ID: 383199
Sample Name:
CU3e1CWzlr.exe
Cookbook: default.jbs
Time: 13:11:11
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

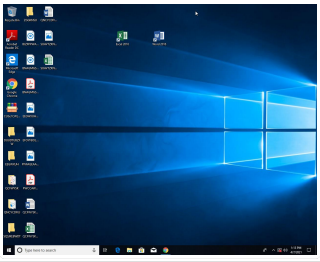
Analysis Report CU3e1CWzlr.exe

Overview

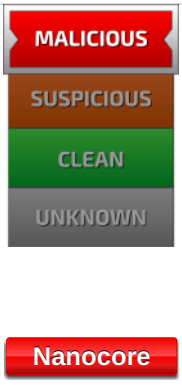
General Information

Sample Name:	CU3e1CWzlr.exe
Analysis ID:	383199
MD5:	bc906f26edfec13..
SHA1:	33933248690d87..
SHA256:	23ac7754b6ad5fc..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



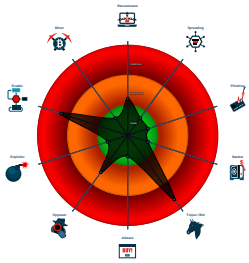
Nanocore

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

Signatures

- Antivirus detection for dropped file
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- CU3e1CWzlr.exe (PID: 6072 cmdline: 'C:\Users\user\Desktop\CU3e1CWzlr.exe' MD5: BC906F26EDFEC13CDB13D8A6B97F344B)
  - cmd.exe (PID: 6240 cmdline: C:\Windows\system32\cmd.exe /c "C:\1.bat" ' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Quotation.sfx.exe (PID: 6312 cmdline: Quotation.sfx.exe -p123 dc:\ MD5: 9C30B408BBF38395C4BB213682044B68)
      - Quotation.exe (PID: 6488 cmdline: 'C:\Quotation.exe' MD5: C83BD9093E7AE550FC49FDC1A90B7F9E)
        - schtasks.exe (PID: 6512 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA16B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 6520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - schtasks.exe (PID: 6568 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpA45A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 6576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Quotation.exe (PID: 6636 cmdline: C:\Quotation.exe 0 MD5: C83BD9093E7AE550FC49FDC1A90B7F9E)
- dhcpmon.exe (PID: 6656 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: C83BD9093E7AE550FC49FDC1A90B7F9E)
- dhcpmon.exe (PID: 6872 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: C83BD9093E7AE550FC49FDC1A90B7F9E)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "894ac765-a5c8-42af-bb6a-ac66f210",
  "Group": "Default",
  "Domain1": "185.244.26.250",
  "Domain2": "oleg321.ddns.net",
  "Port": 3231,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "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": "",
  "BackupDNSServer": "",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	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

Source	Rule	Description	Author	Strings
C:\Quotation.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 3 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.471922157.00000000051B0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000005.00000002.471922157.00000000051B0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
0000000C.00000000.230390276.0000000000AA2000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000000.230390276.0000000000AA2000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000000.230390276.0000000000AA2000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Click to see the 50 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.dhcpmon.exe.3fd311d.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x24178:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x241a5:$x2: IClientNetworkHost
11.2.dhcpmon.exe.3fd311d.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x24178:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x25253:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x24192:$s5: IClientLoggingHost
11.2.dhcpmon.exe.3fd311d.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
12.2.dhcpmon.exe.424eaf4.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x287a1:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x287ce:$x2: IClientNetworkHost
12.2.dhcpmon.exe.424eaf4.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x287a1:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x2987c:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x287bb:$s5: IClientLoggingHost
Click to see the 98 entries				

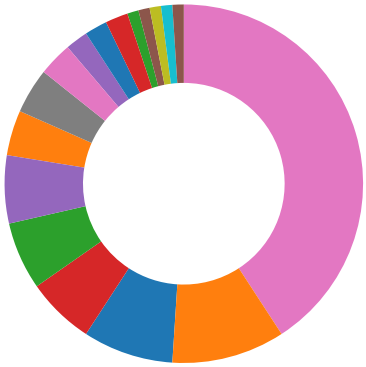
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

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

Boot Survival:

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)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

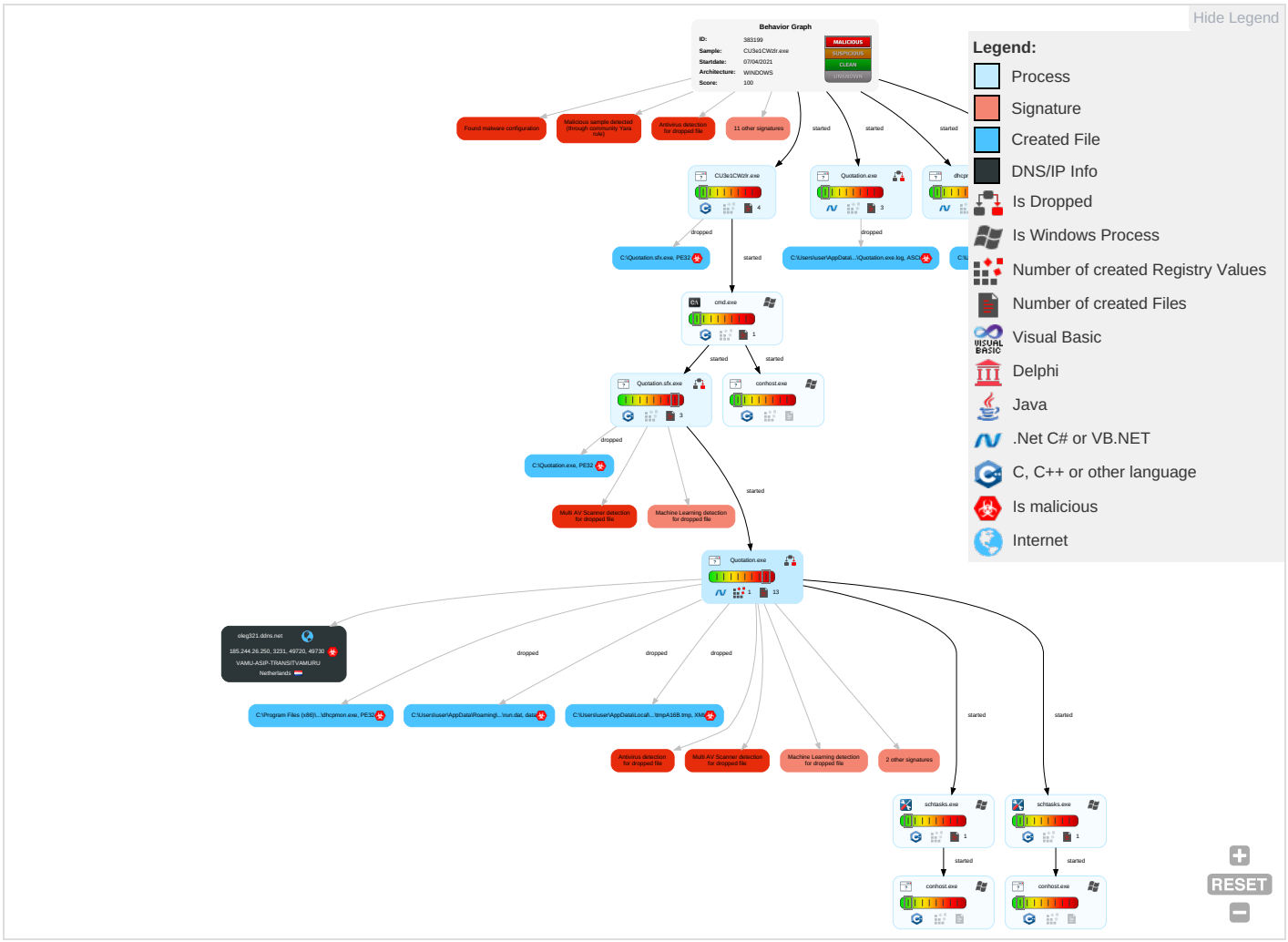
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Con
Valid Accounts	Scripting 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypte Channel
Default Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Sta Port 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Process Injection 1 2	Scripting 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Software
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applicati Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Security Software Discovery 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Applicati Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tran Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Prot

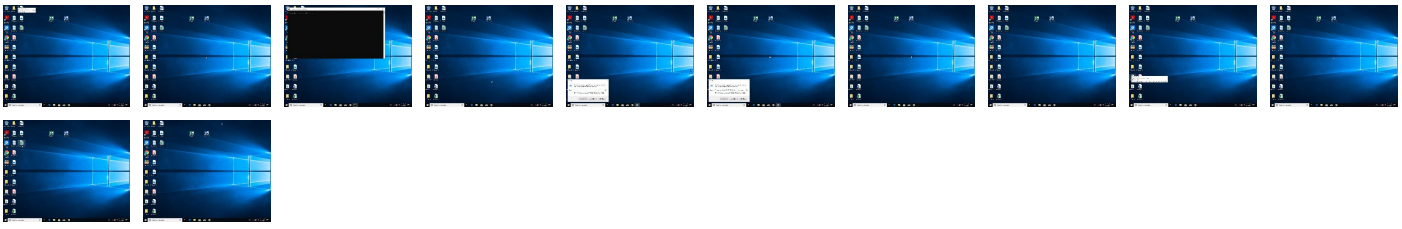
Behavior Graph



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
CU3e1CWzlr.exe	57%	Virustotal		Browse
CU3e1CWzlr.exe	35%	Metadefender		Browse
CU3e1CWzlr.exe	73%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
CU3e1CWzlr.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Quotation.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Quotation.sfx.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Quotation.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	86%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Quotation.exe	86%	Metadefender		Browse
C:\Quotation.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Quotation.sfx.exe	32%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Quotation.sfx.exe	76%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.Quotation.exe.390000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.Quotation.exe.5440000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
11.2.dhcpmon.exe.860000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.Quotation.exe.390000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.Quotation.exe.160000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.dhcpmon.exe.860000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.dhcpmon.exe.aa0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.Quotation.exe.160000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.dhcpmon.exe.aa0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
185.244.26.250	0%	Virustotal		Browse
185.244.26.250	0%	Avira URL Cloud	safe	
oleg321.ddns.net	0%	Avira URL Cloud	safe	

