ID: 553236
Sample Name: price quote.exe
Cookbook: default.jbs
Time: 14:30:28
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

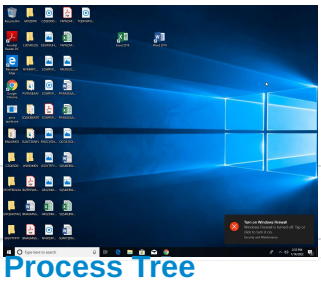
Windows Analysis Report price quote.exe

Overview

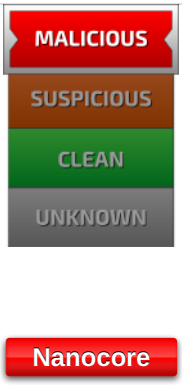
General Information

Sample Name:	price quote.exe
Analysis ID:	553236
MD5:	5c7d156ca2eb99..
SHA1:	f149bece20ca820..
SHA256:	e2228ae0e77d09..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

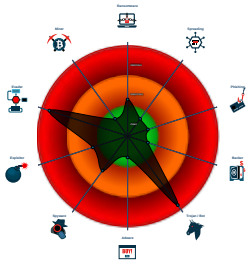


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- price quote.exe (PID: 4348 cmdline: "C:\Users\user\Desktop\price quote.exe" MD5: 5C7D156CA2EB9956E2DAE2DE52697AD5)
  - price quote.exe (PID: 5572 cmdline: C:\Users\user\Desktop\price quote.exe MD5: 5C7D156CA2EB9956E2DAE2DE52697AD5)
- dhcpmon.exe (PID: 6856 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 5C7D156CA2EB9956E2DAE2DE52697AD5)
  - dhcpmon.exe (PID: 5756 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 5C7D156CA2EB9956E2DAE2DE52697AD5)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c48b433d-6e7a-4320-ac18-2f1271be",
  "Group": "Default",
  "Domain1": "derarawfile10.ddns.net",
  "Domain2": "212.192.246250",
  "Port": 1187,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.305911719.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000000.305911719.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000000.305911719.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000009.00000000.347828924.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000009.00000000.347828924.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 50 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.dhcpmon.exe.400000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
9.0.dhcpmon.exe.400000.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
9.0.dhcpmon.exe.400000.8.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
9.0.dhcpmon.exe.400000.8.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
7.2.dhcpmon.exe.3e20908.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 88 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

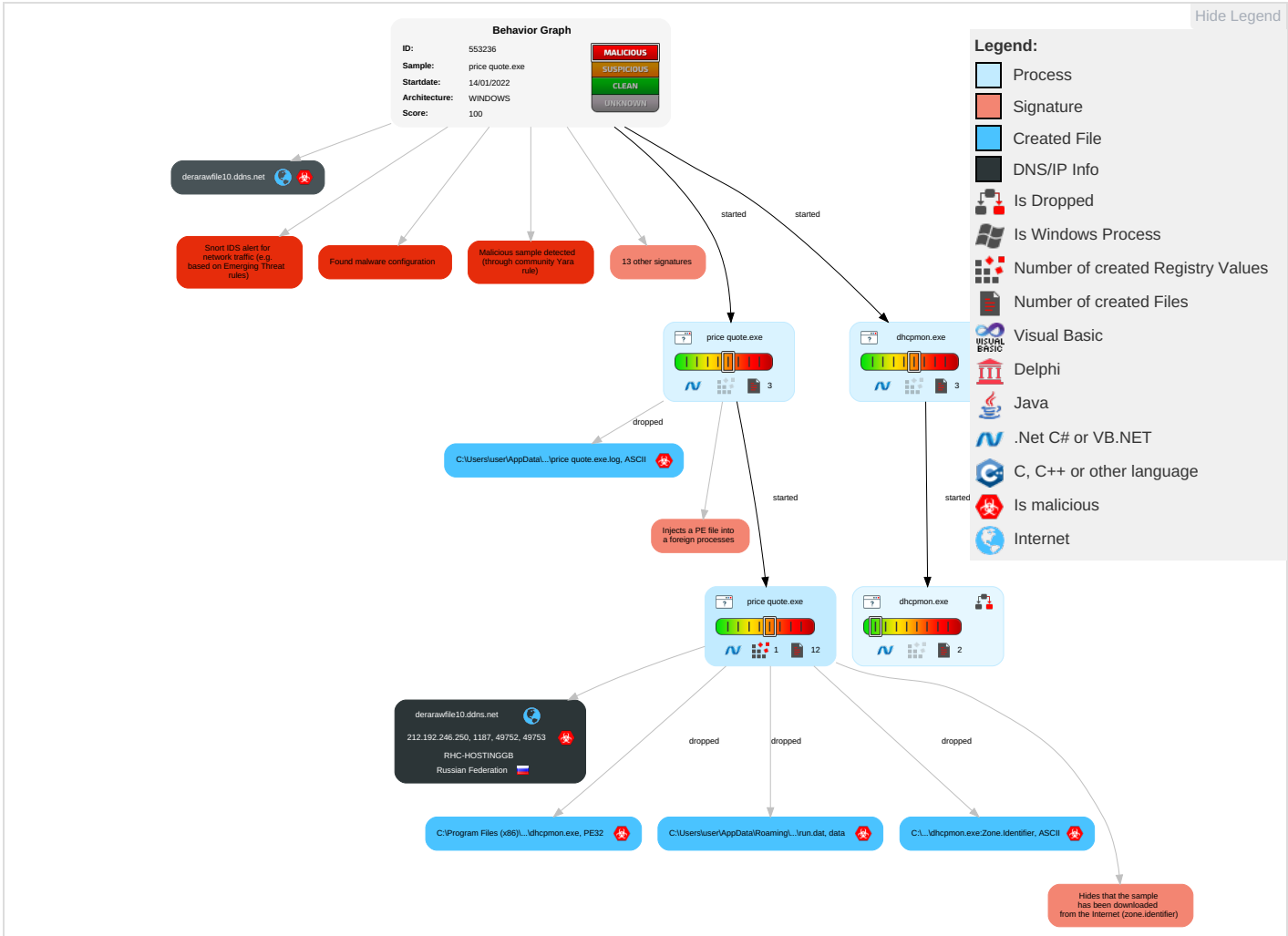
Yara detected Nanocore RAT

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	Path Interception	Process Injection 1 1 1	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1

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

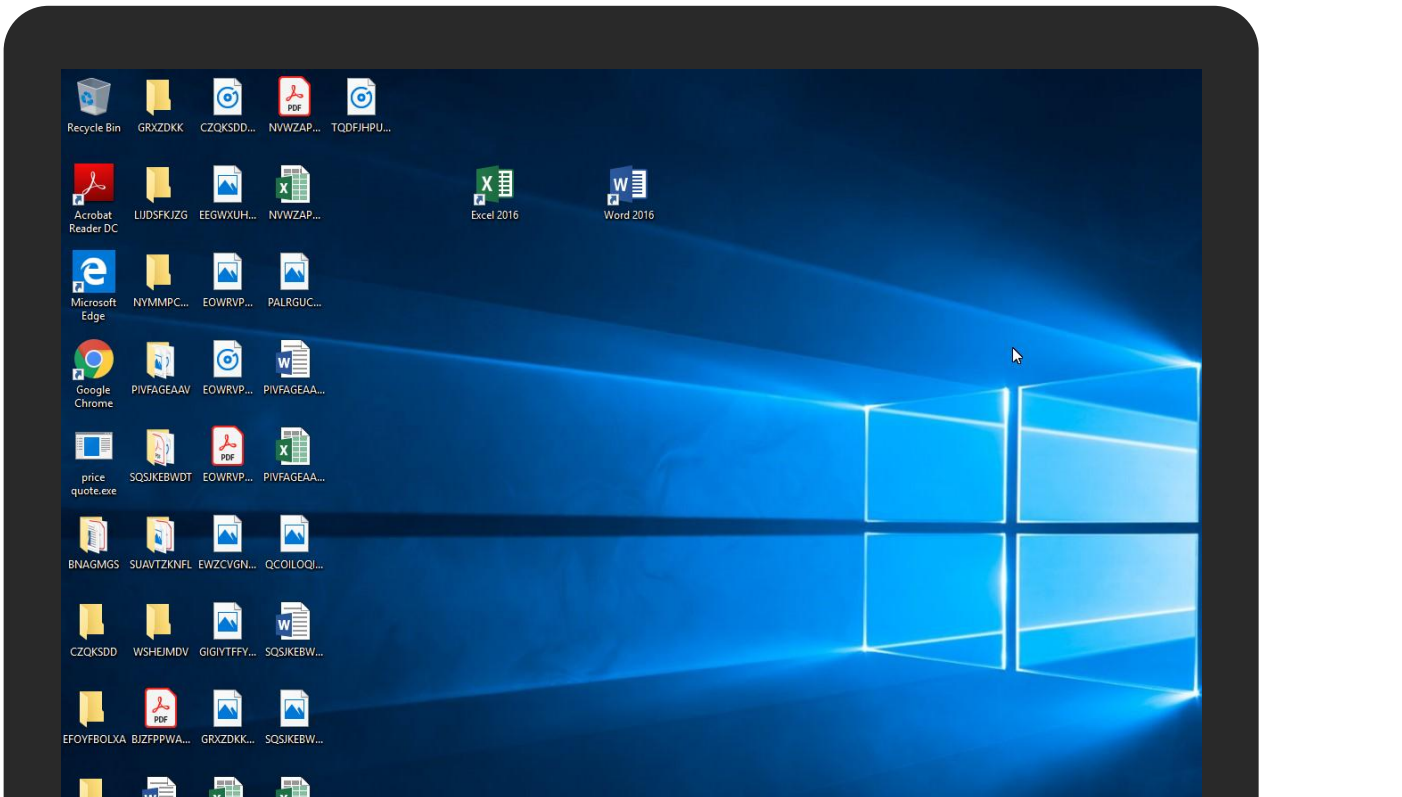
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
price quote.exe	28%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
price quote.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	28%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.price quote.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.price quote.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.price quote.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.price quote.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.price quote.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://en.wF	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comepko	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comT.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.commTTF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/tionV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.fontbureau.comH	0%	URL Reputation	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
derarawfile10.ddns.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cns-c	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
212.192.246250	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals9	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn6	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/aali~	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnicr	0%	URL Reputation	safe	
http://www.sakkal.com-b	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-h	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitud	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
derarawfile10.ddns.net	212.192.246.250	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
derarawfile10.ddns.net	true	• Avira URL Cloud: safe	unknown
212.192.246250	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.192.246.250	derarawfile10.ddns.net	Russian Federation		205220	RHC-HOSTINGGB	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553236
Start date:	14.01.2022
Start time:	14:30:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	price quote.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/8@20/1

EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.3%) • Quality average: 74.9% • Quality standard deviation: 23.8%
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

Simulations

Behavior and APIs

Time	Type	Description
14:31:30	API Interceptor	935x Sleep call for process: price quote.exe modified
14:31:38	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
14:31:49	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\price quote.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	576512
Entropy (8bit):	7.196584773251095
Encrypted:	false
SSDEEP:	12288:qbuK777777777777N7/PBmE7dRrFdaN7pgT8WOEQtxYqwEm:kuK777777777777l/Z/ZRrapgT1Oftxf
MD5:	5C7D156CA2EB9956E2DAE2DE52697AD5
SHA1:	F149BECE20CA820F558A40FDCA18D6B48BB0A46B
SHA-256:	E2228AE0E77D09A5B1592D133120E6B39171186E81E6837AE0DA254689127A00

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
SHA-512:	D3C9B4E3AEEED60D9056EA9CF584EA0DEC76027BA0CC1B19051F4A915669E82F310254E3747C1315D81DCFC2C9A4B0E0D9FBDFE7C8D0A971165E351B128D8E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....>.a..... .....@.. .....@..... ..@.....`...K..... ..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....e..(.....E.....L.....{...*"..}....*....{...*"..}....*....{...*"..}....*....{...*"..}....*....{...*"..}....*....0..... .....8}..... (....9....r...p.(.....(....:....~....8.....(.....(.....(.....(.....(....:....~....8.....(.....(.....(.....(....:....~....8.....(.....(.....(....8....~.....(..... .....8.....(..... .....8....8....r...p.(..... . .....8u.....(....:.... ....(

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\price quote.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\price quote.exe.log	
Process:	C:\Users\user\Desktop\price quote.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\price quote.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\price quote.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Lh:Lh
MD5:	CF4BDC77B88392AFBE1DE8BB1D6D8F9C
SHA1:	5ACDD85C54BD762CDFBF95542A6384290FD3BED1
SHA-256:	66F72D5D27839727A74911E1B5A4E9C1D9DBD136468F1A5F4AF88D21EC407718
SHA-512:	22EF3B82200CBFAA23276C013D0FCD0CBDFFB7D513B38DD4AEAF953AD79BEA66053BCE255A29FFECA327C2AC6B6B727F1441E06BFC52C9D27CE7E3DC300D27A
Malicious:	**true**
Reputation:	low
Preview:	.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\price quote.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\price quote.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_....Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.196584773251095
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:	price quote.exe
File size:	576512
MD5:	5c7d156ca2eb9956e2dae2de52697ad5
SHA1:	f149bece20ca820f558a40fdca18d6b48bb0a46b
SHA256:	e2228ae0e77d09a5b1592d133120e6b39171186e81e683 7ae0da254689127a00
SHA512:	d3c9b4e3aeeed60d9056ea9cf584ea0dec76027ba0cc1b 19051f4a915669e82f310254e3747c1315d81dcfc2c9a4b 0e0d9fbdfe7c8d0a971165e351b128d8d8e
SSDEEP:	12288:qbuK777777777777N7/PBmE7dRrFdaN7pgT8W OEQtxYqwEm:kuK777777777777l/Z/ZRrapgT1Oftxf
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.... >.a..... ....@.. .....@..... ...@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48e0ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E13E19 [Fri Jan 14 09:10:49 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x8c0b4	0x8c200	False	0.749325727587	data	7.20663433115	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x90000	0x5e4	0x600	False	0.4375	data	4.1740575342	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x92000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:31:36.305086	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64021	8.8.8.8	192.168.2.3
01/14/22-14:31:36.385914	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	1187	192.168.2.3	212.192.246.250
01/14/22-14:31:43.626684	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60784	8.8.8.8	192.168.2.3
01/14/22-14:31:43.655613	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	1187	192.168.2.3	212.192.246.250
01/14/22-14:31:49.157020	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	1187	192.168.2.3	212.192.246.250
01/14/22-14:31:53.858500	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59026	8.8.8.8	192.168.2.3
01/14/22-14:31:53.922916	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:00.547470	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49572	8.8.8.8	192.168.2.3
01/14/22-14:32:00.611402	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:05.615665	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60823	8.8.8.8	192.168.2.3
01/14/22-14:32:05.644233	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:11.637017	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:17.819218	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:24.425765	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:28.827318	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55393	8.8.8.8	192.168.2.3
01/14/22-14:32:28.857518	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49808	1187	192.168.2.3	212.192.246.250

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:32:34.833633	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49810	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:40.166937	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49812	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:46.159349	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55108	8.8.8.8	192.168.2.3
01/14/22-14:32:46.188304	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:52.149047	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49836	1187	192.168.2.3	212.192.246.250
01/14/22-14:32:58.123975	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64432	8.8.8.8	192.168.2.3
01/14/22-14:32:58.160779	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49837	1187	192.168.2.3	212.192.246.250
01/14/22-14:33:04.999424	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61120	8.8.8.8	192.168.2.3
01/14/22-14:33:05.029043	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	1187	192.168.2.3	212.192.246.250
01/14/22-14:33:11.043066	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49844	1187	192.168.2.3	212.192.246.250
01/14/22-14:33:17.100182	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49845	1187	192.168.2.3	212.192.246.250
01/14/22-14:33:23.115490	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56706	8.8.8.8	192.168.2.3
01/14/22-14:33:23.144789	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49846	1187	192.168.2.3	212.192.246.250
01/14/22-14:33:28.120108	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	1187	192.168.2.3	212.192.246.250

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:31:36.284166098 CET	192.168.2.3	8.8.8.8	0x6f0c	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:31:43.606801033 CET	192.168.2.3	8.8.8.8	0xc9d5	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:31:49.026016951 CET	192.168.2.3	8.8.8.8	0x3e32	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:31:53.837132931 CET	192.168.2.3	8.8.8.8	0x76d4	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:00.526484013 CET	192.168.2.3	8.8.8.8	0xb88d	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:05.593990088 CET	192.168.2.3	8.8.8.8	0x95b7	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:11.583415985 CET	192.168.2.3	8.8.8.8	0xcdca	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:17.748780966 CET	192.168.2.3	8.8.8.8	0x9e10	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:24.374528885 CET	192.168.2.3	8.8.8.8	0x5862	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:28.805947065 CET	192.168.2.3	8.8.8.8	0x2178	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:34.785166979 CET	192.168.2.3	8.8.8.8	0x19b2	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:40.117568970 CET	192.168.2.3	8.8.8.8	0xe37e	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:46.138710022 CET	192.168.2.3	8.8.8.8	0xd0bf	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:52.102338076 CET	192.168.2.3	8.8.8.8	0xce5	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:58.101628065 CET	192.168.2.3	8.8.8.8	0xf709	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:33:04.979983091 CET	192.168.2.3	8.8.8.8	0xbc99	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:33:10.995089054 CET	192.168.2.3	8.8.8.8	0x5e32	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:33:17.051153898 CET	192.168.2.3	8.8.8.8	0x30cf	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:33:23.095994949 CET	192.168.2.3	8.8.8.8	0x5945	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 14, 2022 14:33:28.072895050 CET	192.168.2.3	8.8.8.8	0x928b	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:31:36.305085897 CET	8.8.8.8	192.168.2.3	0x6f0c	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:31:43.626683950 CET	8.8.8.8	192.168.2.3	0xc9d5	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:31:49.045732021 CET	8.8.8.8	192.168.2.3	0x3e32	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:31:53.858500004 CET	8.8.8.8	192.168.2.3	0x76d4	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:00.547470093 CET	8.8.8.8	192.168.2.3	0xb88d	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:05.615664959 CET	8.8.8.8	192.168.2.3	0x95b7	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:11.602782965 CET	8.8.8.8	192.168.2.3	0xcdca	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:17.769610882 CET	8.8.8.8	192.168.2.3	0x9e10	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:24.393874884 CET	8.8.8.8	192.168.2.3	0x5862	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:28.827317953 CET	8.8.8.8	192.168.2.3	0x2178	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:34.804244041 CET	8.8.8.8	192.168.2.3	0x19b2	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:40.137969971 CET	8.8.8.8	192.168.2.3	0xe37e	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:46.159348965 CET	8.8.8.8	192.168.2.3	0xd0bf	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:52.120066881 CET	8.8.8.8	192.168.2.3	0xce5	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:32:58.123975039 CET	8.8.8.8	192.168.2.3	0xf709	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:33:04.999423981 CET	8.8.8.8	192.168.2.3	0xbc99	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:33:11.014730930 CET	8.8.8.8	192.168.2.3	0x5e32	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:33:17.070703030 CET	8.8.8.8	192.168.2.3	0x30cf	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:33:23.115489960 CET	8.8.8.8	192.168.2.3	0x5945	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)
Jan 14, 2022 14:33:28.092343092 CET	8.8.8.8	192.168.2.3	0x928b	No error (0)	derarawfil e10.ddns.net		212.192.246.250	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: price quote.exe PID: 4348 Parent PID: 3928

General

Start time:	14:31:23
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\price quote.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\price quote.exe"
Imagebase:	0x8f0000
File size:	576512 bytes
MD5 hash:	5C7D156CA2EB9956E2DAE2DE52697AD5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.309197369.0000000002D21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.309268951.0000000002D6A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.309685884.0000000003D29000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.309685884.0000000003D29000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.309685884.0000000003D29000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: price quote.exe PID: 5572 Parent PID: 4348

General

Start time:	14:31:31
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\price quote.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\price quote.exe
Imagebase:	0x5f0000
File size:	576512 bytes
MD5 hash:	5C7D156CA2EB9956E2DAE2DE52697AD5
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: 00000004.00000000.305911719.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.305911719.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.305911719.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.305509637.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.305509637.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.305509637.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.306358552.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.306358552.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.306358552.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.306874630.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.306874630.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.306874630.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 6856 Parent PID: 3352

General

Start time:	14:31:46
Start date:	14/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x910000

File size:	576512 bytes
MD5 hash:	5C7D156CA2EB9956E2DAE2DE52697AD5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000007.00000002.352160668.0000000002E0A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.352641807.0000000003DC9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.352641807.0000000003DC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.352641807.0000000003DC9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000007.00000002.351964936.0000000002DC1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 5756 Parent PID: 6856

General

Start time:	14:31:50
Start date:	14/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x650000
File size:	576512 bytes
MD5 hash:	5C7D156CA2EB9956E2DAE2DE52697AD5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.347828924.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.347828924.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.347828924.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.367879293.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.367879293.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.367879293.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.347339128.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.347339128.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.347339128.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.368705179.0000000002A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.368705179.0000000002A31000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.348315033.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.348315033.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.348315033.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.346842313.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.346842313.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.346842313.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.368784464.0000000003A39000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.368784464.0000000003A39000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis