ID: 321029
Sample Name: Quotation ATB-PR28500KINH.exe
Cookbook: default.jbs
Time: 09:25:51
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

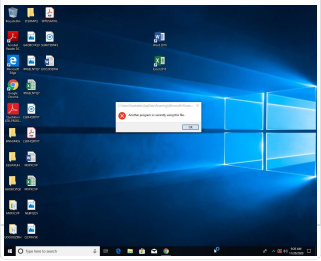
Analysis Report Quotation ATB-PR28500KINH.exe

Overview

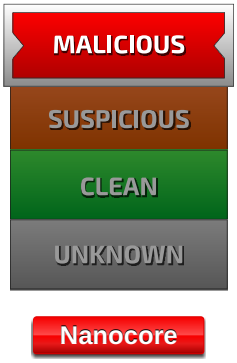
General Information

Sample Name:	Quotation ATB-PR28500KINH.exe
Analysis ID:	321029
MD5:	ddb5d5410477cd..
SHA1:	5fc06ec885cafa6..
SHA256:	9f76f4b990ce938..
Tags:	exe NanoCore nVpn RAT

Most interesting Screenshot:



Detection

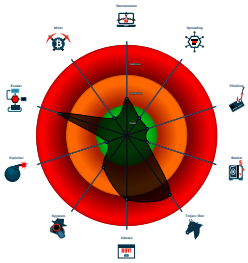


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- 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: 7036 cmdline: 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe' MD5: DDB5D5410477CD3855A1F542112808C0)
  - RegAsm.exe (PID: 3392 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - schtasks.exe (PID: 5816 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpAC5D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Quotation ATB-PR28500KINH.exe (PID: 6248 cmdline: 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe' MD5: DDB5D5410477CD3855A1F542112808C0)
    - RegAsm.exe (PID: 7160 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- RegAsm.exe (PID: 6200 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe 0 MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - conhost.exe (PID: 6396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "185.140.53.139"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.304004800.0000000002D41000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.304004800.0000000002D41000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x6b457:$a: NanoCore • 0x6b4b0:$a: NanoCore • 0x6b4ed:$a: NanoCore • 0x6b566:$a: NanoCore • 0x6b4b9:$b: ClientPlugin • 0x6b4f6:$b: ClientPlugin • 0x6bdf4:$b: ClientPlugin • 0x6be01:$b: ClientPlugin • 0x615c2:$e: KeepAlive • 0x6b941:$g: LogClientMessage • 0x6b8c1:$i: get_Connected • 0x5b88d:$j: #=q • 0x5b8bd:$j: #=q • 0x5b8f9:$j: #=q • 0x5b921:$j: #=q • 0x5b951:$j: #=q • 0x5b981:$j: #=q • 0x5b9b1:$j: #=q • 0x5b9e1:$j: #=q • 0x5b9fd:$j: #=q • 0x5ba2d:$j: #=q
00000001.00000002.503999050.00000000040E9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.503999050.00000000040E9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x359d:$a: NanoCore • 0x35f6:$a: NanoCore • 0x3633:$a: NanoCore • 0x36ac:$a: NanoCore • 0x16d57:$a: NanoCore • 0x16d6c:$a: NanoCore • 0x16da1:$a: NanoCore • 0x2fd33:$a: NanoCore • 0x2fd48:$a: NanoCore • 0x2fd7d:$a: NanoCore • 0x35ff:$b: ClientPlugin • 0x363c:$b: ClientPlugin • 0x3f3a:$b: ClientPlugin • 0x3f47:$b: ClientPlugin • 0x16b13:$b: ClientPlugin • 0x16b2e:$b: ClientPlugin • 0x16b5e:$b: ClientPlugin • 0x16d75:$b: ClientPlugin • 0x16daa:$b: ClientPlugin • 0x2faef:$b: ClientPlugin • 0x2fb0a:$b: ClientPlugin
00000000.00000002.497351250.0000000000B1E000.00000004.00000020.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4b17d:$x1: NanoCore.ClientPluginHost • 0x4b1ba:$x2: IClientNetworkHost • 0x4eced:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 42 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.RegAsm.exe.6670000.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
1.2.RegAsm.exe.6670000.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
1.2.RegAsm.exe.6670000.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.RegAsm.exe.5aa0000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
1.2.RegAsm.exe.5aa0000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 19 entries				

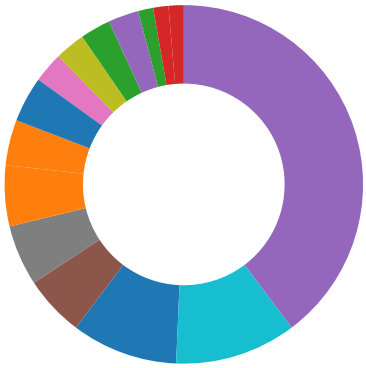
Sigma Overview

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:

- 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

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:

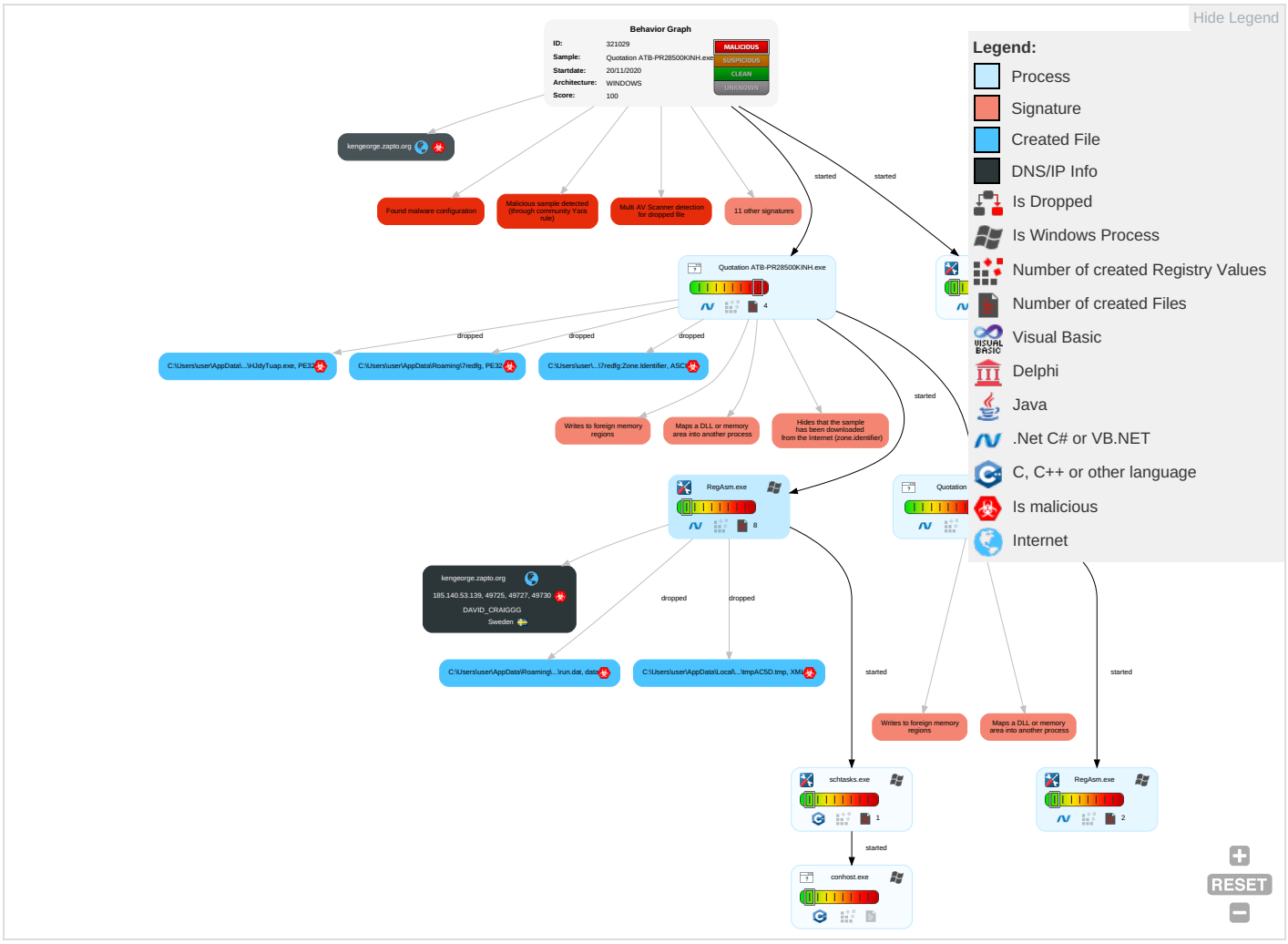
Detected Nanocore Rat

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
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

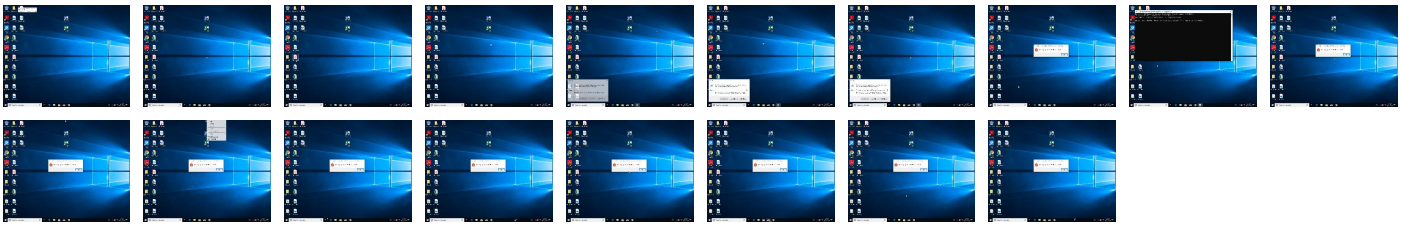
Behavior Graph



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.AgentTesla	
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%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\7redfg	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\7redfg	27%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.Quotation ATB-PR28500KINH.exe.5340000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.Quotation ATB-PR28500KINH.exe.5b40000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

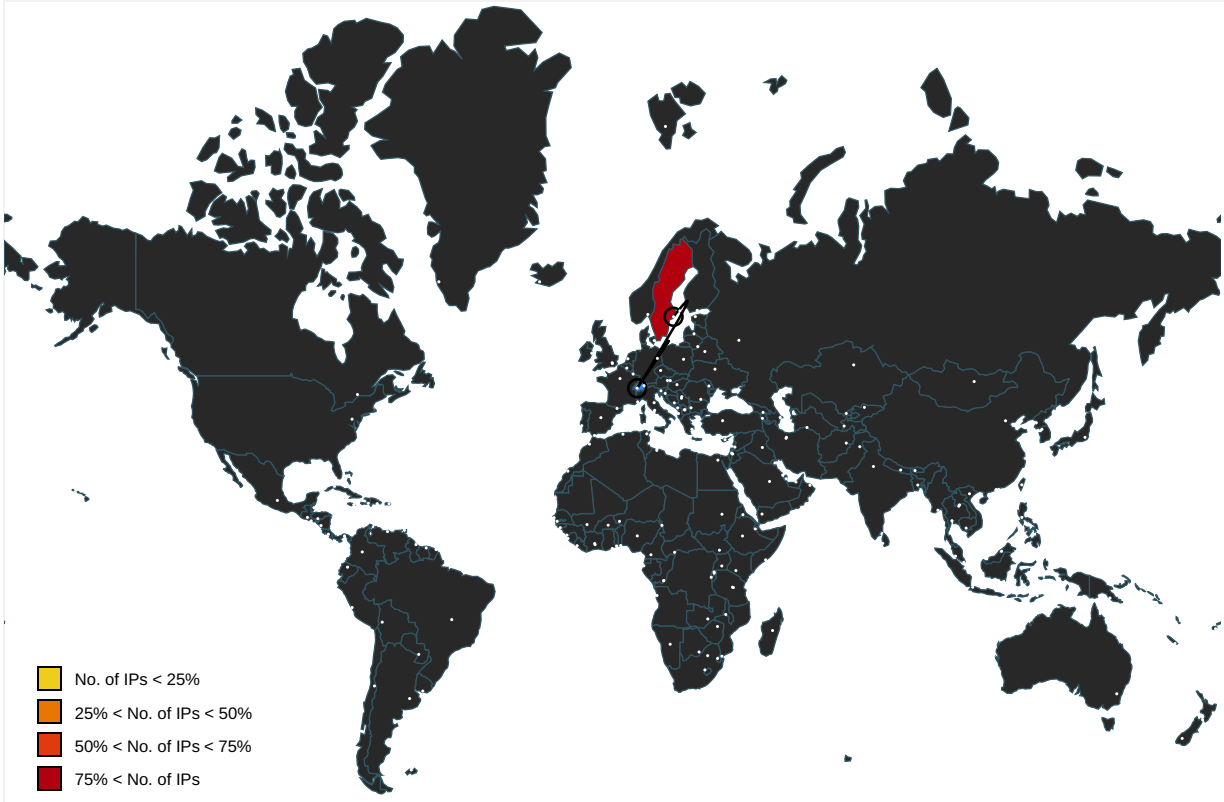
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kengeorge.zapto.org	185.140.53.139	true	true		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.139	unknown	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321029
Start date:	20.11.2020
Start time:	09:25:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 0s
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:	27
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@12/8@23/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.4%) • Quality average: 70.5% • Quality standard deviation: 17.4%
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): 13.64.90.137, 13.88.21.125, 92.122.144.200, 51.104.139.180, 8.248.113.254, 8.253.95.249, 8.241.122.254, 8.248.115.254, 8.248.121.254, 40.67.254.36, 52.155.217.156, 20.54.26.129, 95.101.22.134, 95.101.22.125, 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, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, db5p.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, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, 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, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:26:49	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe
09:26:55	API Interceptor	963x Sleep call for process: RegAsm.exe modified
09:26:56	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.139	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	
	RFQ-BOHB-SS-FD6L4.exe	Get hash	malicious	Browse	
	PURCHASE_FABRICS_APPAREL_100%_COOTON.exe	Get hash	malicious	Browse	
	GT-082568-HSO-280820.DOCX.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 185.140.53.139
	Ups file de.exe	Get hash	malicious	Browse	• 185.140.53.221
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 185.140.53.149
	purchase order.exe	Get hash	malicious	Browse	• 185.140.53.233
	Remittance Details.xls	Get hash	malicious	Browse	• 185.140.53.184
	PaymentConfirmation.exe	Get hash	malicious	Browse	• 185.140.53.183
	ORDER #02676.doc.exe	Get hash	malicious	Browse	• 185.244.30.92
	b11305c6ab207f830062f80eeec728c4.exe	Get hash	malicious	Browse	• 185.140.53.233
	ShippingDoc.jar	Get hash	malicious	Browse	• 185.244.30.139
	1kn1ejwPxi.exe	Get hash	malicious	Browse	• 185.140.53.132
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 185.140.53.149
	7iatifHQEp.exe	Get hash	malicious	Browse	• 185.140.53.132
	Sbext4ZNBq.exe	Get hash	malicious	Browse	• 185.140.53.197
	xEdiPz1bC3.exe	Get hash	malicious	Browse	• 185.140.53.234
	7D1wvBrRib.exe	Get hash	malicious	Browse	• 185.140.53.234
	O8LDCTOK07.exe	Get hash	malicious	Browse	• 185.140.53.233
	aE78QTkV5H.exe	Get hash	malicious	Browse	• 185.244.30.98
	DHL Shipment Notice of Arrival AWB 8032697940773.js	Get hash	malicious	Browse	• 185.165.153.158
	ORDER-#00654.doc.....exe	Get hash	malicious	Browse	• 185.165.153.116
	SMJshb9rCD.exe	Get hash	malicious	Browse	• 185.140.53.154

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

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\tmpAC5D.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
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\7redfg	
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):	1020416
Entropy (8bit):	6.746514435463881
Encrypted:	false
SSDEEP:	24576:MbHvzJzELhKXqKNxNTmV3s03o1+pUfOA:MzzJYLhKlpmV3s6o1UUfP
MD5:	DDB5D5410477CD3855A1F542112808C0
SHA1:	5FC06EC885CAFA6E8F955651B9E2115B705B2B4D
SHA-256:	9F76F4B990CE938D48B11501AD00D99795B172B44B1F94EA7CA3A26CEB64C1D5
SHA-512:	E9C60CC1C03D40C7C45C53FC5A78F1E8B801572A0FDDE422FBF8F80BCC8EEE89C023C48398A15D388275CF6589F6BAAB42E511933ACAD3B3C94CBE4B3D1F8 9B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....]._..... ... .@.. ....@.....D...W.... ..N..... ....H.....text..... ....`.rsrc...N.... .....@..@.rel oc.....@..B.....H.....pc.....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....*.(....*.(....*.r/..p.....*6..{b...(^.. .*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

C:\Users\user\AppData\Roaming\7redfg:Zone.Identifier	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Roaming\7redfg:Zone.Identifier	
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:tccgt:ttgt
MD5:	D47A6CEF4DA0DC89FA704BAE78647F81
SHA1:	E938FA778A75E957E694F7BBE15A8EAA0B0B96EA
SHA-256:	5C74BB1765AD749D734E7096ABA5C913996CAB20EC42EB3637F8C8DACEA9BDD1
SHA-512:	4D9E7F9E56C3F7CFB64EEDD5078ECF762FEF4093493ECC54290395EC3DF64453E603537DC57246A819CF7A8A5C5D2E007D7455ACAEB894A3D4C4ABE1048D33 6
Malicious:	**true**
Reputation:	low
Preview:	K..yy..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
Reputation:	moderate, very likely benign file
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):	6.739426849800377
Encrypted:	false
SSDEEP:	24576:MbHvzJzELhKXqKNxNTmV3s03o1+pUfOA:MzzJYLhKlpmV3s6o1UUfP
MD5:	E8989A1CE5543A7E4693DD416A46BE22
SHA1:	FD0B198079671C3D6C6B01802B9240E8EF80475B
SHA-256:	676AE550EFF3F5D6E6520604EDD804C606213EB2C5B8B93D449309BEA9B09CC0
SHA-512:	F3B7F5F8723B3CDAA47D2B1E53B7E96275E3CD9888F37D05D9C654873E3EC434F21140C3E1986FF519EEA5F962C028B0777F10019329C1BC524CAFFA79FD4CC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....]._..... ... .@.. ....@.....D...W.... ..N..... ....H.....text..... ....`.rsrc...N.... .....@..@.rel oc.....@..B.....H.....pc.....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....*.(....*.(....*.(....*.r/..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
Entropy (8bit):	6.746514435463881
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:	1020416
MD5:	ddb5d5410477cd3855a1f542112808c0
SHA1:	5fc06ec885cafa6e8f955651b9e2115b705b2b4d
SHA256:	9f76f4b990ce938d48b11501ad00d99795b172b44b1f94ea7ca3a26ceb64c1d5
SHA512:	e9c60cc1c03d40c7c45c53fc5a78f1e8b801572a0fdde422fbf8f80bcc8eee89c023c48398a15d388275cf6589f6baab42e511933acad3b3c94cbe4b3d1f819b
SSDEEP:	24576:MbHvzJzELhKXqKNxNTmV3s03o1+pUfOA:MzzJYLhKlpmV3s6o1UUfP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....]._..... ... .@.. ..... @.....

File Icon

Icon Hash:	905ada12e9cc368b

Static PE Info

General

Entrypoint:	0x4a039e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB75DD0 [Fri Nov 20 06:10:24 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa0344	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x9e3a4	0x9e400	False	0.921722267476	data	7.86314578381	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
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

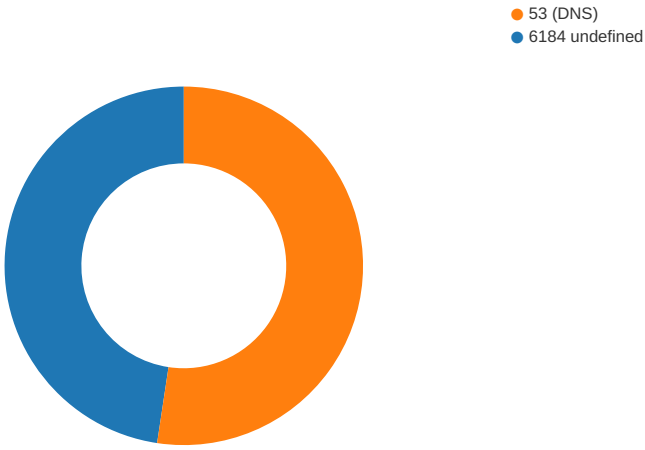
Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 105



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 09:26:56.135529041 CET	49725	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:26:56.161993980 CET	6184	49725	185.140.53.139	192.168.2.7
Nov 20, 2020 09:26:56.667889118 CET	49725	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:26:56.694283962 CET	6184	49725	185.140.53.139	192.168.2.7
Nov 20, 2020 09:26:57.198714972 CET	49725	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:26:57.224991083 CET	6184	49725	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:02.588973999 CET	49727	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:02.615282059 CET	6184	49727	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:03.121628046 CET	49727	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:03.148569107 CET	6184	49727	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:03.652827978 CET	49727	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:03.679325104 CET	6184	49727	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:07.725398064 CET	49730	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:07.751748085 CET	6184	49730	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:08.262631893 CET	49730	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:08.288739920 CET	6184	49730	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:08.793904066 CET	49730	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:08.820143938 CET	6184	49730	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:12.901868105 CET	49731	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:12.930203915 CET	6184	49731	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:13.434906960 CET	49731	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:13.463443995 CET	6184	49731	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:13.974385977 CET	49731	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:14.003876925 CET	6184	49731	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:18.046519995 CET	49732	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:18.072860003 CET	6184	49732	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:18.701004982 CET	49732	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:18.727283001 CET	6184	49732	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:19.310412884 CET	49732	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:19.336898088 CET	6184	49732	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:23.383054972 CET	49733	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:23.410958052 CET	6184	49733	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:23.920149088 CET	49733	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:23.948600054 CET	6184	49733	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:24.451509953 CET	49733	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:24.478183985 CET	6184	49733	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:28.548549891 CET	49736	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:28.574753046 CET	6184	49736	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:29.093298912 CET	49736	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:29.120059013 CET	6184	49736	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:29.655231953 CET	49736	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:29.681921959 CET	6184	49736	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:33.734447002 CET	49738	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:33.760849953 CET	6184	49738	185.140.53.139	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 09:27:34.277954102 CET	49738	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:34.304286003 CET	6184	49738	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:34.983653069 CET	49738	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:35.009541035 CET	6184	49738	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:39.057404995 CET	49749	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:39.083404064 CET	6184	49749	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:39.593693018 CET	49749	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:39.619728088 CET	6184	49749	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:40.296585083 CET	49749	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:40.324564934 CET	6184	49749	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:44.412208080 CET	49755	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:44.438590050 CET	6184	49755	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:45.093842030 CET	49755	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:45.119945049 CET	6184	49755	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:45.797017097 CET	49755	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:45.823246956 CET	6184	49755	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:50.218314886 CET	49756	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:50.244765043 CET	6184	49756	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:50.859947920 CET	49756	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:50.886248112 CET	6184	49756	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:51.547516108 CET	49756	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:51.574143887 CET	6184	49756	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:55.622875929 CET	49757	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:55.649090052 CET	6184	49757	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:56.297931910 CET	49757	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:56.324323893 CET	6184	49757	185.140.53.139	192.168.2.7
Nov 20, 2020 09:27:56.891716957 CET	49757	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:27:56.918060064 CET	6184	49757	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:00.992399931 CET	49758	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:01.018563032 CET	6184	49758	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:01.532746077 CET	49758	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:01.558955908 CET	6184	49758	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:02.063973904 CET	49758	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:02.090981960 CET	6184	49758	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:06.137979984 CET	49759	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:06.163880110 CET	6184	49759	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:06.673902035 CET	49759	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:06.699908972 CET	6184	49759	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:07.205127954 CET	49759	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:07.231425047 CET	6184	49759	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:11.280884981 CET	49760	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:11.307646036 CET	6184	49760	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:11.816543102 CET	49760	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:11.842854023 CET	6184	49760	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:12.346164942 CET	49760	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:12.372693062 CET	6184	49760	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:16.456875086 CET	49763	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:16.485682011 CET	6184	49763	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:16.987375975 CET	49763	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:17.013942957 CET	6184	49763	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:17.521506071 CET	49763	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:17.548383951 CET	6184	49763	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:21.605441093 CET	49764	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:21.632688046 CET	6184	49764	185.140.53.139	192.168.2.7
Nov 20, 2020 09:28:22.143814087 CET	49764	6184	192.168.2.7	185.140.53.139
Nov 20, 2020 09:28:22.170222044 CET	6184	49764	185.140.53.139	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 09:26:35.912642002 CET	58052	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:35.939836979 CET	53	58052	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:36.980882883 CET	54008	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:37.007913113 CET	53	54008	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 09:26:38.436265945 CET	59451	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:38.463397026 CET	53	59451	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:39.522572994 CET	52914	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:39.549721956 CET	53	52914	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:40.618621111 CET	64569	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:40.645675898 CET	53	64569	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:41.769871950 CET	52816	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:41.798651934 CET	53	52816	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:42.877338886 CET	50781	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:42.912965059 CET	53	50781	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:44.836189985 CET	54230	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:44.863204002 CET	53	54230	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:45.893138885 CET	54911	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:45.920321941 CET	53	54911	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:46.935808897 CET	49958	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:46.962971926 CET	53	49958	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:48.047569990 CET	50860	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:48.074825048 CET	53	50860	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:49.102062941 CET	50452	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:49.129266977 CET	53	50452	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:50.216165066 CET	59730	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:50.243244886 CET	53	59730	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:51.362644911 CET	59310	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:51.389772892 CET	53	59310	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:56.079119921 CET	51919	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:56.116950035 CET	53	51919	8.8.8.8	192.168.2.7
Nov 20, 2020 09:26:58.627288103 CET	64296	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:26:58.678628922 CET	53	64296	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:02.549174070 CET	56680	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:02.586632013 CET	53	56680	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:04.589431047 CET	58820	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:04.616455078 CET	53	58820	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:07.688446045 CET	60983	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:07.723908901 CET	53	60983	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:12.862723112 CET	49247	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:12.900499105 CET	53	49247	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:18.017364979 CET	52286	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:18.044465065 CET	53	52286	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:23.346471071 CET	56064	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:23.381779909 CET	53	56064	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:25.628304958 CET	63744	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:25.655551910 CET	53	63744	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:26.802903891 CET	61457	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:26.840817928 CET	53	61457	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:28.510669947 CET	58367	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:28.546705008 CET	53	58367	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:33.006752968 CET	60599	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:33.043761969 CET	53	60599	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:33.692368031 CET	59571	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:33.728956938 CET	53	59571	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:33.806638002 CET	52689	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:33.841949940 CET	53	52689	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:34.320183039 CET	50290	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:34.347261906 CET	53	50290	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:34.723608017 CET	60427	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:34.759438038 CET	53	60427	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:35.256510973 CET	56209	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:35.292018890 CET	53	56209	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:35.805032015 CET	59582	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:35.842928886 CET	53	59582	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:36.356888056 CET	60949	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:36.384005070 CET	53	60949	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:36.436245918 CET	58542	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:36.487503052 CET	53	58542	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 09:27:37.080786943 CET	59179	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:37.116519928 CET	53	59179	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:37.968655109 CET	60927	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:38.005314112 CET	53	60927	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:38.481499910 CET	57854	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:38.508708954 CET	53	57854	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:39.020487070 CET	62026	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:39.055859089 CET	53	62026	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:42.851494074 CET	59453	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:42.888559103 CET	53	59453	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:44.373290062 CET	62468	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:44.409041882 CET	53	62468	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:50.148700953 CET	52563	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:50.184417963 CET	53	52563	8.8.8.8	192.168.2.7
Nov 20, 2020 09:27:55.584182978 CET	54721	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:27:55.621418953 CET	53	54721	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:00.953408957 CET	62826	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:00.989820004 CET	53	62826	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:06.099515915 CET	62046	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:06.136332989 CET	53	62046	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:11.240219116 CET	51223	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:11.277551889 CET	53	51223	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:12.293785095 CET	63908	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:12.322207928 CET	53	63908	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:13.937680006 CET	49226	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:13.964711905 CET	53	49226	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:16.412998915 CET	60212	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:16.448510885 CET	53	60212	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:21.568610907 CET	58867	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:21.604264975 CET	53	58867	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:26.713026047 CET	50864	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:26.748627901 CET	53	50864	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:34.338577032 CET	61504	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:34.374263048 CET	53	61504	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:39.479101896 CET	60231	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:39.514548063 CET	53	60231	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:44.617322922 CET	50095	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:44.652806997 CET	53	50095	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:49.757090092 CET	59654	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:49.792437077 CET	53	59654	8.8.8.8	192.168.2.7
Nov 20, 2020 09:28:55.054315090 CET	58233	53	192.168.2.7	8.8.8.8
Nov 20, 2020 09:28:55.090053082 CET	53	58233	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 09:26:56.079119921 CET	192.168.2.7	8.8.8.8	0xb1c3	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:02.549174070 CET	192.168.2.7	8.8.8.8	0xace9	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:07.688446045 CET	192.168.2.7	8.8.8.8	0xa96a	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:12.862723112 CET	192.168.2.7	8.8.8.8	0x8a48	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:18.017364979 CET	192.168.2.7	8.8.8.8	0xf2e6	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:23.346471071 CET	192.168.2.7	8.8.8.8	0x3e7b	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:28.510669947 CET	192.168.2.7	8.8.8.8	0xe9fa	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:33.692368031 CET	192.168.2.7	8.8.8.8	0x9a6f	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:39.020487070 CET	192.168.2.7	8.8.8.8	0x27e5	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:44.373290062 CET	192.168.2.7	8.8.8.8	0x176c	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 09:27:50.148700953 CET	192.168.2.7	8.8.8.8	0xce7	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:55.584182978 CET	192.168.2.7	8.8.8.8	0xa6ad	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:00.953408957 CET	192.168.2.7	8.8.8.8	0x7cd	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:06.099515915 CET	192.168.2.7	8.8.8.8	0xaa79	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:11.240219116 CET	192.168.2.7	8.8.8.8	0xb912	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:16.412998915 CET	192.168.2.7	8.8.8.8	0x8288	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:21.568610907 CET	192.168.2.7	8.8.8.8	0x6bf4	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:26.713026047 CET	192.168.2.7	8.8.8.8	0xb27	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:34.338577032 CET	192.168.2.7	8.8.8.8	0xdca9	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:39.479101896 CET	192.168.2.7	8.8.8.8	0x3bfb	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:44.617322922 CET	192.168.2.7	8.8.8.8	0xe95a	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:49.757090092 CET	192.168.2.7	8.8.8.8	0x85c5	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:55.054315090 CET	192.168.2.7	8.8.8.8	0x6ae4	Standard query (0)	kengeorge.zapto.org	A (IP address)	IN (0x0001)

DNS Answers

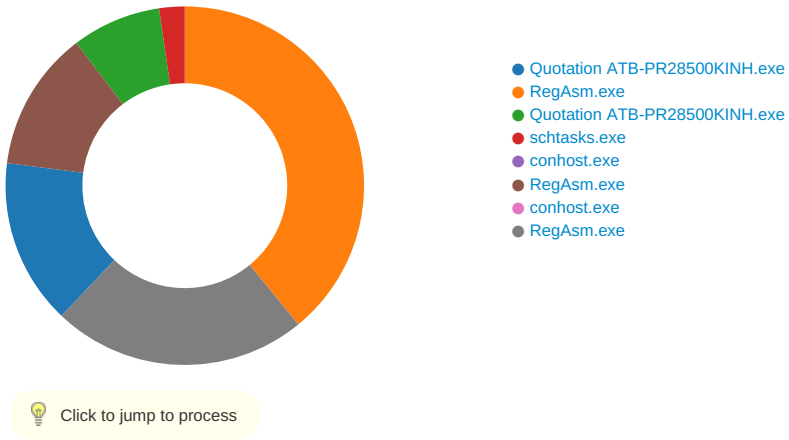
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 09:26:56.116950035 CET	8.8.8.8	192.168.2.7	0xb1c3	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:02.586632013 CET	8.8.8.8	192.168.2.7	0xace9	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:07.723908901 CET	8.8.8.8	192.168.2.7	0xa96a	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:12.900499105 CET	8.8.8.8	192.168.2.7	0x8a48	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:18.044465065 CET	8.8.8.8	192.168.2.7	0xf2e6	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:23.381779909 CET	8.8.8.8	192.168.2.7	0x3e7b	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:28.546705008 CET	8.8.8.8	192.168.2.7	0xe9fa	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:33.728956938 CET	8.8.8.8	192.168.2.7	0x9a6f	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:39.055859089 CET	8.8.8.8	192.168.2.7	0x27e5	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:44.409041882 CET	8.8.8.8	192.168.2.7	0x176c	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:50.184417963 CET	8.8.8.8	192.168.2.7	0xce7	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:27:55.621418953 CET	8.8.8.8	192.168.2.7	0xa6ad	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:00.989820004 CET	8.8.8.8	192.168.2.7	0x7cd	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:06.136332989 CET	8.8.8.8	192.168.2.7	0xaa79	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:11.277551889 CET	8.8.8.8	192.168.2.7	0xb912	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 09:28:16.448510885 CET	8.8.8.8	192.168.2.7	0x8288	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:21.604264975 CET	8.8.8.8	192.168.2.7	0x6bf4	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:26.748627901 CET	8.8.8.8	192.168.2.7	0xb27	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:34.374263048 CET	8.8.8.8	192.168.2.7	0xdca9	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:39.514548063 CET	8.8.8.8	192.168.2.7	0x3bfb	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:44.652806997 CET	8.8.8.8	192.168.2.7	0xe95a	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:49.792437077 CET	8.8.8.8	192.168.2.7	0x85c5	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Nov 20, 2020 09:28:55.090053082 CET	8.8.8.8	192.168.2.7	0x6ae4	No error (0)	kengeorge.zapto.org		185.140.53.139	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Quotation ATB-PR28500KINH.exe PID: 7036 Parent PID: 5720

General

Start time:	09:26:41
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:	0x4f0000
File size:	1020416 bytes
MD5 hash:	DDB5D5410477CD3855A1F542112808C0
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: 00000000.00000002.497351250.0000000000B1E000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.497351250.0000000000B1E000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.497351250.0000000000B1E000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.505763687.0000000005342000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.505763687.0000000005342000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.505763687.0000000005342000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.503615613.00000000038A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.503615613.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.503615613.00000000038A1000.00000004.00000001.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\7redfg	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	6C3ADD66	CopyFileW
C:\Users\user\AppData\Roaming\7redfg\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C3ADD66	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	508201B	NtCreateFile

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\7redfg:Zone.Identifier	success or wait	1	2719359	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\7redfg	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 d0 5d b7 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e4 09 00 00 ac 05 00 00 00 00 00 9e 03 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 a2 15 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....]._.......... ....@.. ....@................	success or wait	4	6C3ADD66	CopyFileW
C:\Users\user\AppData\Roaming\7redfg: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	6C3ADD66	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 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 d0 5d b7 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e4 09 00 00 ac 05 00 00 00 00 00 9e 03 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 a2 15 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....]._.......... ....@.. ....@................	pending	1	508204E	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	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D535705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D53CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4903DE	ReadFile
C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	0	1024000	pending	1	5081D6A	NtReadFile

Analysis Process: RegAsm.exe PID: 3392 Parent PID: 7036

General

Start time:	09:26:52
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:	0xd30000
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: 00000001.00000002.503999050.00000000040E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.503999050.00000000040E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.506528891.0000000005AA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.506528891.0000000005AA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.495967274.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.495967274.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.495967274.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.507063640.0000000006670000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.507063640.0000000006670000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.507063640.0000000006670000.00000004.00000001.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	6D55CF06	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	6D55CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6C3ABEFF	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	6C3A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpAC5D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C3A7038	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	6C3A1E60	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	6C3ABEFF	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	6C3ABEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAC5D.tmp	success or wait	1	6C3A6A95	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	4b 0f 92 79 79 8d d8 48	K..yy..H	success or wait	1	6C3A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpAC5D.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	6C3A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	6C3A1B4F	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	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D535705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D53CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D53CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D53CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C3A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C3A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	unknown	4096	success or wait	1	6D51D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	unknown	512	success or wait	1	6D51D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D535705	unknown

Analysis Process: Quotation ATB-PR28500KINH.exe PID: 6248 Parent PID: 7036

General

Start time:	09:26:53
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:	0xd00000
File size:	1020416 bytes
MD5 hash:	DDB5D5410477CD3855A1F542112808C0
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: 00000002.00000002.497878671.0000000001474000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.497878671.0000000001474000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.497878671.0000000001474000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.504002256.0000000004101000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.504002256.0000000004101000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.504002256.0000000004101000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.515094519.0000000005B42000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.515094519.0000000005B42000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.515094519.0000000005B42000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Written

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 00 00 50 45 00 00 4c 01 03 00 d0 5d b7 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e4 09 00 00 ac 05 00 00 00 00 00 9e 03 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 a2 15 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....]._.......... ....@.. ....@................	invalid handle	1	586204E	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	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D535705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D53CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4903DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	0	1024000	pending	1	5861D6A	NtReadFile

Analysis Process: schtasks.exe PID: 5816 Parent PID: 3392

General

Start time:	09:26:54
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\tmpAC5D.tmp'
Imagebase:	0x200000
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\tmpAC5D.tmp	unknown	2	success or wait	1	20AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpAC5D.tmp	unknown	1320	success or wait	1	20ABD9	ReadFile

Analysis Process: conhost.exe PID: 5824 Parent PID: 5816

General

Start time:	09:26:54
Start date:	20/11/2020
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: RegAsm.exe PID: 6200 Parent PID: 1104

General

Start time:	09:26:56
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:	0xa60000
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	6D86C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6C3A1B4F	WriteFile
\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	6C3A1B4F	WriteFile
\Device\ConDrv	unknown	0			success or wait	1	6C3A1B4F	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	6C3A1B4F	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	6D86C907	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	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D535705	unknown

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	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D535705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4903DE	ReadFile

Analysis Process: conhost.exe PID: 6396 Parent PID: 6200

General

Start time:	09:26:58
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6e70f0000
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: 7160 Parent PID: 6248

General

Start time:	09:27:07
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:	0xa40000
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: 0000000F.00000002.304004800.0000000002D41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.304004800.0000000002D41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.303385478.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.303385478.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.303385478.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.304067682.0000000003D49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.304067682.0000000003D49000.00000004.00000001.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	6D55CF06	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	6D55CF06	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	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D535705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D53CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D53CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D53CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D535705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C3A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C3A1B4F	ReadFile

Disassembly

Code Analysis