ID: 339193
Sample Name: Invoice# 77-83992-8297382 (2).exe
Cookbook: default.jbs
Time: 17:08:28
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

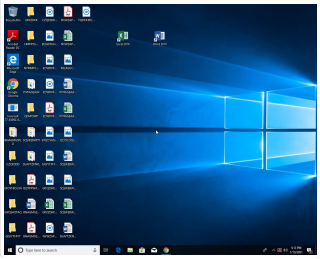
Analysis Report Invoice# 77-83992-8297382 (2).exe

Overview

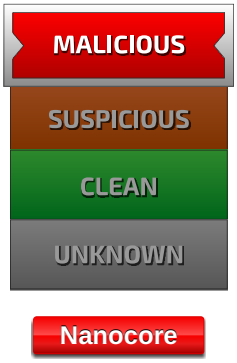
General Information

Sample Name:	Invoice# 77-83992-8297382 (2).exe
Analysis ID:	339193
MD5:	4c67eb7b3f4ea88.
SHA1:	d118ae4beef8907.
SHA256:	db433304c3e22d..
Tags:	exe NanoCore

Most interesting Screenshot:



Detection

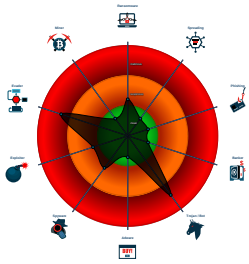


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Antivirus or Machine Learning detec…
- Contains functionality to launch a pr…
- Contains long sleeps (>= 3 min)

Classification



Startup

- **System is w10x64**
- Invoice# 77-83992-8297382 (2).exe (PID: 4120 cmdline: 'C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe' MD5: 4C67EB7B3F4EA88E5E5487ADE487DE3F)
  - Invoice# 77-83992-8297382 (2).exe (PID: 5800 cmdline: C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe MD5: 4C67EB7B3F4EA88E5E5487ADE487DE3F)
- dhcpmon.exe (PID: 1020 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 4C67EB7B3F4EA88E5E5487ADE487DE3F)
  - dhcpmon.exe (PID: 6228 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 4C67EB7B3F4EA88E5E5487ADE487DE3F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.619051050.000000000406 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.619051050.000000000406 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2ee5:$a: NanoCore • 0x2f3e:$a: NanoCore • 0x2f7b:$a: NanoCore • 0x2ff4:$a: NanoCore • 0x1669f:$a: NanoCore • 0x166b4:$a: NanoCore • 0x166e9:$a: NanoCore • 0x2f173:$a: NanoCore • 0x2f188:$a: NanoCore • 0x2f1bd:$a: NanoCore • 0x2f47:$b: ClientPlugin • 0x2f84:$b: ClientPlugin • 0x3882:$b: ClientPlugin • 0x388f:$b: ClientPlugin • 0x1645b:$b: ClientPlugin • 0x16476:$b: ClientPlugin • 0x164a6:$b: ClientPlugin • 0x166bd:$b: ClientPlugin • 0x166f2:$b: ClientPlugin • 0x2ef2f:$b: ClientPlugin • 0x2ef4a:$b: ClientPlugin
00000001.00000002.621166702.00000000059E 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000001.00000002.621166702.00000000059E 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000001.00000002.621166702.00000000059E 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Invoice# 77-83992-8297382 (2).exe.5730000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
1.2.Invoice# 77-83992-8297382 (2).exe.5730000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
1.2.Invoice# 77-83992-8297382 (2).exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
1.2.Invoice# 77-83992-8297382 (2).exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
1.2.Invoice# 77-83992-8297382 (2).exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 11 entries				

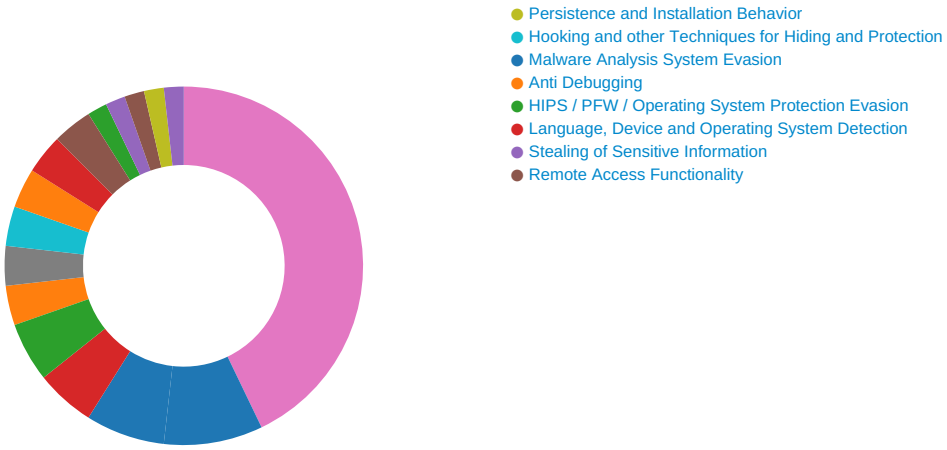
Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