Domains and IPs

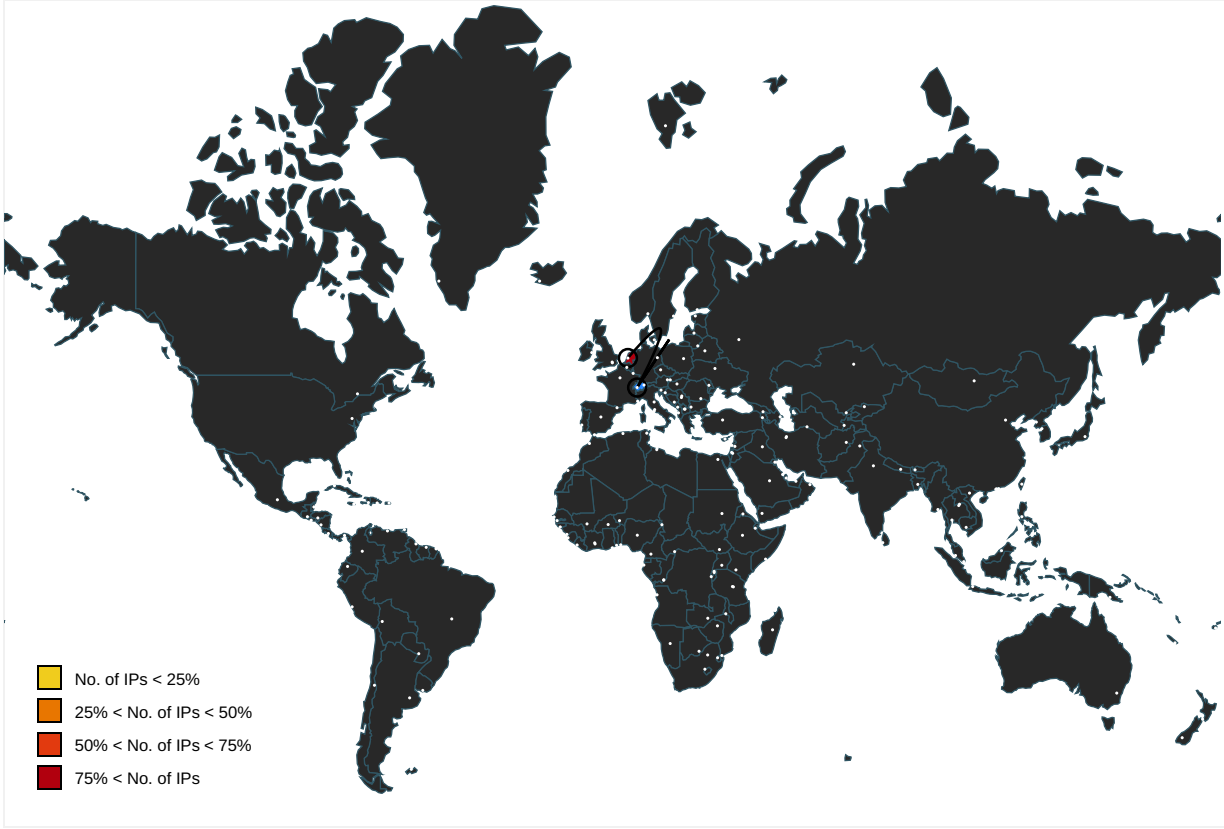
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
oleg321.ddns.net	185.244.26.250	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
185.244.26.250	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
oleg321.ddns.net	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.244.26.250	oleg321.ddns.net	Netherlands		47158	VAMU-ASIP-TRANSITVAMURU	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383199
Start date:	07.04.2021
Start time:	13:11:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CU3e1CWzlr.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:	35
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@18/10@9/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 99.8% (good quality ratio 95.5%) • Quality average: 79.5% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 70% • 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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:12:03	Task Scheduler	Run new task: DHCP Monitor path: "C:\Quotation.exe" s>$(Arg0)
13:12:03	API Interceptor	1012x Sleep call for process: Quotation.exe modified
13:12:03	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
13:12:04	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VAMU-ASIP-TRANSITVAMURU	odW62S0306.exe	Get hash	malicious	Browse	• 185.244.26.204
	ORDEN.exe	Get hash	malicious	Browse	• 185.244.26.196
	sB2ppXd9nd1DsMC.exe	Get hash	malicious	Browse	• 185.244.26.241
	2CBPOfVTs5QeG8Z.exe	Get hash	malicious	Browse	• 185.244.26.208
	i5TiYkAYkWJy1O8.exe	Get hash	malicious	Browse	• 185.244.26.208
	NEW ORDERS.exe	Get hash	malicious	Browse	• 185.244.26.227
	DHL STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 185.244.26.194
	DHLMT-BL-PL-CI08348-SHIPMENT.pdf.xls.exe	Get hash	malicious	Browse	• 185.244.26.221
	sf_express_waybill_parcelArrival.docx.exe	Get hash	malicious	Browse	• 185.244.26.221

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	COVID-19 CDC Secon Outbreak Warning release.exe	Get hash	malicious	Browse	• 185.244.26.221
	Kaszfnrcg7.exe	Get hash	malicious	Browse	• 185.244.26.213
	Inv No.5200003959 (FL).exe	Get hash	malicious	Browse	• 185.244.26.247
	CDC GUIDES COVID-19 Second Outbreak Warning release.exe	Get hash	malicious	Browse	• 185.244.26.221
	85RNPseqgJ.exe	Get hash	malicious	Browse	• 185.244.26.206
	Olzcqxcxnf9.exe	Get hash	malicious	Browse	• 185.244.26.213
	R1MfM3z2Nz.exe	Get hash	malicious	Browse	• 185.244.26.206
	Fh06tuCZaK.exe	Get hash	malicious	Browse	• 185.244.26.206
	AlTKG0L5d8.exe	Get hash	malicious	Browse	• 185.244.26.206
	Rbmmuoavjkz8.exe	Get hash	malicious	Browse	• 185.244.26.213
	PO 6300019918..exe	Get hash	malicious	Browse	• 185.244.26.206

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\1.bat	
Process:	C:\Users\user\Desktop\CU3e1CWzlr.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.378783493486176
Encrypted:	false
SSDEEP:	3:pSeEJNFIVUGCf5:WNyVUGCf5
MD5:	31C145900B71996E1EF9D60F37899282
SHA1:	C6CE32DD6F468585A47AB317D5FBC14643F04BAE
SHA-256:	64A6B58057E1FAF070B6757CB96699E6037079013D2F6103C146EC14C0788014
SHA-512:	C93AE9E6EF4CF26A07D4C610A9FF66C27C822A98F48F858E671959209CFEE6DC65C9862DF33285D397FBBAB18E6D162596F4FCBBC939ADEF9D65C91D5E47C25
Malicious:	false
Reputation:	low
Preview:	Quotation.sfx.exe -p123 dc:\

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Quotation.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	7.45145986611402
Encrypted:	false
SSDEEP:	3072:MzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIPhO1RxN+dAu8imqhVPd63DfOM:MLV6Bta6dtJmakIM5ewC86hV1UfUgrTJ
MD5:	C83BD9093E7AE550FC49FDC1A90B7F9E
SHA1:	59E77D7E3C293A81C1113EF21B93F0D2792CF0D2
SHA-256:	C3E6B1EB9B5B402489CA89A617577E0794E3B6D6A542AD11B43F9D37F0664622
SHA-512:	0812172CA01847BA1161A7A82D93E25B132D311B085EE643D915F0168A7333BBE8E77830D726A2E037744FCA24EC0285E36B017BC9CF28C4668CAACA52800532
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 100%
Reputation:	low

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....b..... .....@.. ....8...W.... ..._..... .....`.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ...3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Quotation.exe

Process:	C:\Quotation.sfx.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	207872
Entropy (8bit):	7.45145986611402
Encrypted:	false
SSDEEP:	3072:MzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIPhO1RxN+dAu8imqhVPd63DfOM:MLV6Bta6dtJmakIM5ewC86hV1UfUgrTJ
MD5:	C83BD9093E7AE550FC49FDC1A90B7F9E
SHA1:	59E77D7E3C293A81C1113EF21B93F0D2792CF0D2
SHA-256:	C3E6B1EB9B5B402489CA89A617577E0794E3B6D6A542AD11B43F9D37F0664622
SHA-512:	0812172CA01847BA1161A7A82D93E25B132D311B085EE643D915F0168A7333BBE8E77830D726A2E037744FCA24EC0285E36B017BC9CF28C4668CAACA52800532
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Quotation.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Quotation.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Quotation.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Quotation.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....b..... .....@.. ....8...W.... ..._..... .....`.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ...3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Quotation.sfx.exe

Process:	C:\Users\user\Desktop\CU3e1CWzlr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	458627
Entropy (8bit):	7.315371843776508
Encrypted:	false
SSDEEP:	12288:9crNS33L10QdrXP/X+tGfn8uFLRw46p2ptRv:ANA3R5drXPrf8uXdbV
MD5:	9C30B408BBF38395C4BB213682044B68
SHA1:	05B0F3897EC86D4803B4E631A68AB86DDDC6CA54
SHA-256:	23748678A2C83CEE8C47A97C1263E57E3439F0E78141E2962966F59BAE87110A
SHA-512:	0480FDC58E4B5D8785CFEDE13C601E587EBA67968F117E678FFE893516B087C7057EF381B0DD246B61F5710EB06253CBAE7E1A712A4B3C98796954EFD5102213
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 32%, Browse • Antivirus: ReversingLabs, Detection: 76%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....b.....b..<....b.....)^..... ....%..... .....Rich.....PE..L.....\.....Y.....@.....@.....4.....<.....n..T.....(...@.....\...L... .....text...T..... ..`.rdata.....@..@.data.....@....gfids.....@..@.rsrc.....@..@.reloc..... ...x.....@..B.....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Quotation.exe.log

Process:	C:\Quotation.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Quotation.exe.log	
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_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):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpA16B.tmp	
Process:	C:\Quotation.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1279
Entropy (8bit):	5.075594439226328
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK01xtn:cbk4oL600QydbQxIYODOLedq3cj
MD5:	020431D764EA265AB8462B9C69828063
SHA1:	257B24D0FF69B531CA5C0BA7E8D0A9CA208EEB9C
SHA-256:	F85E229E04B155C4E0B5C7788DD735FB17542CE2028B3441560B77B30BB35306
SHA-512:	A83EDADF38E8A2FE3AC31B0FBEA47BDDF693B5873E88BCE4E00739691AF1486A83F083C6D5A62C1CED1EACFA81702734B694DF0FA4246483C6B729A91CB6D4 72
Malicious:	**true**
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\Local\Temp\tmpA45A.tmp	
Process:	C:\Quotation.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpA45A.tmp	
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\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Quotation.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:3UVt:a
MD5:	D6676EE740B651B46142810DB18B57F0
SHA1:	EE8AC1B50C1DE890E23B6B536AC43F7A7EE1E485
SHA-256:	25A1101CDA6648DBA36FE002068CAB8D886668E21D6D4776F1042B430F813981
SHA-512:	994EB04B85B4E2BE93A177E020382B24E32FC1B9C1CA6CF0257BCD823251596EF8C08166602034D4DCCCD38BB22699E6707B0038EC5DB51B46A4DB252D9C83A7
Malicious:	**true**
Preview:	.'.g...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Quotation.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.625
Encrypted:	false
SSDEEP:	3:oFMeNn:oFh
MD5:	CCF14158D80722DA582C415C0CD0C267
SHA1:	1EEA0355F97142D9C9B123C04A9855A00695FA96
SHA-256:	42A6CC1CA4FD2D7225F9D7ACB0243D15BAC13BB70D4B5716F55AFEED5551AF14
SHA-512:	B6D9CCBF825A1361C3AC2715EE7560D099645B532E2D2E9BECC5D69834D2F55E4D1D11854488E09A587D462F535A7E8DBD96434B1DC1AA2893D3726D9CFD936
Malicious:	false
Preview:	C:\Quotation.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.567706196816486
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	CU3e1CWzlr.exe
File size:	620007
MD5:	bc906f26edfec13cdb13d8a6b97f344b
SHA1:	33933248690d87f77693865e7393395ec2ea3792
SHA256:	23ac7754b6ad5fc382857b05ad514a716cd3dcf861867d3be02a5a92ca7fe067
SHA512:	cbeeaade944273775bc4a7f7a436599c5c7212ab7d2b864045424d8f69b0d91fb6e01fae7390f38f5dd119c3457d534ed4547c725e300ed8c6416e47d58549ae
SSDEEP:	12288:9crNS33L10QdrXP/X+tGfnYMOwYgc4T7fkj0D+8:ANA3R5drXPrfY+BS0i8

General

File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....~..... .....b.....b..<....b.....)^..... ....%..... .....

File Icon

Icon Hash:	d49494d6c88ecec2

Static PE Info

General

Entrypoint:	0x41d759
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5CC4B58F [Sat Apr 27 20:03:27 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	00be6e6c4f9e287672c8301b72bdabf3

Entrypoint Preview

Instruction
call 00007F09B877247Fh
jmp 00007F09B8771EB3h
cmp ecx, dword ptr [0043A1C8h]
jne 00007F09B8772025h
ret
jmp 00007F09B87725F5h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 00430FE8h
mov dword ptr [ecx], 00431994h
ret
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F09B87655CBh
mov dword ptr [esi], 004319A0h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 004319A8h
mov dword ptr [ecx], 004319A0h
ret

Instruction
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F09B8771FCCh
push 00437B74h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F09B87748B6h
int3
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F09B8771FE2h
push 00437DA4h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F09B8774899h
int3
jmp 00007F09B87768E5h
jmp dword ptr [0043025Ch]
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push 004209A0h
push dword ptr fs:[00000000h]
mov eax, dword ptr [esp+10h]

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [EXP] VS2015 UPD3.1 build 24215 • [LNK] VS2015 UPD3.1 build 24215 • [IMP] VS2008 SP1 build 30729 • [C++] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x38cc0	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x38cf4	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5d000	0xdfd0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6b000	0x1fcc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x36ee0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x31928	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x30000	0x25c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3824c	0x120	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2e854	0x2ea00	False	0.590891002011	data	6.69230972772	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x30000	0x9a9c	0x9c00	False	0.457131410256	DOS executable (COM, 0x8C-variant)	5.13286467456	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3a000	0x213d0	0xc00	False	0.2802734375	data	3.25381103208	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x5c000	0xe8	0x200	False	0.33984375	data	2.11154177446	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5d000	0xdfd0	0xe000	False	0.637067522321	data	6.63679065017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6b000	0x1fcc	0x2000	False	0.794555664062	data	6.64554135223	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x5d650	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x5e198	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x5f748	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x5fcb0	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x60558	0xea8	data	English	United States
RT_ICON	0x61400	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x61868	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x62910	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x64eb8	0x3d71	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_DIALOG	0x69588	0x286	data	English	United States
RT_DIALOG	0x69358	0x13a	data	English	United States
RT_DIALOG	0x69498	0xec	data	English	United States
RT_DIALOG	0x69228	0x12e	data	English	United States
RT_DIALOG	0x68ef0	0x338	data	English	United States
RT_DIALOG	0x68c98	0x252	data	English	United States
RT_STRING	0x69f68	0x1e2	data	English	United States
RT_STRING	0x6a150	0x1cc	data	English	United States
RT_STRING	0x6a320	0x1ee	data	English	United States
RT_STRING	0x6a510	0x146	Hitachi SH big-endian COFF object file, not stripped, 17152 sections, symbol offset=0x73006500	English	United States
RT_STRING	0x6a658	0x446	data	English	United States
RT_STRING	0x6aaa0	0x166	data	English	United States
RT_STRING	0x6ac08	0x120	data	English	United States
RT_STRING	0x6ad28	0x10a	data	English	United States
RT_STRING	0x6ae38	0xbc	data	English	United States
RT_STRING	0x6aef8	0xd6	data	English	United States
RT_GROUP_ICON	0x68c30	0x68	data	English	United States
RT_MANIFEST	0x69810	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetLastError, SetLastError, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, GetTickCount, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetOEMCP, GetCommandLineA, GetEnvironmentStringsW, FreeEnvironmentStringsW, DecodePointer
gdiplus.dll	GdiplusShutdown, GdiplusStartup, GdipCreateHBITMAPFromBitmap, GdipCreateBitmapFromStreamICM, GdipCreateBitmapFromStream, GdipDisposeImage, GdipCloneImage, GdipFree, GdipAlloc

Possible Origin

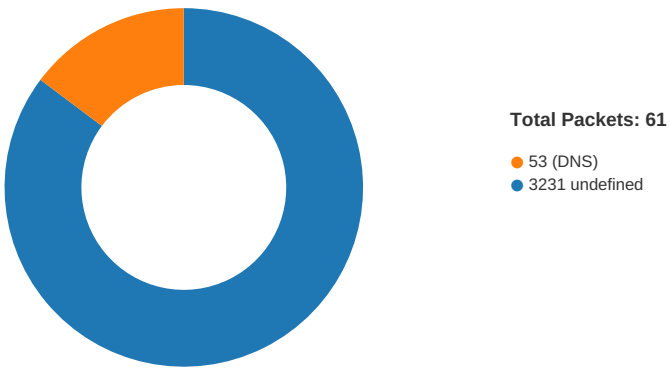
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/07/21-13:13:12.481307	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63619	37.235.1.174	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 13:12:04.284943104 CEST	49717	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:07.274842024 CEST	49717	3231	192.168.2.3	185.244.26.250

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 13:12:13.275221109 CEST	49717	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:23.153405905 CEST	49720	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:23.207156897 CEST	3231	49720	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:23.713697910 CEST	49720	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:23.767625093 CEST	3231	49720	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:24.276237965 CEST	49720	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:24.329905987 CEST	3231	49720	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:28.340193033 CEST	49730	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:28.396034956 CEST	3231	49730	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:28.932753086 CEST	49730	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:28.986098051 CEST	3231	49730	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:29.635945082 CEST	49730	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:29.689321041 CEST	3231	49730	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:33.851739883 CEST	49736	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:33.905407906 CEST	3231	49736	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:34.433254957 CEST	49736	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:34.486736059 CEST	3231	49736	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:35.136393070 CEST	49736	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:35.189851999 CEST	3231	49736	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:40.075057983 CEST	49738	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:40.131113052 CEST	3231	49738	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:40.636879921 CEST	49738	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:40.690064907 CEST	3231	49738	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:41.324430943 CEST	49738	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:41.377650976 CEST	3231	49738	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:45.530728102 CEST	49741	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:45.584055901 CEST	3231	49741	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:46.124057055 CEST	49741	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:46.178337097 CEST	3231	49741	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:46.824892044 CEST	49741	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:46.878628016 CEST	3231	49741	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:50.904771090 CEST	49743	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:50.958117008 CEST	3231	49743	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:51.637808084 CEST	49743	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:51.690824032 CEST	3231	49743	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:52.297792912 CEST	49743	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:52.351032019 CEST	3231	49743	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:56.423825026 CEST	49750	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:56.479959011 CEST	3231	49750	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:57.138377905 CEST	49750	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:57.192867041 CEST	3231	49750	185.244.26.250	192.168.2.3
Apr 7, 2021 13:12:57.700845957 CEST	49750	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:12:57.754596949 CEST	3231	49750	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:01.765269041 CEST	49751	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:01.818501949 CEST	3231	49751	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:02.327560902 CEST	49751	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:02.380445004 CEST	3231	49751	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:02.889513016 CEST	49751	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:02.942847967 CEST	3231	49751	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:07.101444960 CEST	49752	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:07.154831886 CEST	3231	49752	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:07.654999018 CEST	49752	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:07.708323002 CEST	3231	49752	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:08.217320919 CEST	49752	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:08.270323992 CEST	3231	49752	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:12.519479036 CEST	49753	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:12.573050976 CEST	3231	49753	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:13.077043056 CEST	49753	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:13.130373955 CEST	3231	49753	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:13.639755964 CEST	49753	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:13.693152905 CEST	3231	49753	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:17.929892063 CEST	49754	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:17.983099937 CEST	3231	49754	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:18.483767986 CEST	49754	3231	192.168.2.3	185.244.26.250

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 13:13:18.537029028 CEST	3231	49754	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:19.046360970 CEST	49754	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:19.099663019 CEST	3231	49754	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:23.359709024 CEST	49755	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:23.413091898 CEST	3231	49755	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:23.921894073 CEST	49755	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:23.974956989 CEST	3231	49755	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:24.479491949 CEST	49755	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:24.533152103 CEST	3231	49755	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:28.694823027 CEST	49757	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:28.748089075 CEST	3231	49757	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:29.265958071 CEST	49757	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:29.319535017 CEST	3231	49757	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:29.828583956 CEST	49757	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:29.882317066 CEST	3231	49757	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:33.893865108 CEST	49759	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:33.948729992 CEST	3231	49759	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:34.454088926 CEST	49759	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:34.507719040 CEST	3231	49759	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:35.016555071 CEST	49759	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:35.069547892 CEST	3231	49759	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:39.187438965 CEST	49760	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:39.243577957 CEST	3231	49760	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:39.751199961 CEST	49760	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:39.805200100 CEST	3231	49760	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:40.313762903 CEST	49760	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:40.370985031 CEST	3231	49760	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:44.520028114 CEST	49761	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:44.573076963 CEST	3231	49761	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:45.079724073 CEST	49761	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:45.133033037 CEST	3231	49761	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:45.642371893 CEST	49761	3231	192.168.2.3	185.244.26.250
Apr 7, 2021 13:13:45.696996927 CEST	3231	49761	185.244.26.250	192.168.2.3
Apr 7, 2021 13:13:50.252599001 CEST	49763	3231	192.168.2.3	185.244.26.250

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 13:12:33.791883945 CEST	54366	53	192.168.2.3	37.235.1.174
Apr 7, 2021 13:12:33.844490051 CEST	53	54366	37.235.1.174	192.168.2.3
Apr 7, 2021 13:12:39.319566011 CEST	57762	53	192.168.2.3	37.235.1.174
Apr 7, 2021 13:12:40.073358059 CEST	53	57762	37.235.1.174	192.168.2.3
Apr 7, 2021 13:12:45.461173058 CEST	56132	53	192.168.2.3	37.235.1.174
Apr 7, 2021 13:12:45.529616117 CEST	53	56132	37.235.1.174	192.168.2.3
Apr 7, 2021 13:13:06.998872042 CEST	61292	53	192.168.2.3	37.235.1.174
Apr 7, 2021 13:13:07.099144936 CEST	53	61292	37.235.1.174	192.168.2.3
Apr 7, 2021 13:13:12.341939926 CEST	63619	53	192.168.2.3	37.235.1.174
Apr 7, 2021 13:13:12.481307030 CEST	53	63619	37.235.1.174	192.168.2.3
Apr 7, 2021 13:13:17.773648977 CEST	64938	53	192.168.2.3	37.235.1.174
Apr 7, 2021 13:13:17.928342104 CEST	53	64938	37.235.1.174	192.168.2.3
Apr 7, 2021 13:13:39.110472918 CEST	52123	53	192.168.2.3	37.235.1.174
Apr 7, 2021 13:13:39.134844065 CEST	53	52123	37.235.1.174	192.168.2.3
Apr 7, 2021 13:13:44.493109941 CEST	56130	53	192.168.2.3	37.235.1.174
Apr 7, 2021 13:13:44.517874002 CEST	53	56130	37.235.1.174	192.168.2.3
Apr 7, 2021 13:13:49.753454924 CEST	56338	53	192.168.2.3	37.235.1.174
Apr 7, 2021 13:13:50.250629902 CEST	53	56338	37.235.1.174	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 13:12:33.791883945 CEST	192.168.2.3	37.235.1.174	0x393c	Standard query (0)	oleg321.ddns.net	A (IP address)	IN (0x0001)
Apr 7, 2021 13:12:39.319566011 CEST	192.168.2.3	37.235.1.174	0x803	Standard query (0)	oleg321.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 13:12:45.461173058 CEST	192.168.2.3	37.235.1.174	0x72b0	Standard query (0)	oleg321.ddns.net	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:06.998872042 CEST	192.168.2.3	37.235.1.174	0xc0f8	Standard query (0)	oleg321.ddns.net	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:12.341939926 CEST	192.168.2.3	37.235.1.174	0x4543	Standard query (0)	oleg321.ddns.net	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:17.773648977 CEST	192.168.2.3	37.235.1.174	0xfcf1	Standard query (0)	oleg321.ddns.net	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:39.110472918 CEST	192.168.2.3	37.235.1.174	0x46e1	Standard query (0)	oleg321.ddns.net	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:44.493109941 CEST	192.168.2.3	37.235.1.174	0x2b7a	Standard query (0)	oleg321.ddns.net	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:49.753454924 CEST	192.168.2.3	37.235.1.174	0x8bee	Standard query (0)	oleg321.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

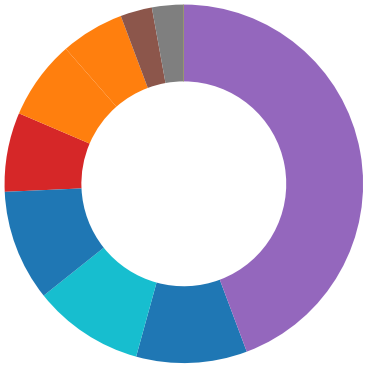
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 13:12:33.844490051 CEST	37.235.1.174	192.168.2.3	0x393c	No error (0)	oleg321.ddns.net		185.244.26.250	A (IP address)	IN (0x0001)
Apr 7, 2021 13:12:40.073358059 CEST	37.235.1.174	192.168.2.3	0x803	No error (0)	oleg321.ddns.net		185.244.26.250	A (IP address)	IN (0x0001)
Apr 7, 2021 13:12:45.529616117 CEST	37.235.1.174	192.168.2.3	0x72b0	No error (0)	oleg321.ddns.net		185.244.26.250	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:07.099144936 CEST	37.235.1.174	192.168.2.3	0xc0f8	No error (0)	oleg321.ddns.net		185.244.26.250	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:12.481307030 CEST	37.235.1.174	192.168.2.3	0x4543	No error (0)	oleg321.ddns.net		185.244.26.250	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:17.928342104 CEST	37.235.1.174	192.168.2.3	0xfcf1	No error (0)	oleg321.ddns.net		185.244.26.250	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:39.134844065 CEST	37.235.1.174	192.168.2.3	0x46e1	No error (0)	oleg321.ddns.net		185.244.26.250	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:44.517874002 CEST	37.235.1.174	192.168.2.3	0x2b7a	No error (0)	oleg321.ddns.net		185.244.26.250	A (IP address)	IN (0x0001)
Apr 7, 2021 13:13:50.250629902 CEST	37.235.1.174	192.168.2.3	0x8bee	No error (0)	oleg321.ddns.net		185.244.26.250	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- CU3e1CWzlr.exe
- cmd.exe
- conhost.exe
- Quotation.sfx.exe
- Quotation.exe
- schtasks.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- Quotation.exe
- dhcpmon.exe
- dhcpmon.exe



Click to jump to process

System Behavior

Analysis Process: CU3e1CWzlr.exe PID: 6072 Parent PID: 5704

General

Start time:	13:11:56
Start date:	07/04/2021
Path:	C:\Users\user\Desktop\CU3e1CWzlr.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CU3e1CWzlr.exe'
Imagebase:	0xcc0000
File size:	620007 bytes
MD5 hash:	BC906F26EDFEC13CDB13D8A6B97F344B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:__tmp_rar_sfx_access_check_3772593	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	CC95CF	CreateFileW
C:\\1.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	CC95CF	CreateFileW
C:\\Quotation.sfx.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	CC95CF	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:__tmp_rar_sfx_access_check_3772593	success or wait	1	CC9E13	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\1.bat	unknown	28	51 75 6f 74 61 74 69 6f 6e 2e 73 66 78 2e 65 78 65 20 2d 70 31 32 33 20 64 63 3a 5c	Quotation.sfx.exe -p123 dc:\	success or wait	1	CC9CA6	WriteFile
C:\Quotation.sfx.exe	unknown	65536	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 10 01 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 f3 9f 7e 98 b7 fe 10 cb b7 fe 10 cb b7 fe 10 cb 03 62 e1 cb bc fe 10 cb 03 62 e3 cb 3c fe 10 cb 03 62 e2 cb af fe 10 cb 29 5e d7 cb b6 fe 10 cb 8c a0 13 ca a1 fe 10 cb 8c a0 14 ca a4 fe 10 cb 8c a0 15 ca 9b fe 10 cb be 86 93 cb bd fe 10 cb be 86 83 cb b2 fe 10 cb b7 fe 11 cb bc ff 10 cb 20 a0 15 ca 87 fe 10 cb 20 a0 10 ca b6 fe 10 cb 25 a0 ef cb b6 fe 10 cb 20 a0 12 ca b6 fe 10	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.........~..............b.......b.. <....b......)^.......... ....%.......	success or wait	28	CC9CA6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CU3e1CWzlr.exe	unknown	8192	success or wait	75	CC9691	ReadFile

Analysis Process: cmd.exe PID: 6240 Parent PID: 6072

General

Start time:	13:11:57
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ''C:\1.bat' '
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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\1.bat	unknown	8191	success or wait	1	BDFB07	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\1.bat	unknown	8191	end of file	1	BDFB07	ReadFile
C:\1.bat	unknown	8191	end of file	1	BDFB07	ReadFile
C:\1.bat	unknown	8191	end of file	1	BDFB07	ReadFile

Analysis Process: conhost.exe PID: 6256 Parent PID: 6240

General

Start time:	13:11:58
Start date:	07/04/2021
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.sfx.exe PID: 6312 Parent PID: 6240

General

Start time:	13:11:58
Start date:	07/04/2021
Path:	C:\Quotation.sfx.exe
Wow64 process (32bit):	true
Commandline:	Quotation.sfx.exe -p123 dc:\
Imagebase:	0x340000
File size:	458627 bytes
MD5 hash:	9C30B408BBF38395C4BB213682044B68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 32%, Metadefender, Browse • Detection: 76%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:__tmp_rar_sfx_access_check_3774828	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	3495CF	CreateFileW
C:\\Quotation.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3495CF	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:__tmp_rar_sfx_access_check_3774828	success or wait	1	349E13	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Quotation.exe	unknown	47616	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 a1 27 e9 54 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 c8 01 00 00 62 01 00 00 00 00 00 92 e7 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....'.T..... .....b..... .....@..	success or wait	11	349CA6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Quotation.sfx.exe	unknown	8192	success or wait	72	349691	ReadFile

Analysis Process: Quotation.exe PID: 6488 Parent PID: 6312

General

Start time:	13:12:00
Start date:	07/04/2021
Path:	C:\Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Quotation.exe'
Imagebase:	0x160000
File size:	207872 bytes
MD5 hash:	C83BD9093E7AE550FC49FDC1A90B7F9E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.471922157.00000000051B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.471922157.00000000051B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.464609033.0000000000162000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.464609033.0000000000162000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.464609033.0000000000162000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.472020860.0000000005440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.472020860.0000000005440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.472020860.0000000005440000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.470841608.00000000037B7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.470841608.00000000037B7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.205169235.0000000000162000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.205169235.0000000000162000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.205169235.0000000000162000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Quotation.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Quotation.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Quotation.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Quotation.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 86%, Metadefender, Browse • Detection: 100%, ReversingLabs
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	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	4A807A1	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	4A8089B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4A807A1	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	4A80B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpA16B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4A80D1C	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	4A8089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA45A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4A80D1C	GetTempFileNameW
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	4A807A1	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	4A807A1	CreateDirectoryW
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	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA16B.tmp	success or wait	1	88BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA45A.tmp	success or wait	1	88BF0E	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	15 27 b1 67 01 fa d8 48	.'.g...H	success or wait	1	4A80A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 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 00 80 00 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 a1 27 e9 54 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 c8 01 00 00 62 01 00 00 00 00 00 92 e7 01 00 00 20 00 00 00 00 02 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 80 03 00 00 02 00 00 00 00 00 00 02 00 00 00 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....'.T.......... ....b........... ....@..	success or wait	2	4A80B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpA16B.tmp	unknown	1279	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.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveTo ken</LogonType>	success or wait	1	4A80A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	16	43 3a 5c 51 75 6f 74 61 74 69 6f 6e 2e 65 78 65	C:\Quotation.exe	success or wait	1	4A80A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA45A.tmp	unknown	1310	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	4A80A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Quotation.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Quotation.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4A80A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	4A80C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 6512 Parent PID: 6488

General

Start time:	13:12:01
Start date:	07/04/2021
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\tmpA16B.tmp'

Imagebase:	0x11b0000
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\tmpA16B.tmp	unknown	2	success or wait	1	11BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA16B.tmp	unknown	1280	success or wait	1	11BABD9	ReadFile

Analysis Process: conhost.exe PID: 6520 Parent PID: 6512

General

Start time:	13:12:01
Start date:	07/04/2021
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: schtasks.exe PID: 6568 Parent PID: 6488

General

Start time:	13:12:02
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpA45A.tmp'
Imagebase:	0x11b0000
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\tmpA45A.tmp	unknown	2	success or wait	1	11BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA45A.tmp	unknown	1311	success or wait	1	11BABD9	ReadFile

Analysis Process: conhost.exe PID: 6576 Parent PID: 6568

General

Start time:	13:12:02
Start date:	07/04/2021
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.exe PID: 6636 Parent PID: 528

General

Start time:	13:12:03
Start date:	07/04/2021
Path:	C:\Quotation.exe
Wow64 process (32bit):	true
Commandline:	C:\Quotation.exe 0
Imagebase:	0x390000
File size:	207872 bytes
MD5 hash:	C83BD9093E7AE550FC49FDC1A90B7F9E
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.00000000.212196362.0000000000392000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.212196362.0000000000392000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.212196362.0000000000392000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.233036781.0000000002A11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.233036781.0000000002A11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.233182479.0000000003A11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.233182479.0000000003A11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.227002724.0000000000392000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.227002724.0000000000392000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.227002724.0000000000392000.00000002.00020000.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Quotation.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Quotation.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6656 Parent PID: 528

General

Start time:	13:12:04

Start date:	07/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x860000
File size:	207872 bytes
MD5 hash:	C83BD9093E7AE550FC49FDC1A90B7F9E
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: 0000000B.00000002.227835211.0000000000862000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.227835211.0000000000862000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.227835211.0000000000862000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.212881601.0000000000862000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.212881601.0000000000862000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.212881601.0000000000862000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.233656875.0000000003F81000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.233656875.0000000003F81000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.233269566.0000000002F81000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.233269566.0000000002F81000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 86%, Metadefender, Browse • Detection: 100%, ReversingLabs
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	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6872 Parent PID: 3388

General

Start time:	13:12:11
Start date:	07/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xaa0000
File size:	207872 bytes
MD5 hash:	C83BD9093E7AE550FC49FDC1A90B7F9E
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: 0000000C.00000000.230390276.0000000000AA2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.230390276.0000000000AA2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.230390276.0000000000AA2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.246968442.0000000004201000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.246968442.0000000004201000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.245771019.0000000000AA2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.245771019.0000000000AA2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.245771019.0000000000AA2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.246931446.0000000003201000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.246931446.0000000003201000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Disassembly

Code Analysis