ID: 321079
Sample Name: Quotation ATB-PR28500KINH.exe
Cookbook: default.jbs
Time: 10:52:16
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

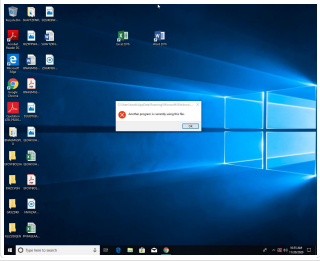
Analysis Report Quotation ATB-PR28500KINH.exe

Overview

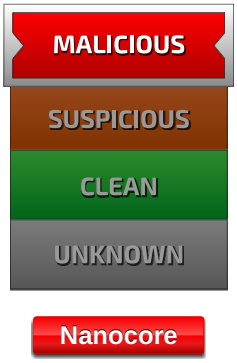
General Information

Sample Name:	Quotation ATB-PR28500KINH.exe
Analysis ID:	321079
MD5:	03c41991be46ed..
SHA1:	17193a4a9fad92f..
SHA256:	749b86298b1735..
Tags:	exe NanoCore

Most interesting Screenshot:



Detection

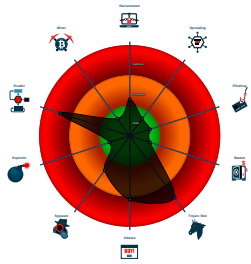


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 3980 cmdline: 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe' MD5: 03C41991BE46EDACB01B18D7FFE97B33)
  - Quotation ATB-PR28500KINH.exe (PID: 6148 cmdline: Quotation ATB-PR28500KINH.exe MD5: 03C41991BE46EDACB01B18D7FFE97B33)
    - schtasks.exe (PID: 6284 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpECB7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 1760 cmdline: 'schtasks.exe' /delete /f /tn 'DHCP Monitor' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5344 cmdline: 'schtasks.exe' /delete /f /tn 'DHCP Monitor Task' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6052 cmdline: 'cmd.exe' /C taskkill /f /im 'Quotation ATB-PR28500KINH.exe' & ping -n 1 -w 3000 1.1.1.1 & type nul > 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe' & del /f /q 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - taskkill.exe (PID: 4968 cmdline: taskkill /f /im 'Quotation ATB-PR28500KINH.exe' MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
      - PING.EXE (PID: 5604 cmdline: ping -n 1 -w 3000 1.1.1.1 MD5: 70C24A306F768936563ABDADB9CA9108)
- Quotation ATB-PR28500KINH.exe (PID: 6424 cmdline: 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe' 0 MD5: 03C41991BE46EDACB01B18D7FFE97B33)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.320687638.000000000409E000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000006.00000002.328310332.00000000073C0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5fee:$x1: NanoCore.ClientPluginHost • 0x602b:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
00000006.00000002.328310332.00000000073C0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5fee:$x2: NanoCore.ClientPluginHost • 0x9441:$s4: PipeCreated • 0x6018:$s5: IClientLoggingHost
00000006.00000002.316582541.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000006.00000002.316582541.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.Quotation ATB-PR28500KINH.exe.7380000.11.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
6.2.Quotation ATB-PR28500KINH.exe.7380000.11.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
6.2.Quotation ATB-PR28500KINH.exe.73c0000.13.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x41ee:$x1: NanoCore.ClientPluginHost • 0x422b:$x2: IClientNetworkHost
6.2.Quotation ATB-PR28500KINH.exe.73c0000.13.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x41ee:$x2: NanoCore.ClientPluginHost • 0x7641:$s4: PipeCreated • 0x4218:$s5: IClientLoggingHost
2.2.Quotation ATB-PR28500KINH.exe.54e0000.1.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 35 entries				

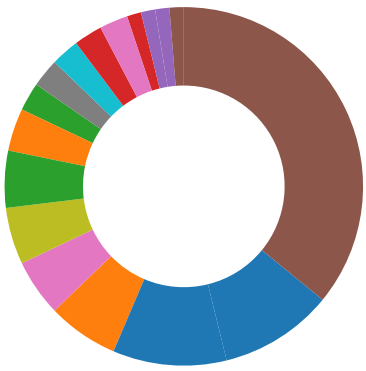
Sigma Overview

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

Click to jump to signature section

AV Detection:

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

Networking:

Uses ping.exe to check the status of other devices and networks

E-Banking Fraud:

Yara detected Nanocore RAT

Operating System Destruction:

Protects its processes via BreakOnTermination flag

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)

Malware Analysis System Evasion:

Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

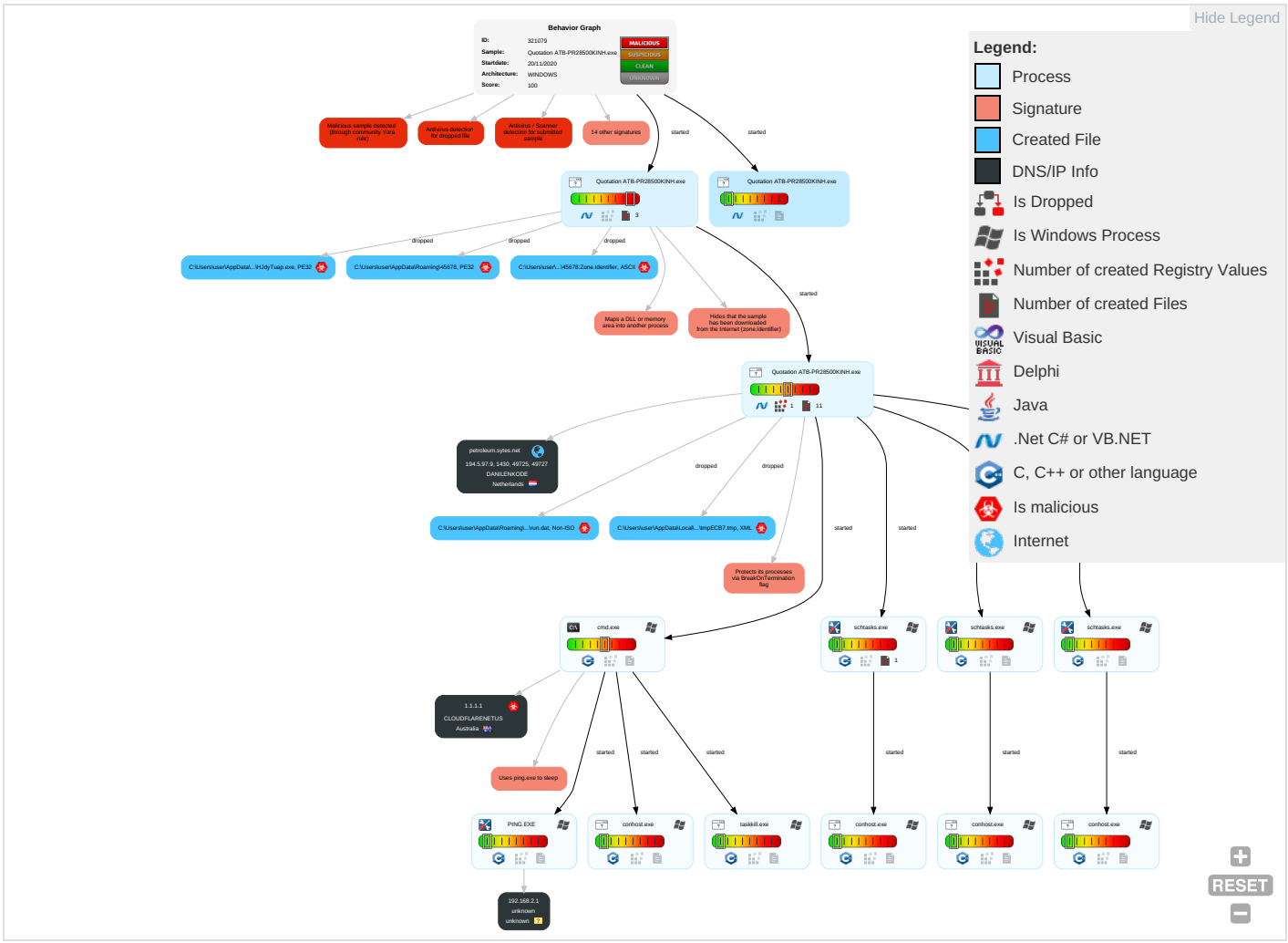
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

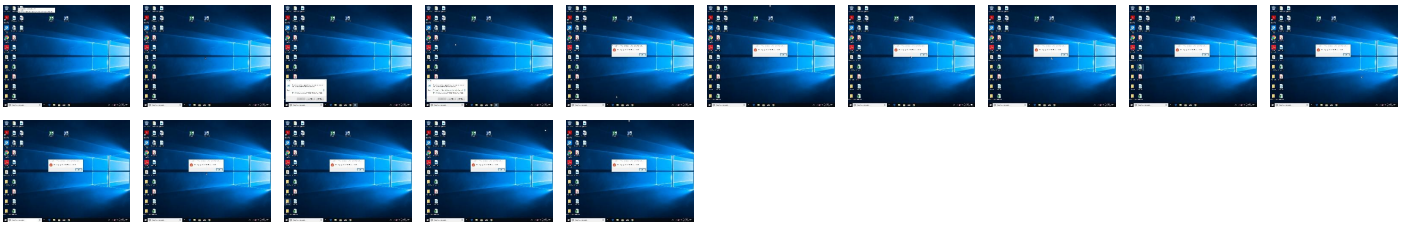
Behavior Graph



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.Hacktool.Mimikatz	
Quotation ATB-PR28500KINH.exe	100%	Avira	TR/AD.Nanocore.qhfnr	
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.qhfnr	
C:\Users\user\AppData\Roaming\45678	100%	Avira	TR/AD.Nanocore.qhfnr	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\45678	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\45678	27%	ReversingLabs	ByteCode-MSIL.Hacktool.Mimikatz	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.Quotation ATB-PR28500KINH.exe.57f0000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
2.2.Quotation ATB-PR28500KINH.exe.54e0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
6.2.Quotation ATB-PR28500KINH.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
petroleum.sytes.net	1%	Virustotal		Browse

URLs

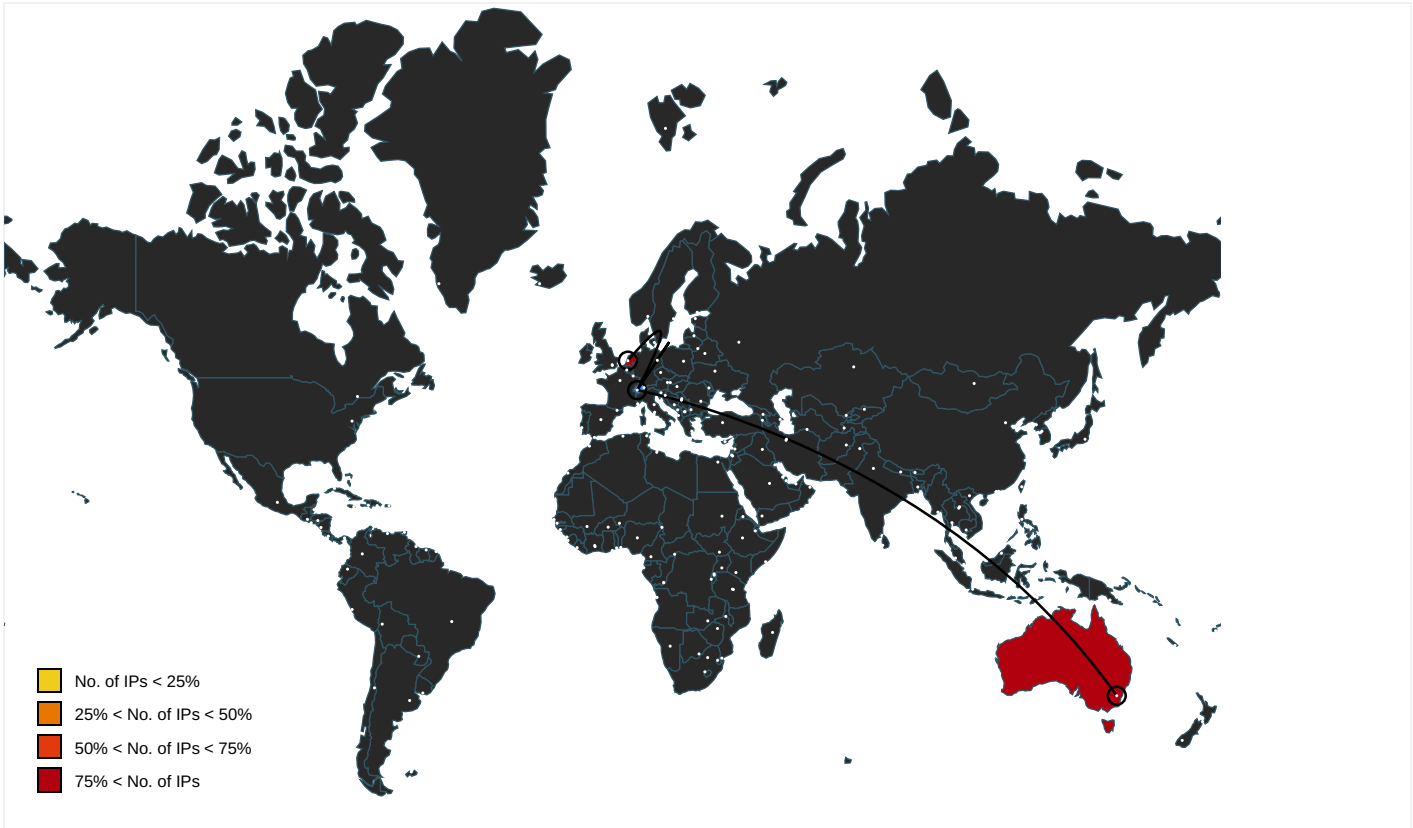
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
petroleum.sytes.net	194.5.97.9	true	false	• 1%, Virustotal, Browse	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	true
194.5.97.9	unknown	Netherlands		208476	DANILENKODE	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321079
Start date:	20.11.2020
Start time:	10:52:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 42s
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:	40
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@43520/9@2/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 60.3% • Quality standard deviation: 29.8%
HCA Information:	• Successful, ratio: 96% • 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): 52.255.188.83, 92.122.145.220, 104.43.193.48, 23.210.248.85, 84.53.167.113, 51.104.139.180, 8.241.11.126, 8.248.125.254, 8.248.117.254, 67.26.137.254, 8.248.119.254, 52.155.217.156, 20.54.26.129, 95.101.22.134, 95.101.22.125 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e15275.g.akamaiedge.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wildcard.weather.microsoft.com.edgekey.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, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:53:21	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HJdyTuap.exe
10:53:33	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
1.1.1.1	QQ9.0.1.exe	Get hash	malicious	Browse	• url-quality-stat.xf.qq.com/Analyze/Data?v=1&&format=json&&qq=0&&cmd=21&&product=qqdownload
194.5.97.9	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
petroleum.sytes.net	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 185.140.53.139
	RFQ-BOHB-SS-FD6L4.exe	Get hash	malicious	Browse	• 185.140.53.139
	new order is in the attached.exe	Get hash	malicious	Browse	• 185.244.30.10
	Claim 001 & 002_pdf.exe	Get hash	malicious	Browse	• 185.244.30.10
	Claim 001 & 002_JPEG.exe	Get hash	malicious	Browse	• 185.244.30.10
	Product lists.exe	Get hash	malicious	Browse	• 185.244.30.10
	End of the yr shipment#102120.exe	Get hash	malicious	Browse	• 185.244.30.10
	ALLPLATES-P.O#008012019.pdf.exe	Get hash	malicious	Browse	• 185.244.30.10
	ALLPLATES-P.O#008012019.exe	Get hash	malicious	Browse	• 185.244.30.10
	Request price listing.exe	Get hash	malicious	Browse	• 185.244.30.10
	894H-2CH-F-C G03 6VDC.exe	Get hash	malicious	Browse	• 185.244.30.10
	894H-2CH-F-C G03 6VDC.exe	Get hash	malicious	Browse	• 185.244.30.10

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	23prRlqeGr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.23.46
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.22.46
	iG9YiwEMru.exe	Get hash	malicious	Browse	• 104.27.132.115
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 104.22.54.159
	SUSPENSION LETTER ON SIM SWAP.pdf.exe	Get hash	malicious	Browse	• 172.67.131.55
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	SaXJC2CZ8m.exe	Get hash	malicious	Browse	• 104.27.133.115
	PO91666. pdf.exe	Get hash	malicious	Browse	• 172.67.143.180
	BT2wDapfoI.exe	Get hash	malicious	Browse	• 104.23.98.190
	ara.exe	Get hash	malicious	Browse	• 172.65.200.133
	ORDER FORM DENK.exe	Get hash	malicious	Browse	• 104.18.47.150
	araiki.exe	Get hash	malicious	Browse	• 172.65.200.133
	arailk.exe	Get hash	malicious	Browse	• 172.65.200.133
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 104.26.4.196
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 104.16.18.94
	http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000	Get hash	malicious	Browse	• 104.16.149.64
	http://https://www.canva.com/design/DAEN9RID8Vk/acBvt6UoL-DafjXmQk38pA/view?utm_content=DAEN9RID8Vk&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 104.18.215.67
	http://https://gazeta-echo.ru/wp-includes/assets/<>/?mail=tfagot@dupaco.com	Get hash	malicious	Browse	• 104.16.123.175
	http://https://go.pardot.com/e/395202/siness-insights-dashboard-html/bnmpz6/1446733421?h=AwLDfNsCVbkjEN13pzY-7AXMPolL_XMigGsJSppGaiM	Get hash	malicious	Browse	• 104.16.19.94
DANILENKODE	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 194.5.97.9
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\tmpECB7.tmp	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1315
Entropy (8bit):	5.1337076542548274
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0LFxtn:cbk4oL600QydbQxIYODOLedq3uFj
MD5:	5C24CCED27B3FB5CB89EE64C7E4FD458
SHA1:	EBC586E78D6BDC8F916D4FAB269033293F7980BD
SHA-256:	D7B6F315482BBFD57BD9AA6C302F2F55798D8BC3655853ABD6412B1D4289AFCC
SHA-512:	48E75213BEDEF4014E44F4C2B38643A7D4DF888CE261DD07908121F4A73B88F2A931AF5F0D27DB3FED120FDA2B7A75E074697CF2C94EEBD54CB403CA9C7F5D0
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <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\45678	
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):	1021440
Entropy (8bit):	6.747456626425728
Encrypted:	false
SSDEEP:	12288:cf9LurGfMzvqv7G9pq+0+Rcd70FOKWb4nlph7Qq4xohcYgpqC:g9LurGfPDmpq+0ZqVWcnlUFDYg
MD5:	03C41991BE46EDACB01B18D7FFE97B33
SHA1:	17193A4A9FAD92F1473D42BBE0D14E83DA481A72
SHA-256:	749B86298B1735B41E92EEF8B48C0AA38F1D7FA55BD0958B7B752BFCB5CB5A87
SHA-512:	0A75BF191A00F1C641F6811D98C987F0248BE5CACEDD8C3C7E93E0CA5AE8913B4813BA792021B035A843DF78BE186D054221A311E185F3A37CC92F28EE2730D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Reputation:	low

C:\Users\user\AppData\Roaming\45678	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._..... ... .@.. ..... .@.....W.... ..N..... ....H.....text...4.... ....`.rsrc...N.... .....@..@.reloc..... .....@..B.....H.....e.....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....*.(....*.(....*.r1..p.....*6..{b... (^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

C:\Users\user\AppData\Roaming\45678: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\catalog.dat	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
File Type:	data
Category:	dropped
Size (bytes):	128
Entropy (8bit):	6.527114648336088
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRH5/ljRAaTlKYrI1Sj9txROIsxcMek2:X4LDAn1rplKTYBROIsxek2
MD5:	0A9C5EAE8756D6FC90F59D8D71A79E1E
SHA1:	0F7D6AAED17CD18DC614535ED26335C147E29ED7
SHA-256:	B1921EA14C66927397BAF3FA456C22B93C30C3DE23546087C0B18551CE5001C5
SHA-512:	78C2F399AC49C78D89915DFF99AC955B5E0AB07BAAD61B07B0CE073C88C1D3A9F1D302C2413691B349DD34441B0FF909C08A4F71E2F1B73F46C1FF308BC7CFA
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P.OT....g.t.....'7.....)..8zIl..K/....n3...3.5.....&.7].)..wL...:}g...@...mV.....JUP...w

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.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:JIP:aP
MD5:	179401BA509B78E5613624E70B9E2ECA
SHA1:	FB3A31D8A8900CADB2820CAF4FC8B3AE2AA6581F
SHA-256:	9AA369E0924A94912AB3C3CFD1ACC04CFC7470DBBA6829A03BD576FB15537FEC
SHA-512:	9D9379F07B9E607509FC84F858973BB81A03D97CDB620DC9C0F79AB4473DF5E2C37E6F5AA2C57A4E195F11A6082C683A3CC5C7BDB0768E698E1D7740BCA75D4
Malicious:	**true**
Preview:	._k....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
File Type:	data
Category:	dropped
Size (bytes):	285608
Entropy (8bit):	**7.99942192025113**
Encrypted:	**true**
SSDEEP:	6144:KpKR3kz0ohkLsRC9wjZ59AbuaY5O+gRGD9Hcj4Tdw:IaUYweYC9wjZ59AyA5YFc0Te
MD5:	30E23835B6123B3250D73C3E313FEB01
SHA1:	52CDA23480DA64C5B16D9F6554D6B66E9FA1AE22
SHA-256:	20CC3B053C43B689D3C669DDDA6DF6E3C939B2059F9FA5B578AE2BB887269EB3
SHA-512:	DBF82EE996D82D0DAF95A3A9733056EF1FFE80D05D6ED88514FD728E9AA29161EEA8E75B12BB77E0D0B4F81C77A26CDAE4ABC29C8FA661D40C1941CA51E17 9B
Malicious:	false
Preview:	.....W*.....P&4.....E..v+...mc...C<_..0....40=.....[..3.q....\..[.l.....g....=.cl5w...h{2...c..l.j...4.R..$*X..<....q%...Y.:19..Y....f.uy..Q....=t...Q....\KuA.Z...ze...?.....o....BX...Eh....(F W..\|Mn.B>...R.>_Yz.....U..>n....h..g5.._..vY.dN..]Bi=....&.._.8...9.Et...y..h1...uMy..G...._1by.)...H.....ws...C.S..?6.i.N.....8:..t..?.Z..?^..{.....".fsb....m.<..3..<.{ ..;+..v..H.6.....C..r_..Hv.?....z...F.=...%2...'C...LqF]....6/,.....)WuH..~..1.W.....#..D.P_.Z8..n.~c. .....F$,bI...m../..dO..O...o..).3.M,...0.q..N..n...%BtO.i...L.N.^i[.<...#_.....+z.! (...y.XN....^.K. E....2n.!.wa./yy(../...b:..Oq..j2Q- .....n(..\....Q;..ue...G..#!.2.\@lH....o..\?.K.Q..=qW}..|.....6.....{.Y..e:.7..P`.H.....o.....}..t."C#.i.<z.4Y.e..j..G.RO.$.[.l8...A....U; (...s..C..|...y....w.7?....}.....D.h.....Ip.t.8....9%./...K...#G.2.s.....E.....tX.}..O...X.....S.9>k.hY..-."\..X.y@w.U...|._3.]R..:.^4l.....L.....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	52
Entropy (8bit):	5.003042362247046
Encrypted:	false
SSDEEP:	3:oNWXp5v0fyMQkq3CAdA:oNWXpF0fyn3CN
MD5:	69CBDC701874E0618836B88761CDB7C2
SHA1:	00B9CDA4949AA22EBAAB35427447140F0DAEE0A4
SHA-256:	E4135CACE67B6B8D98545C5BAF81F6762EAA0BF6577BCCC7674E19B4E6DE9EA3
SHA-512:	D61307D607B94A5D70D9AC8FB8DCBF44A0DD9FADACFA59CD3BD160EEBABE578F23CE717D9EB5CA5AEDCB7692BCF5FF11406606504D438F99EFDA9BB81AE D7E1
Malicious:	false
Preview:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.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):	6.742400621297182
Encrypted:	false
SSDEEP:	12288:cf9LurGfMzvqv7G9pq+0+Rcd70FOKWb4nlph7Qq4xohcYgpqC:g9LurGfPDmpq+0ZqVWcnlUFDYg
MD5:	08AD546B0A6F6C8AAC626B2E0F24C879
SHA1:	62B8943CC7F8DDFDF36518398E9393E4C5F336D5
SHA-256:	47B9259DCC96B694585C2E2E216C309E1B83AA46025599A996605B2D2314C3DB
SHA-512:	ECD93E63F4706D5BBFA36C9003B18DFD19CA02FED78E3F59C4ED9B7185AA43274D9327C980E9BAFD879E58CFD77BB120B7922A35C985642E72833AD86FFD64 1
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._..... ... .@.. ..... .@.....W.... ..N..... ..... .H.....text...4.... ....`.rsrc...N.... .....@..@.reloc..... .....@..B.....H.....e.....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....*.(....*.(....*.r1..p.....*6..{b... (^..*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.747456626425728
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:	1021440
MD5:	03c41991be46edacb01b18d7ffe97b33
SHA1:	17193a4a9fad92f1473d42bbe0d14e83da481a72
SHA256:	749b86298b1735b41e92eef8b48c0aa38f1d7fa55bd0958b7b752bfcb5cb5a87
SHA512:	0a75bf191a00f1c641f6811d98c987f0248be5cacedd8c3c7e93e0ca5ae8913b4813ba792021b035a843df78be186d054221a311e185f3a37cc92f28ee2730d0
SSDEEP:	12288:cf9LurGfMzvqv7G9pq+0+Rcd70FOKWb4nlph7Qq4xohcYgpqC:g9LurGfPDmpq+0ZqVWcnlUFDYg
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:	0x4a062e
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:	0x5FB6EFA2 [Thu Nov 19 22:20:18 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa05d4	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	0x9e634	0x9e800	False	0.921431388013	data	7.8618274721	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

Name	RVA	Size	Type	Language	Country
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

