	5A6B8A02021146DBE686B9A5EB628D9A
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: 00000005.00000002.511416569.0000000003FF1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.511416569.0000000003FF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.511416569.0000000003FF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.517841818.0000000005A82000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.517841818.0000000005A82000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.517841818.0000000005A82000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.506085283.0000000001233000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.506085283.0000000001233000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.506085283.0000000001233000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	1024000	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 70 f0 b6 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e6 09 00 00 ac 05 00 00 00 00 00 ce 04 0a 00 00 20 00 00 00 20 0a 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 00 10 00 00 02 00 00 24 48 10 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ....................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...p.._.......... ....@.. ....$H....@................	invalid handle	1	57C204E	NtWriteFile

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	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC303DE	ReadFile
C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	0	1024000	pending	1	57C1D6A	NtReadFile

Analysis Process: schtasks.exe PID: 7012 Parent PID: 6916

General

Start time:	10:51:56
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp21A1.tmp'
Imagebase:	0xb50000
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\tmp21A1.tmp	unknown	2	success or wait	1	B5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp21A1.tmp	unknown	1320	success or wait	1	B5ABD9	ReadFile

Analysis Process: conhost.exe PID: 7036 Parent PID: 7012

General

Start time:	10:51:57
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: RegAsm.exe PID: 7088 Parent PID: 904

General

Start time:	10:51:57
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe 0
Imagebase:	0x7ff797770000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E00C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CB41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	186	4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 41 73 73 65 6d 62 6c 79 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 76 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 76 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft .NET Framework Assembly Registration Utility version 4.7.3056.0..for Microsoft . NET Framework version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CB41B4F	WriteFile
\Device\ConDrv	unknown	0			success or wait	1	6CB41B4F	WriteFile
\Device\ConDrv	unknown	89	52 65 67 41 73 6d 20 3a 20 65 72 72 6f 72 20 52 41 30 30 30 30 20 3a 20 55 6e 61 62 6c 65 20 74 6f 20 6c 6f 63 61 74 65 20 69 6e 70 75 74 20 61 73 73 65 6d 62 6c 79 20 27 30 27 20 6f 72 20 6f 6e 65 20 6f 66 20 69 74 73 20 64 65 70 65 6e 64 65 6e 63 69 65 73 2e 0d 0a	RegAsm : error RA0000 : Unable to locate input assembly '0' or one of its dependencies...	success or wait	1	6CB41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	unknown	42	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	1,"fusion","GAC",0..1,"WinRT","NotApp",1..	success or wait	1	6E00C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC303DE	ReadFile

Analysis Process: conhost.exe PID: 7132 Parent PID: 7088

General

Start time:	10:51:58
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: RegAsm.exe PID: 7048 Parent PID: 6988

General

Start time:	10:52:11
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xc50000
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: 00000012.00000002.315767298.0000000002F81000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.315767298.0000000002F81000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.315860307.0000000003F89000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.315860307.0000000003F89000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.315053355.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.315053355.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.315053355.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.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	6DCFCF06	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	6DCFCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DCDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6CB41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6CB41B4F	ReadFile

Disassembly

Code Analysis