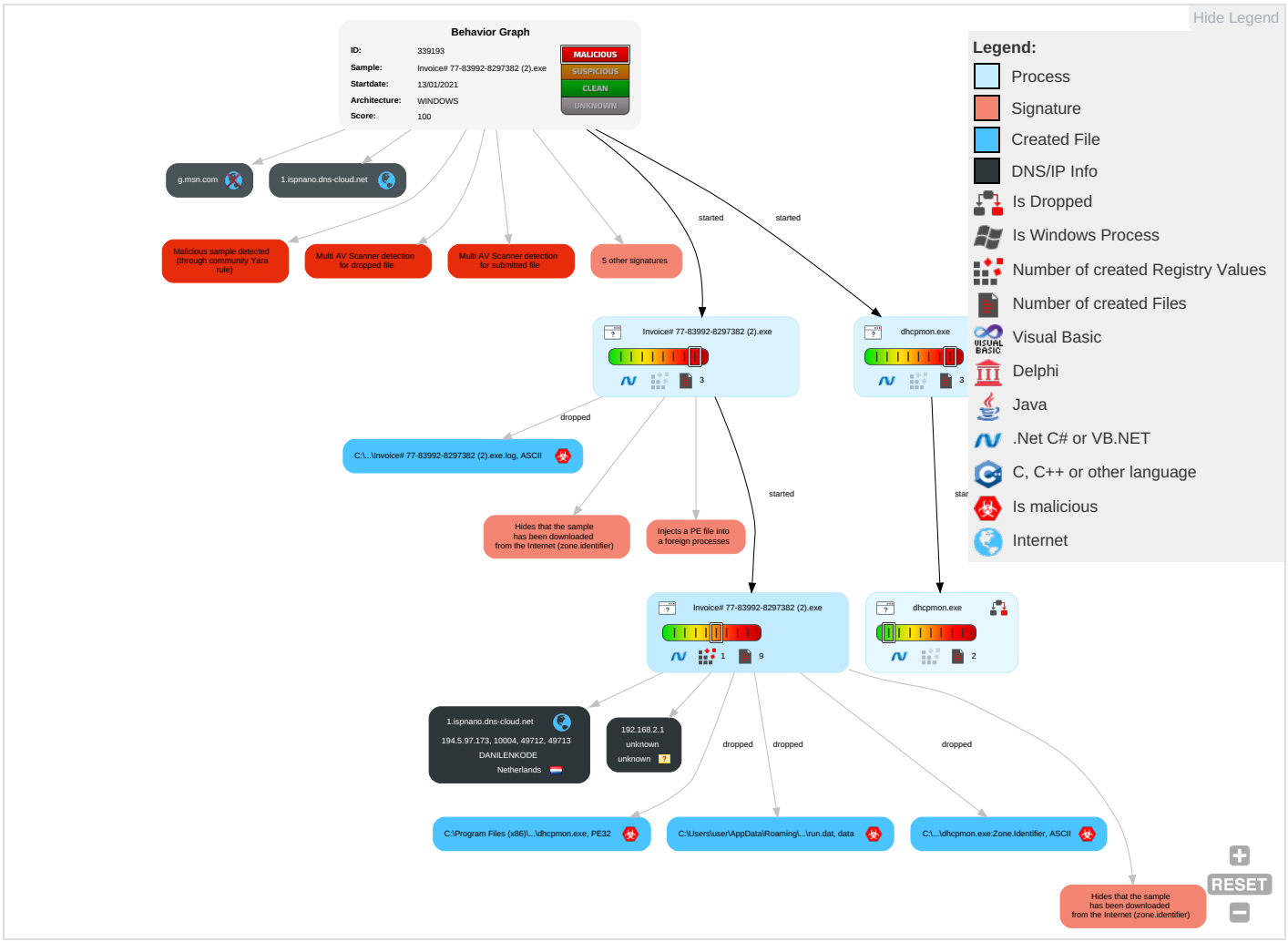
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation	Valid Accounts 1	Valid Accounts 1	Masquerading 2	Input Capture 1 1	Security Software Discovery 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-S Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remot Softwa
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Disable or Modify Tools 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Deobfuscate/Decode Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer I
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Obfuscated Files or Information 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Software Packing 1 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc

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
Invoice# 77-83992-8297382 (2).exe	26%	ReversingLabs	Win32.Trojan.Bulz	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	26%	ReversingLabs	Win32.Trojan.Bulz	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Invoice# 77-83992-8297382 (2).exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.Invoice# 77-83992-8297382 (2).exe.59e0000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://go.microsoft.c	0%	Avira URL Cloud	safe	
http://ns.ado/Ident	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
1.ispnano.dns-cloud.net	194.5.97.173	true	false		unknown
g.msn.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://go.microsoft.c	Invoice# 77-83992-8297382 (2).exe, 00000000.00000003.2338247 22.0000000001326000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.ado/Ident	Invoice# 77-83992-8297382 (2).exe, 00000000.00000002.2403390 78.00000000016E9000.00000004.0 0000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339193
Start date:	13.01.2021
Start time:	17:08:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice# 77-83992-8297382 (2).exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/5@39/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.5%) • Quality average: 76.8% • Quality standard deviation: 17.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 23.210.248.85, 51.104.146.109, 92.122.213.194, 92.122.213.247, 52.147.198.201, 52.255.188.83, 2.20.142.210, 2.20.142.209, 51.103.5.159, 20.54.26.129, 52.142.114.176, 51.11.168.160, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/339193/sample/Invoice# 77-83992-8297382 (2).exe

Simulations

Behavior and APIs

Time	Type	Description
17:09:35	API Interceptor	1468x Sleep call for process: Invoice# 77-83992-8297382 (2).exe modified
17:09:38	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.173	Invoice #756-77988-23989646.exe	Get hash	malicious	Browse	
	shipping order.exe	Get hash	malicious	Browse	
	shipping order#.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
1.ispnano.dns-cloud.net	shipping order.exe	Get hash	malicious	Browse	• 194.5.97.173
	shipping order#.exe	Get hash	malicious	Browse	• 194.5.97.173

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	PO-Scan-Documents00012910993993.exe	Get hash	malicious	Browse	• 194.5.97.155
	Wjhus order 13.1.2021.exe	Get hash	malicious	Browse	• 194.5.98.176
	Invoice #756-77988-23989646.exe	Get hash	malicious	Browse	• 194.5.97.173
	Quotation.exe	Get hash	malicious	Browse	• 194.5.98.200
	December SOA.exe	Get hash	malicious	Browse	• 194.5.97.66
	IMG-001GE-0HUE48E-001012-001.exe	Get hash	malicious	Browse	• 194.5.97.155
	shipping order.exe	Get hash	malicious	Browse	• 194.5.97.173
	shipping order#.exe	Get hash	malicious	Browse	• 194.5.97.173
	BL,IN&PL.exe	Get hash	malicious	Browse	• 194.5.97.206
	New PO.exe	Get hash	malicious	Browse	• 194.5.98.32
	Order Inquiry.exe	Get hash	malicious	Browse	• 194.5.97.235
	IMG 01-06-2021 93899283.exe	Get hash	malicious	Browse	• 194.5.97.177
	SWIFT345343445pdf.exe	Get hash	malicious	Browse	• 194.5.97.164
	DHL1.exe	Get hash	malicious	Browse	• 194.5.98.145
	Original BL_pdf.exe	Get hash	malicious	Browse	• 194.5.97.107
	AWB & CI_pdf.exe	Get hash	malicious	Browse	• 194.5.97.107
	File.exe	Get hash	malicious	Browse	• 194.5.98.108
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 194.5.98.215
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	849920
Entropy (8bit):	5.429435248347001
Encrypted:	false
SSDEEP:	12288:L0Fi3dg/zDNj6udDKlNCyPhf223d9ZSn9Vb:oi3dg/PNj/KlRbZSnb
MD5:	4C67EB7B3F4EA88E5E5487ADE487DE3F
SHA1:	D118AE4BEEF890783251D53F3F7FE5E6C9A65A10
SHA-256:	DB433304C3E22D8222CFE510E8548515C9DCCFC9F080F94EFC67AA11F44A6B3F
SHA-512:	37609EA4261FE4DADF403A05014DB11DEFAE9A65CEF8C5639A56166A379B1151EE48100F6726D8160AEFAD9C49EA6A5430E17526B87A41DC2366E6C23CE4759C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....7.....P..... ... .@.. .....`..... ..`.....O.... .....@..... ....H.....text...$.... ....`.rsrc..... .....@..@.reloc.....@ .....@..B.....H.....<*.....Z....E.....&..(.....*.s.....s.....s.....s .....*&.....*"..... *Vs ...(3...t.....*..(4...*..(....*N. .....(-....*V....(E.....(2....*^.~....(b.....(8....*v.~....~.....(C.....(<....*.....(R....*^.....(F...t....o`....*..(G...*....0..d.....0.....0.....0.....(!...t0.....0.....\.....0.....-0 .+..(!...t....&.....-...&.....+?.

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe
File Type:	ASCII text, with CRLF line terminators

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice# 77-83992-8297382 (2).exe.log	
Process:	C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895E ABB
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

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):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895E ABB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SSDEEP:	3:aYl:aQ
MD5:	49CFF363A29F80058C2F4C57C1021A70
SHA1:	A498CB7524C13C67F39E088417AEE9193645F6F0
SHA-256:	04941065834332F29ECCFACA73DD5BFA47DE6B7628E23F45C50EB229893210AD
SHA-512:	0E2FB71980BA615F463FB5FF6C6CCA2893912B0219F4B0497AA19A6D856155DAD0D3C5DC5B7808EEAE9545791C2656B633B978F583DA6E2AC2B1BCA331976C06
Malicious:	**true**
Reputation:	low
Preview:	.}..)..H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.429435248347001
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:	Invoice# 77-83992-8297382 (2).exe
File size:	849920
MD5:	4c67eb7b3f4ea88e5e5487ade487de3f
SHA1:	d118ae4beef890783251d53f3f7fe5e6c9a65a10
SHA256:	db433304c3e22d8222cfe510e8548515c9dccfc9f080f94efc67aa11f44a6b3f
SHA512:	37609ea4261fe4dadf403a05014db11defae9a65cef8c5639a56166a379b1151ee48100f6726d8160aefad9c49ea6a5430e17526b87a41dc2366e6c23ce4759c
SSDEEP:	12288:L0Fi3dg/zDNj6udDKlNCyPhf223d9ZSn9Vb:oi3dg/PNj/KlRbZSnb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....7.....P..... ... .@.. .....`.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d0c1e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x37DD8418 [Mon Sep 13 23:09:12 1999 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0

General

Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd0bcc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd2000	0x596	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcec24	0xcee00	False	0.490468041918	data	5.43331937316	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd2000	0x596	0x600	False	0.413411458333	data	4.05390274957	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd20a0	0x30c	data		
RT_MANIFEST	0xd23ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

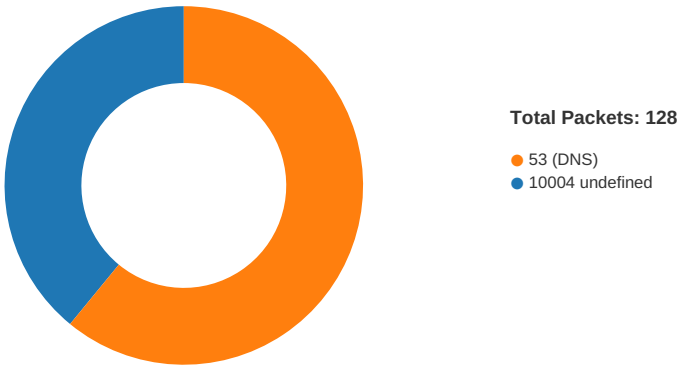
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	Stub52.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Stub52
ProductVersion	1.0.0.0
FileDescription	Stub52
OriginalFilename	Stub52.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:09:36.716850042 CET	49712	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:36.768384933 CET	10004	49712	194.5.97.173	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:09:37.277143955 CET	49712	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:37.326282978 CET	10004	49712	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:37.839719057 CET	49712	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:37.889018059 CET	10004	49712	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:43.399245024 CET	49713	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:43.448784113 CET	10004	49713	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:44.027650118 CET	49713	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:44.077121973 CET	10004	49713	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:44.637187958 CET	49713	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:44.686736107 CET	10004	49713	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:48.800421953 CET	49717	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:48.849715948 CET	10004	49717	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:49.528851986 CET	49717	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:49.578217983 CET	10004	49717	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:50.137547016 CET	49717	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:50.186742067 CET	10004	49717	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:54.329802036 CET	49720	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:54.379086018 CET	10004	49720	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:55.028629065 CET	49720	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:55.077912092 CET	10004	49720	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:55.638024092 CET	49720	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:55.688035011 CET	10004	49720	194.5.97.173	192.168.2.3
Jan 13, 2021 17:09:59.924818993 CET	49724	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:09:59.974153042 CET	10004	49724	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:00.540069103 CET	49724	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:00.589448929 CET	10004	49724	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:01.138472080 CET	49724	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:01.254395962 CET	10004	49724	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:05.364154100 CET	49728	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:05.414776087 CET	10004	49728	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:05.928263903 CET	49728	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:05.977524996 CET	10004	49728	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:06.530002117 CET	49728	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:06.579221010 CET	10004	49728	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:10.730393887 CET	49738	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:10.779676914 CET	10004	49738	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:11.279241085 CET	49738	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:11.328452110 CET	10004	49738	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:11.983228922 CET	49738	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:12.033037901 CET	10004	49738	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:16.135730982 CET	49749	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:16.184935093 CET	10004	49749	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:16.686604023 CET	49749	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:16.735814095 CET	10004	49749	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:17.374187946 CET	49749	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:17.423360109 CET	10004	49749	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:21.603288889 CET	49750	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:21.652797937 CET	10004	49750	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:22.187079906 CET	49750	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:22.236682892 CET	10004	49750	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:22.780889988 CET	49750	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:22.833842993 CET	10004	49750	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:26.931889057 CET	49753	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:26.981302977 CET	10004	49753	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:27.484529018 CET	49753	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:27.533932924 CET	10004	49753	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:28.046943903 CET	49753	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:28.096316099 CET	10004	49753	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:32.224612951 CET	49754	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:32.274112940 CET	10004	49754	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:32.781811953 CET	49754	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:32.831726074 CET	10004	49754	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:33.344243050 CET	49754	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:33.393853903 CET	10004	49754	194.5.97.173	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:10:37.569816113 CET	49755	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:37.619103909 CET	10004	49755	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:38.125946045 CET	49755	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:38.175285101 CET	10004	49755	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:38.688491106 CET	49755	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:38.737788916 CET	10004	49755	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:42.835010052 CET	49756	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:42.884427071 CET	10004	49756	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:43.392069101 CET	49756	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:43.460846901 CET	10004	49756	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:43.970176935 CET	49756	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:44.019666910 CET	10004	49756	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:48.126225948 CET	49757	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:48.175662994 CET	10004	49757	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:48.689410925 CET	49757	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:48.738691092 CET	10004	49757	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:49.252041101 CET	49757	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:49.301299095 CET	10004	49757	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:53.429653883 CET	49758	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:53.479063034 CET	10004	49758	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:53.989485025 CET	49758	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:54.038609982 CET	10004	49758	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:54.549243927 CET	49758	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:54.598433971 CET	10004	49758	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:58.731355906 CET	49759	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:58.780493975 CET	10004	49759	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:59.284090042 CET	49759	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:59.333575010 CET	10004	49759	194.5.97.173	192.168.2.3
Jan 13, 2021 17:10:59.846481085 CET	49759	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:10:59.895761967 CET	10004	49759	194.5.97.173	192.168.2.3
Jan 13, 2021 17:11:04.107656002 CET	49760	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:11:04.157145023 CET	10004	49760	194.5.97.173	192.168.2.3
Jan 13, 2021 17:11:04.659398079 CET	49760	10004	192.168.2.3	194.5.97.173
Jan 13, 2021 17:11:04.709103107 CET	10004	49760	194.5.97.173	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:09:28.497873068 CET	57544	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:28.545753002 CET	53	57544	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:30.097846985 CET	55984	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:30.148536921 CET	53	55984	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:36.633502007 CET	64185	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:36.703766108 CET	53	64185	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:43.339847088 CET	65110	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:43.396136045 CET	53	65110	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:47.129807949 CET	58361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:47.187757015 CET	53	58361	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:48.737692118 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:48.799089909 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:49.170738935 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:49.221443892 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:54.257950068 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:54.327219009 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:57.605323076 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:57.665364027 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:58.054920912 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:58.105823994 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:58.906404972 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:58.954344034 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 17:09:59.875073910 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:09:59.922853947 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:01.104103088 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:01.154850006 CET	53	51352	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:10:04.195559025 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:04.251647949 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:05.037314892 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:05.085202932 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:05.305628061 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:05.362389088 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:05.939368010 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:05.987246990 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:06.753321886 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:06.804006100 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:07.158162117 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:07.216087103 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:07.363090038 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:07.420190096 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:07.619266987 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:07.667121887 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:08.528155088 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:08.578916073 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:08.703545094 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:08.762765884 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:09.439726114 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:09.490441084 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:10.292624950 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:10.340560913 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:10.680809975 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:10.728758097 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:11.144009113 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:11.191858053 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:11.978118896 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:12.027245045 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:13.100095987 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:13.147995949 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:13.912931919 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:13.960949898 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:14.609074116 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:14.669406891 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:14.829952002 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:14.877903938 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:16.075653076 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:16.134773016 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:21.541862011 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:21.602304935 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:23.246170044 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:23.294035912 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:26.182544947 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:26.246912003 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:26.873873949 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:26.930425882 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:32.166691065 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:32.223047972 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:37.515794039 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:37.566517115 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:42.785608053 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:42.833533049 CET	53	55708	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:48.068613052 CET	56803	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:48.124769926 CET	53	56803	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:53.342681885 CET	57145	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:53.399116993 CET	53	57145	8.8.8.8	192.168.2.3
Jan 13, 2021 17:10:58.670852900 CET	55359	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:10:58.729885101 CET	53	55359	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:04.047702074 CET	58306	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:04.105832100 CET	53	58306	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:11.220237970 CET	64124	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:11.268183947 CET	53	64124	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:11:12.391298056 CET	49361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:12.441092014 CET	53	49361	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:16.535574913 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:16.591797113 CET	53	63150	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:21.867281914 CET	53279	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:21.917999029 CET	53	53279	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:27.144418955 CET	56881	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:27.200948954 CET	53	56881	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:32.449100018 CET	53642	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:32.505148888 CET	53	53642	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:37.825323105 CET	55667	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:37.884396076 CET	53	55667	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:43.098982096 CET	54833	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:43.155555964 CET	53	54833	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:47.840683937 CET	62476	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:47.889309883 CET	53	62476	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:48.292572975 CET	49705	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:48.363360882 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:48.474570036 CET	61477	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:48.533888102 CET	53	61477	8.8.8.8	192.168.2.3
Jan 13, 2021 17:11:53.790071011 CET	61633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:11:53.846435070 CET	53	61633	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:01.194253922 CET	55949	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:01.253833055 CET	53	55949	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:05.255992889 CET	57601	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:05.306658983 CET	53	57601	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:06.062604904 CET	49342	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:06.135001898 CET	53	49342	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:06.609291077 CET	56253	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:06.668634892 CET	53	56253	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:07.035053015 CET	49667	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:07.091231108 CET	53	49667	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:07.822472095 CET	55439	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:07.878669977 CET	53	55439	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:08.999607086 CET	57069	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:09.071839094 CET	53	57069	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:09.929860115 CET	57659	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:09.986413956 CET	53	57659	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:11.465353012 CET	54717	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:11.513204098 CET	53	54717	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:11.913475037 CET	63975	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:11.969543934 CET	53	63975	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:13.596380949 CET	56639	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:13.655941963 CET	53	56639	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:14.919383049 CET	51856	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:14.975591898 CET	53	51856	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:16.517098904 CET	56546	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:16.576900005 CET	53	56546	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:17.317095041 CET	62152	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:17.379125118 CET	53	62152	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:22.594510078 CET	53470	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:22.650772095 CET	53	53470	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:27.921185970 CET	56446	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:27.977909088 CET	53	56446	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:33.220309019 CET	59631	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:33.277091980 CET	53	59631	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:38.455576897 CET	55515	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:38.512006044 CET	53	55515	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:43.689896107 CET	64547	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:43.746169090 CET	53	64547	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:48.924525023 CET	51759	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:48.984445095 CET	53	51759	8.8.8.8	192.168.2.3
Jan 13, 2021 17:12:54.175184011 CET	59207	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:54.234867096 CET	53	59207	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:12:59.425617933 CET	54269	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:12:59.484936953 CET	53	54269	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:09:36.633502007 CET	192.168.2.3	8.8.8.8	0x8d2b	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:43.339847088 CET	192.168.2.3	8.8.8.8	0xb451	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:48.737692118 CET	192.168.2.3	8.8.8.8	0x9a1d	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:54.257950068 CET	192.168.2.3	8.8.8.8	0xa401	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:59.875073910 CET	192.168.2.3	8.8.8.8	0x4d12	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:05.305628061 CET	192.168.2.3	8.8.8.8	0x31b8	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:10.680809975 CET	192.168.2.3	8.8.8.8	0x731b	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:16.075653076 CET	192.168.2.3	8.8.8.8	0xdb7c	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:21.541862011 CET	192.168.2.3	8.8.8.8	0xed52	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:26.182544947 CET	192.168.2.3	8.8.8.8	0xd7bd	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:26.873873949 CET	192.168.2.3	8.8.8.8	0xeab	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:32.166691065 CET	192.168.2.3	8.8.8.8	0x24d2	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:37.515794039 CET	192.168.2.3	8.8.8.8	0x9f9d	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:42.785608053 CET	192.168.2.3	8.8.8.8	0xe9b8	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:48.068613052 CET	192.168.2.3	8.8.8.8	0xc501	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:53.342681885 CET	192.168.2.3	8.8.8.8	0xbada	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:58.670852900 CET	192.168.2.3	8.8.8.8	0x9107	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:04.047702074 CET	192.168.2.3	8.8.8.8	0x1e09	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:11.220237970 CET	192.168.2.3	8.8.8.8	0x395e	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:16.535574913 CET	192.168.2.3	8.8.8.8	0x252c	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:21.867281914 CET	192.168.2.3	8.8.8.8	0xb9bc	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:27.144418955 CET	192.168.2.3	8.8.8.8	0xdab8	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:32.449100018 CET	192.168.2.3	8.8.8.8	0x8966	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:37.825323105 CET	192.168.2.3	8.8.8.8	0x63a5	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:43.098982096 CET	192.168.2.3	8.8.8.8	0x10f8	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:48.474570036 CET	192.168.2.3	8.8.8.8	0x6fc2	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:53.790071011 CET	192.168.2.3	8.8.8.8	0x5cd2	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:01.194253922 CET	192.168.2.3	8.8.8.8	0x25c7	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:06.609291077 CET	192.168.2.3	8.8.8.8	0x264f	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:11.913475037 CET	192.168.2.3	8.8.8.8	0x1e99	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:17.317095041 CET	192.168.2.3	8.8.8.8	0x7030	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:22.594510078 CET	192.168.2.3	8.8.8.8	0x8006	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:27.921185970 CET	192.168.2.3	8.8.8.8	0xb879	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:33.220309019 CET	192.168.2.3	8.8.8.8	0xf2bb	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:12:38.455576897 CET	192.168.2.3	8.8.8.8	0x6341	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:43.689896107 CET	192.168.2.3	8.8.8.8	0xc6af	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:48.924525023 CET	192.168.2.3	8.8.8.8	0xf39f	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:54.175184011 CET	192.168.2.3	8.8.8.8	0xf665	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:59.425617933 CET	192.168.2.3	8.8.8.8	0x7a69	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:09:36.703766108 CET	8.8.8.8	192.168.2.3	0x8d2b	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:36.703766108 CET	8.8.8.8	192.168.2.3	0x8d2b	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:43.396136045 CET	8.8.8.8	192.168.2.3	0xb451	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:43.396136045 CET	8.8.8.8	192.168.2.3	0xb451	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:48.799089909 CET	8.8.8.8	192.168.2.3	0x9a1d	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:48.799089909 CET	8.8.8.8	192.168.2.3	0x9a1d	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:54.327219009 CET	8.8.8.8	192.168.2.3	0xa401	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:54.327219009 CET	8.8.8.8	192.168.2.3	0xa401	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:59.922853947 CET	8.8.8.8	192.168.2.3	0x4d12	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:09:59.922853947 CET	8.8.8.8	192.168.2.3	0x4d12	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:05.362389088 CET	8.8.8.8	192.168.2.3	0x31b8	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:05.362389088 CET	8.8.8.8	192.168.2.3	0x31b8	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:10.728758097 CET	8.8.8.8	192.168.2.3	0x731b	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:10.728758097 CET	8.8.8.8	192.168.2.3	0x731b	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:16.134773016 CET	8.8.8.8	192.168.2.3	0xdb7c	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:16.134773016 CET	8.8.8.8	192.168.2.3	0xdb7c	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:21.602304935 CET	8.8.8.8	192.168.2.3	0xed52	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:21.602304935 CET	8.8.8.8	192.168.2.3	0xed52	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:26.246912003 CET	8.8.8.8	192.168.2.3	0xd7bd	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:10:26.930425882 CET	8.8.8.8	192.168.2.3	0xeab	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:26.930425882 CET	8.8.8.8	192.168.2.3	0xeab	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:10:32.223047972 CET	8.8.8.8	192.168.2.3	0x24d2	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:32.223047972 CET	8.8.8.8	192.168.2.3	0x24d2	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:37.566517115 CET	8.8.8.8	192.168.2.3	0x9f9d	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:37.566517115 CET	8.8.8.8	192.168.2.3	0x9f9d	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:42.833533049 CET	8.8.8.8	192.168.2.3	0xe9b8	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:42.833533049 CET	8.8.8.8	192.168.2.3	0xe9b8	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:48.124769926 CET	8.8.8.8	192.168.2.3	0xc501	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:48.124769926 CET	8.8.8.8	192.168.2.3	0xc501	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:53.399116993 CET	8.8.8.8	192.168.2.3	0xbada	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:53.399116993 CET	8.8.8.8	192.168.2.3	0xbada	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:58.729885101 CET	8.8.8.8	192.168.2.3	0x9107	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:10:58.729885101 CET	8.8.8.8	192.168.2.3	0x9107	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:04.105832100 CET	8.8.8.8	192.168.2.3	0x1e09	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:04.105832100 CET	8.8.8.8	192.168.2.3	0x1e09	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:11.268183947 CET	8.8.8.8	192.168.2.3	0x395e	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:11.268183947 CET	8.8.8.8	192.168.2.3	0x395e	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:16.591797113 CET	8.8.8.8	192.168.2.3	0x252c	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:16.591797113 CET	8.8.8.8	192.168.2.3	0x252c	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:21.917999029 CET	8.8.8.8	192.168.2.3	0xb9bc	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:21.917999029 CET	8.8.8.8	192.168.2.3	0xb9bc	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:27.200948954 CET	8.8.8.8	192.168.2.3	0xdab8	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:27.200948954 CET	8.8.8.8	192.168.2.3	0xdab8	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:32.505148888 CET	8.8.8.8	192.168.2.3	0x8966	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:32.505148888 CET	8.8.8.8	192.168.2.3	0x8966	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:37.884396076 CET	8.8.8.8	192.168.2.3	0x63a5	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:37.884396076 CET	8.8.8.8	192.168.2.3	0x63a5	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)

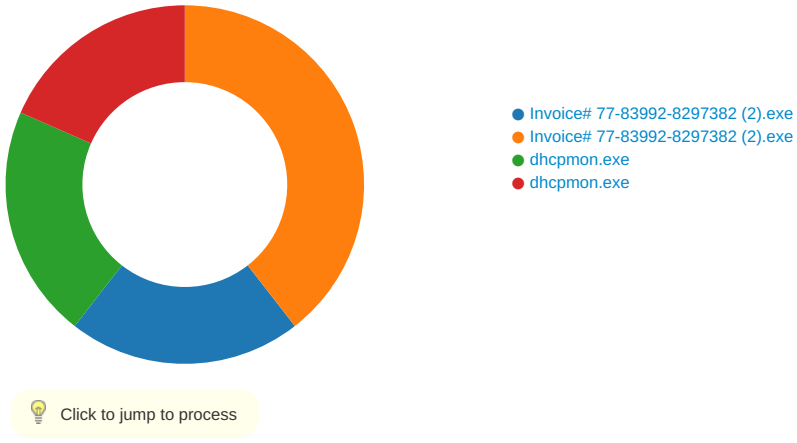
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:11:43.155555964 CET	8.8.8.8	192.168.2.3	0x10f8	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:43.155555964 CET	8.8.8.8	192.168.2.3	0x10f8	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:48.533888102 CET	8.8.8.8	192.168.2.3	0x6fc2	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:48.533888102 CET	8.8.8.8	192.168.2.3	0x6fc2	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:53.846435070 CET	8.8.8.8	192.168.2.3	0x5cd2	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:11:53.846435070 CET	8.8.8.8	192.168.2.3	0x5cd2	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:01.253833055 CET	8.8.8.8	192.168.2.3	0x25c7	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:01.253833055 CET	8.8.8.8	192.168.2.3	0x25c7	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:06.668634892 CET	8.8.8.8	192.168.2.3	0x264f	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:06.668634892 CET	8.8.8.8	192.168.2.3	0x264f	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:11.969543934 CET	8.8.8.8	192.168.2.3	0x1e99	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:11.969543934 CET	8.8.8.8	192.168.2.3	0x1e99	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:17.379125118 CET	8.8.8.8	192.168.2.3	0x7030	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:17.379125118 CET	8.8.8.8	192.168.2.3	0x7030	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:22.650772095 CET	8.8.8.8	192.168.2.3	0x8006	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:22.650772095 CET	8.8.8.8	192.168.2.3	0x8006	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:27.977909088 CET	8.8.8.8	192.168.2.3	0xb879	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:27.977909088 CET	8.8.8.8	192.168.2.3	0xb879	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:33.277091980 CET	8.8.8.8	192.168.2.3	0xf2bb	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:33.277091980 CET	8.8.8.8	192.168.2.3	0xf2bb	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:38.512006044 CET	8.8.8.8	192.168.2.3	0x6341	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:38.512006044 CET	8.8.8.8	192.168.2.3	0x6341	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:43.746169090 CET	8.8.8.8	192.168.2.3	0xc6af	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:43.746169090 CET	8.8.8.8	192.168.2.3	0xc6af	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:48.984445095 CET	8.8.8.8	192.168.2.3	0xf39f	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:48.984445095 CET	8.8.8.8	192.168.2.3	0xf39f	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:12:54.234867096 CET	8.8.8.8	192.168.2.3	0xf665	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:54.234867096 CET	8.8.8.8	192.168.2.3	0xf665	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:59.484936953 CET	8.8.8.8	192.168.2.3	0x7a69	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 13, 2021 17:12:59.484936953 CET	8.8.8.8	192.168.2.3	0x7a69	No error (0)	1.ispnano.dns-cloud.net		23.105.131.188	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Invoice# 77-83992-8297382 (2).exe PID: 4120 Parent PID: 5732

General

Start time:	17:09:23
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe'
Imagebase:	0xc30000
File size:	849920 bytes
MD5 hash:	4C67EB7B3F4EA88E5E5487ADE487DE3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.244571473.0000000004A9F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.244571473.0000000004A9F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.244571473.0000000004A9F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.243948615.0000000004909000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.243948615.0000000004909000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.243948615.0000000004909000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.243390482.0000000003FC1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.243390482.0000000003FC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.243390482.0000000003FC1000.00000004.00000001.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	6DF4CF06	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	6DF4CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice# 77-83992-8297382 (2).exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice# 77-83992-8297382 (2).exe.log	unknown	1451	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 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 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"PresentationCore, Version=	success or wait	1	6E25C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF25705	unknown

Analysis Process: Invoice# 77-83992-8297382 (2).exe PID: 5800 Parent PID: 4120

General

Start time:	17:09:29
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe
Imagebase:	0xca0000
File size:	849920 bytes

MD5 hash:	4C67EB7B3F4EA88E5E5487ADE487DE3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.619051050.0000000004069000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.619051050.0000000004069000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.621166702.00000000059E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.621166702.00000000059E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.621166702.00000000059E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.613044676.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.613044676.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.613044676.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.616036115.0000000003021000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.620857692.0000000005730000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.620857692.0000000005730000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF4CF06	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	6DF4CF06	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	6CD9BEFF	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	6CD91E60	CreateFileW
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	6CD9BEFF	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	6CD9DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identi fier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD9DD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5 F57B9A\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	6CD9BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5 F57B9A\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	6CD9BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe:Zone.Identifier	success or wait	1	6CD12935	unknown

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	18 7d 94 0e 29 b8 d8 48	.}..)..H	success or wait	1	6CD91B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 18 84 dd 37 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 ee 0c 00 00 08 00 00 00 00 00 00 1e 0c 0d 00 00 20 00 00 00 20 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 0d 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......7.......... ....P................. ... .@.. ....` ...........`................	success or wait	4	6CD9DD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CD9DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE803DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD91B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DF0D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DF0D72F	unknown
C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe	unknown	4096	success or wait	1	6DF0D72F	unknown
C:\Users\user\Desktop\Invoice# 77-83992-8297382 (2).exe	unknown	512	success or wait	1	6DF0D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WO W6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe	success or wait	1	6CD9646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 1020 Parent PID: 3388

General

Start time:	17:09:47
Start date:	13/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x420000
File size:	849920 bytes
MD5 hash:	4C67EB7B3F4EA88E5E5487ADE487DE3F
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: 00000004.00000002.300827633.00000000044AF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.300827633.00000000044AF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.300827633.00000000044AF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.296404991.00000000039D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.296404991.00000000039D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.296404991.00000000039D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.297386701.0000000004319000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.297386701.0000000004319000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.297386701.0000000004319000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 26%, 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	6DF4CF06	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	6DF4CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1451	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 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 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"PresentationCore, Version=	success or wait	1	6E25C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF25705	unknown

Analysis Process: dhcpmon.exe PID: 6228 Parent PID: 1020

General

Start time:	17:09:52
Start date:	13/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x810000
File size:	849920 bytes

MD5 hash:	4C67EB7B3F4EA88E5E5487ADE487DE3F
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: 00000007.00000002.307110365.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.307110365.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.307110365.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.308355679.0000000003C49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.308355679.0000000003C49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.308252762.0000000002C41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.308252762.0000000002C41000.00000004.00000001.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	6DF4CF06	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	6DF4CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD91B4F	ReadFile

Disassembly

Code Analysis