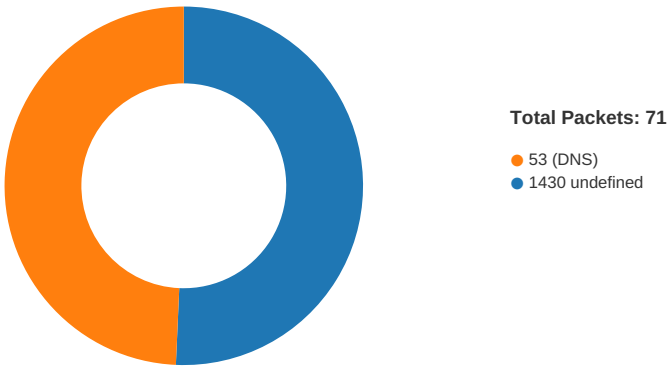
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-10:53:57.838381	ICMP	382	ICMP PING Windows			192.168.2.3	1.1.1.1
11/20/20-10:53:57.838381	ICMP	384	ICMP PING			192.168.2.3	1.1.1.1
11/20/20-10:53:57.854679	ICMP	408	ICMP Echo Reply			1.1.1.1	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:53:34.705584049 CET	49725	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:34.890532017 CET	1430	49725	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:35.408818960 CET	49725	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:35.601016045 CET	1430	49725	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:36.205795050 CET	49725	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:36.409563065 CET	1430	49725	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:40.529350996 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:40.710572004 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:40.710700989 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:40.935179949 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:41.320521116 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:41.320611954 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:41.528413057 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:41.530108929 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:41.738502026 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:41.765830994 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.106080055 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.106118917 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.106195927 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.307099104 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.307138920 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.307157993 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.307176113 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.307431936 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.519011021 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.519826889 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.519933939 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.520948887 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.521869898 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.522413969 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.522795916 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.523842096 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.523941040 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.533906937 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.533946991 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.534017086 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.720133066 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.720911026 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.721029997 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.721724987 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.722816944 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.722923040 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.724050999 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.724838972 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.724980116 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.725795031 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.726804972 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.726888895 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.729020119 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.729854107 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.729964972 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.730771065 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.731781960 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.731870890 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.732804060 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.733844995 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.734746933 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.734822989 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.735846043 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.735939980 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.930031061 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.930794954 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.930886030 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.931830883 CET	1430	49727	194.5.97.9	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:53:42.932857037 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.932943106 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.934791088 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.935798883 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.935868025 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.936789036 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.937764883 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.938740969 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.938790083 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.939851046 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.940080881 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.940145016 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.940820932 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.940959930 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.942058086 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.942826033 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.942919016 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.944037914 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.944782019 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.945833921 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.945914984 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.946908951 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.947004080 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.947834969 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.948826075 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.948899031 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.949785948 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.950874090 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.951874018 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.951981068 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.952819109 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.953331947 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.953821898 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.954814911 CET	1430	49727	194.5.97.9	192.168.2.3
Nov 20, 2020 10:53:42.954898119 CET	49727	1430	192.168.2.3	194.5.97.9
Nov 20, 2020 10:53:42.955823898 CET	1430	49727	194.5.97.9	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:53:04.989098072 CET	55984	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:05.016263008 CET	53	55984	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:05.106074095 CET	64185	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:05.143208027 CET	53	64185	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:05.705660105 CET	65110	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:05.732884884 CET	53	65110	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:06.417464972 CET	58361	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:06.444624901 CET	53	58361	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:11.160722017 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:11.187865973 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:12.272840977 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:12.299959898 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:13.435460091 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:13.471121073 CET	53	60100	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:14.250729084 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:14.277920008 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:15.146070957 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:15.174118996 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:15.943406105 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:15.970540047 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:16.709011078 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:16.755137920 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:17.979852915 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:18.007013083 CET	53	51352	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:53:20.954000950 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:20.991797924 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:21.620935917 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:21.647938013 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:22.740910053 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:22.767949104 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:33.483869076 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:33.521542072 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:34.654174089 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:34.693852901 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:37.311450958 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:37.347163916 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:40.491895914 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:40.527616024 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:40.893130064 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:40.920228004 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 10:53:54.179631948 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:53:54.206603050 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:15.100765944 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:15.127896070 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:15.707856894 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:15.735053062 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:16.168093920 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:16.195135117 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:16.528357983 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:16.563704967 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:16.892540932 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:16.928282976 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:17.144768953 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:17.196007013 CET	53	61292	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:17.540549040 CET	63619	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:17.567495108 CET	53	63619	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:18.273814917 CET	64938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:18.300945044 CET	53	64938	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:18.972325087 CET	61946	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:19.008033037 CET	53	61946	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:19.800508022 CET	64910	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:19.827721119 CET	53	64910	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:20.266268015 CET	52123	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:20.301872969 CET	53	52123	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:23.846113920 CET	56130	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:23.883203030 CET	53	56130	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:52.467478991 CET	56338	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:52.494472027 CET	53	56338	8.8.8.8	192.168.2.3
Nov 20, 2020 10:54:54.532007933 CET	59420	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:54:54.559500933 CET	53	59420	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 20, 2020 10:53:57.838381052 CET	192.168.2.3	1.1.1.1	4d5a		Echo
Nov 20, 2020 10:53:57.854679108 CET	1.1.1.1	192.168.2.3	555a		Echo Reply

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 10:53:34.654174089 CET	192.168.2.3	8.8.8.8	0x3a71	Standard query (0)	petroleum.sytes.net	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:40.491895914 CET	192.168.2.3	8.8.8.8	0x9891	Standard query (0)	petroleum.sytes.net	A (IP address)	IN (0x0001)

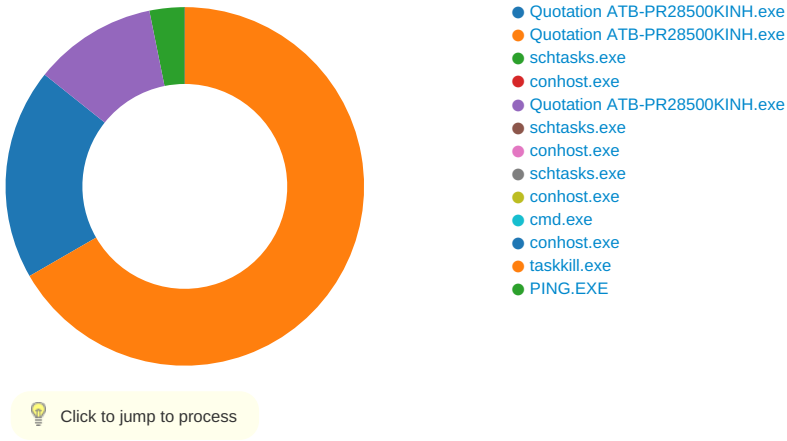
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 10:53:34.693852901 CET	8.8.8.8	192.168.2.3	0x3a71	No error (0)	petroleum.sytes.net		194.5.97.9	A (IP address)	IN (0x0001)
Nov 20, 2020 10:53:40.527616024 CET	8.8.8.8	192.168.2.3	0x9891	No error (0)	petroleum.sytes.net		194.5.97.9	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Quotation ATB-PR28500KINH.exe PID: 3980 Parent PID: 5548

General

Start time:	10:53:11
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:	0x6b0000
File size:	1021440 bytes
MD5 hash:	03C41991BE46EDACB01B18D7FFE97B33
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: 00000002.00000002.321624483.0000000003B61000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.321624483.0000000003B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.321624483.0000000003B61000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.317796226.0000000000E64000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.317796226.0000000000E64000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.317796226.0000000000E64000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.330776176.00000000054E2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.330776176.00000000054E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.330776176.00000000054E2000.00000040.00000001.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\45678	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	6CECDD66	CopyFileW
C:\Users\user\AppData\Roaming\45678\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CECDD66	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	503201B	NtCreateFile

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\45678:Zone.Identifier	success or wait	1	6DEEEAF6	unknown

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\45678	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 a2 ef b6 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e8 09 00 00 ac 05 00 00 00 00 00 2e 06 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 0c 8e 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	6CECDD66	CopyFileW
C:\Users\user\AppData\Roaming\45678: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	6CECDD66	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 a2 ef b6 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e8 09 00 00 ac 05 00 00 00 00 00 2e 06 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 0c 8e 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	503204E	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	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	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	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile

Analysis Process: Quotation ATB-PR28500KINH.exe PID: 6148 Parent PID: 3980

General

Start time:	10:53:29
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe
Wow64 process (32bit):	true
Commandline:	Quotation ATB-PR28500KINH.exe
Imagebase:	0xbd0000
File size:	1021440 bytes
MD5 hash:	03C41991BE46EDACB01B18D7FFE97B33
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: 00000006.00000002.320687638.000000000409E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.328310332.00000000073C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.328310332.00000000073C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.316582541.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.316582541.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.316582541.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.328240077.0000000007380000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.328240077.0000000007380000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.328269653.0000000007390000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.328269653.0000000007390000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.321093889.000000000418C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.321093889.000000000418C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.327974006.00000000071E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.327974006.00000000071E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.325787678.00000000057E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.325787678.00000000057E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.318700397.0000000003041000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.325804891.00000000057F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.325804891.00000000057F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.325804891.00000000057F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.328184231.0000000007370000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.328184231.0000000007370000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.326037509.00000000058C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.326037509.00000000058C0000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E07CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E07CF06	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	6CECBEFF	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	6CEC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpECB7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEC7038	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	6CEC1E60	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	6CECBEFF	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	6CECBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpECB7.tmp	success or wait	1	6CEC6A95	DeleteFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	success or wait	1	6CEC6A95	DeleteFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	success or wait	1	6CEC6A95	DeleteFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	success or wait	1	6CEC6A95	DeleteFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	success or wait	1	6CEC6A95	DeleteFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	success or wait	1	6CEC6A95	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	96 5f 6b 93 85 8d d8 48	._k....H	success or wait	1	6CEC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpECB7.tmp	unknown	1315	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	6CEC1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	52	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 51 75 6f 74 61 74 69 6f 6e 20 41 54 42 2d 50 52 32 38 35 30 30 4b 49 4e 48 2e 65 78 65	C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	success or wait	1	6CEC1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	128	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 f7 4f 54 9a 9e cd ce 67 b2 74 1d 8d f3 84 d5 c8 14 27 37 9d 1c 91 f7 de c0 29 c6 85 f2 9b 38 7a 49 49 d1 ba 8a 4b 2f 1e f9 0e c8 6e 33 10 b7 d5 33 90 35 c3 c9 07 e0 81 87 ea 26 b8 37 5d 98 29 bb eb 77 4c 93 d5 c0 3a 7d 67 09 96 2e 40 ce f9 f7 6d 56 d9 b2 fc bd 83 ad 4a 55 50 9c fa 96 77	Gj.h\.3...A...5.x..&...i+...c(1 .P.OT....g.t.....'7.....).. ..8zII...K/....n3...3.5..... &.7].)..wL...:}g...@...mV..... .JUP...w	success or wait	1	6CEC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	285608	11 b5 1a e5 bb 11 57 2a f2 95 a2 a3 8b b2 d1 89 50 26 34 95 a4 00 e3 e0 1b 7f 45 db b9 f3 76 2b 0a 00 e8 8f 6d 63 98 cb 84 00 43 3c 5f aa a6 30 bf a9 f2 d2 34 30 3d bf db ed 8c 09 84 b7 5b 12 8e 33 f8 71 e5 fd de c1 5c a4 e4 5b 9e 49 ba e9 0b 15 dc 15 08 67 dc 8d 9b f9 d7 3d c8 63 49 35 77 bb af 8f 68 7b 32 fa 12 fb 63 9f f7 6c da a1 6a 06 0a f1 34 fa 52 8e e3 24 2a 58 ac 04 3c 97 cf ec 9a 00 71 25 df 9c 9b 84 59 dd 3a 31 39 cb ae 9d 59 96 06 8c f7 66 f1 75 79 a6 eb 51 ac 8b b6 0e 3d 74 17 18 d9 51 ad 96 a6 a4 5c 4b 75 41 0a 5a ef a8 f7 95 7a 65 96 d6 8f 7f 3f e5 c7 0a 09 9f 8d d7 d4 6f de b0 f1 ef ca 42 58 ff a7 ee 45 68 84 81 89 82 28 46 57 91 d6 7c 4d 6e e6 42 3e 16 0d b5 52 de 3e 5f 59 7a 80 99 80 07 09 f2 55 d4 d9 3e 6e bd d3 91 ee f8 68 b6 d3 b8 67	......W*.....P&4.....E... v+....mc....C<_..0....40=..... ..[..3.q....\..[.l.....g.... .=.cI5w...h{2...c..l..j...4.R. .$*X..<.....q%....Y.:19...Y... .f.uy..Q....=t...Q....\KuA.Z.. ..ze....?.....o.....BX...Eh.... (FW..|Mn.B>...R.>_Yz..... U..>n.....h...g	success or wait	1	6CEC1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6CEC1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	unknown	4096	success or wait	1	6E03D72F	unknown
C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	unknown	512	success or wait	1	6E03D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E03D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E03D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	success or wait	1	740E367	MoveFileExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\?? \C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	\?? \C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe\??\C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\DHCP Monitor\dhcpmon.exe	success or wait	1	740E367	MoveFileExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\?? \C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe\??\C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\DHCP Monitor\dhcpmon.exe	\?? \C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe\??\C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\DHCP Monitor\dhcpmon.exe\?? \C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	740E367	MoveFileExA

Analysis Process: schtasks.exe PID: 6284 Parent PID: 6148

General

Start time:	10:53:31
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\tmpECB7.tmp'
Imagebase:	0x12a0000
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\tmpECB7.tmp	unknown	2	success or wait	1	12AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpECB7.tmp	unknown	1316	success or wait	1	12AABD9	ReadFile

Analysis Process: conhost.exe PID: 6300 Parent PID: 6284

General

Start time:	10:53:32
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: Quotation ATB-PR28500KINH.exe PID: 6424 Parent PID: 528

General

Start time:	10:53:34
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' 0
Imagebase:	0x5b0000
File size:	1021440 bytes
MD5 hash:	03C41991BE46EDACB01B18D7FFE97B33
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: 0000000A.00000002.320831164.0000000003961000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.320831164.0000000003961000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.320831164.0000000003961000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.317682512.0000000000DA5000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.317682512.0000000000DA5000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.317682512.0000000000DA5000.00000004.00000020.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 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 a2 ef b6 5f 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e8 09 00 00 ac 05 00 00 00 00 00 2e 06 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 0c 8e 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	522204E	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	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe	0	1024000	pending	1	5221D6A	NtReadFile

Analysis Process: schtasks.exe PID: 1760 Parent PID: 6148

General

Start time:	10:53:53
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /delete /f /tn 'DHCP Monitor'
Imagebase:	0x12a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 1140 Parent PID: 1760

General

Start time:	10:53:53
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7488e0000
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: schtasks.exe PID: 5344 Parent PID: 6148

General

Start time:	10:53:54
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /delete /f /tn 'DHCP Monitor Task'
Imagebase:	0x12a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 1256 Parent PID: 5344

General

Start time:	10:53:54
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7488e0000
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: cmd.exe PID: 6052 Parent PID: 6148

General

Start time:	10:53:55
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	'cmd.exe' /C taskkill /f /im 'Quotation ATB-PR28500KINH.exe' & ping -n 1 -w 3000 1.1.1.1 & type nul > 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe' & del /f /q 'C:\Users\user\Desktop\Quotation ATB-PR28500KINH.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5908 Parent PID: 6052

General

Start time:	10:53:55
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: taskkill.exe PID: 4968 Parent PID: 6052

General

Start time:	10:53:56
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /f /im 'Quotation ATB-PR28500KINH.exe'
Imagebase:	0x980000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: PING.EXE PID: 5604 Parent PID: 6052

General

Start time:	10:53:56
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping -n 1 -w 3000 1.1.1.1
Imagebase:	0xf00000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis