ID: 412548
Sample Name:
Quotation_Order.pdf.exe
Cookbook: default.jbs
Time: 19:08:39
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

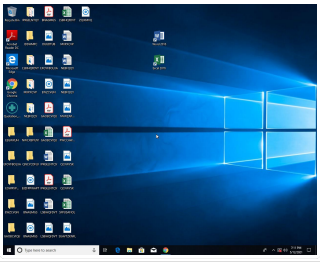
Analysis Report Quotation_Order.pdf.exe

Overview

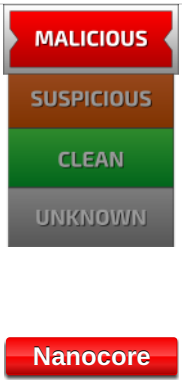
General Information

Sample Name:	Quotation_Order.pdf.exe
Analysis ID:	412548
MD5:	9ec5d09c8adefbf..
SHA1:	f296a55c93796fa..
SHA256:	53e8a1a34cdfdd3.
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection



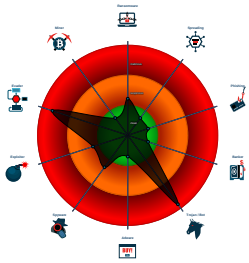
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- Quotation_Order.pdf.exe (PID: 3632 cmdline: 'C:\Users\user\Desktop\Quotation_Order.pdf.exe' MD5: 9EC5D09C8ADEFBF30598A5BD5F8D826E)
  - schtasks.exe (PID: 4728 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NzjsARuyfeoDS' /XML 'C:\Users\user\AppData\Local\Temp\tmpAE98.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 5016 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6f656d69-7475-8807-1300-000c0a4c",
  "Domain1": "185.140.53.138",
  "Domain2": "wealth2021.ddns.net",
  "Port": 20221,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.505268694.00000000056C0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000005.00000002.505268694.00000000056C0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000005.00000002.505644430.00000000058D0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000005.00000002.505644430.00000000058D0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000005.00000002.505644430.00000000058D0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.MSBuild.exe.41eff7c.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
5.2.MSBuild.exe.41eff7c.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
5.2.MSBuild.exe.41eff7c.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
5.2.MSBuild.exe.58d0000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
5.2.MSBuild.exe.58d0000.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
Click to see the 34 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Possible Applocker Bypass

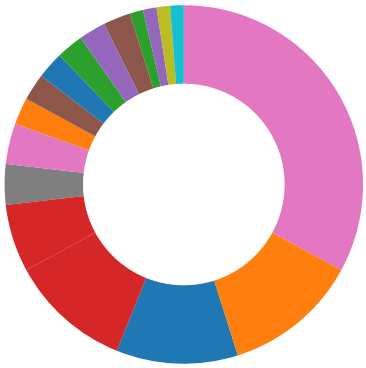
Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

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)

Initial sample is a PE file and has a suspicious name

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:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

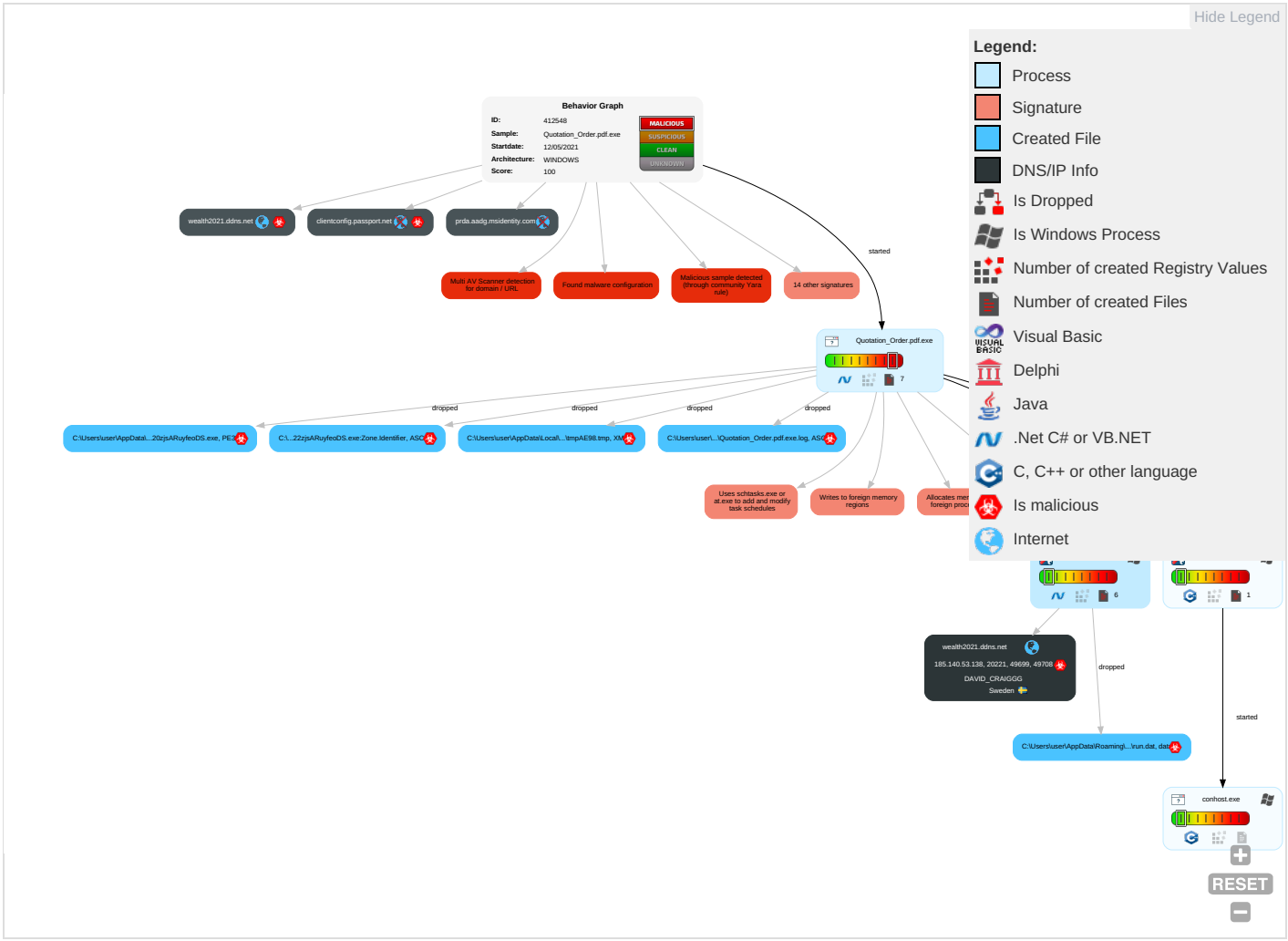
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Process Injection 3 1 2	Masquerading 1 1	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 2	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 2	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Quotation_Order.pdf.exe	26%	ReversingLabs	Win32.Trojan.AgentTesla	
Quotation_Order.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NzjsARuyfeoDS.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\NzjsARuyfeoDS.exe	26%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.MSBuild.exe.58d0000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
wealth2021.ddns.net	7%	Virustotal		Browse
clientconfig.passport.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
wealth2021.ddns.net	7%	Virustotal		Browse
wealth2021.ddns.net	0%	Avira URL Cloud	safe	
185.140.53.138	8%	Virustotal		Browse
185.140.53.138	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealth2021.ddns.net	185.140.53.138	true	true	• 7%, Virustotal, Browse	unknown
clientconfig.passport.net	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
wealth2021.ddns.net	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
185.140.53.138	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Quotation_Order.pdf.exe, 00000001.00000002.242066967.0000000002EB1000.00000004.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Quotation_Order.pdf.exe, 00000001.00000002.242066967.0000000002EB1000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.138	wealth2021.ddns.net	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412548
Start date:	12.05.2021
Start time:	19:08:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation_Order.pdf.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:	31
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@13/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 39% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • 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 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 92.123.150.225, 20.190.160.75, 20.190.160.4, 20.190.160.8, 20.190.160.129, 20.190.160.134, 20.190.160.2, 20.190.160.132, 20.190.160.73, 13.88.21.125, 131.253.33.200, 13.107.22.200, 20.50.102.62, 104.43.193.48, 92.122.145.220, 184.30.24.56, 20.82.210.154, 2.20.143.16, 2.20.142.209, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, msagfx.live.com-6.edgekey.net, e12564.dspb.akamaiedge.net, authgfx.msa.akadns6.net, go.microsoft.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.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, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, www.tm.a.prd.aadg.akadns.net, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:09:31	API Interceptor	2x Sleep call for process: Quotation_Order.pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.138	New_Order.pdf.exe	Get hash	malicious	Browse	
	New_Quotation_Request.pdf.exe	Get hash	malicious	Browse	
	QUOTATION_ORDER.pdf.exe	Get hash	malicious	Browse	
	URGENTPURCHASEORDER.pdf.exe	Get hash	malicious	Browse	
	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	
	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	
	Quotation_Request.pdf.exe	Get hash	malicious	Browse	
	URGENT_ORDER.pdf.exe	Get hash	malicious	Browse	
	Purchase_Order.pdf.exe	Get hash	malicious	Browse	
	1PH37n4Gva.exe	Get hash	malicious	Browse	
	35dbds3GQG.exe	Get hash	malicious	Browse	
	QXJGE2LOdP.exe	Get hash	malicious	Browse	
	O4m3hDFNbh.exe	Get hash	malicious	Browse	
	nrv_remittance#U007eorder#U007epayment.exe	Get hash	malicious	Browse	
	NEW ORDER REQUEST_EXPORT005JKL DOC.exe	Get hash	malicious	Browse	
	WIRE COPY ORDER T104484_PP.exe	Get hash	malicious	Browse	
	71AXBkD1wA.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wealth2021.ddns.net	New_Order.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	New_Quotation_Request.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	QUOTATION_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	URGENTPURCHASEORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	Quotation_Request.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	URGENT_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	Purchase_Order.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	New_Order.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	PaymentConfirmation.exe	Get hash	malicious	Browse	• 185.140.53.71
	Document - Banca Transilvania .exe	Get hash	malicious	Browse	• 185.140.53.73
	ATTACHED DRAWING AND SPECIFICATION.jar	Get hash	malicious	Browse	• 185.244.30.4
	ATTACHED DRAWING AND SPECIFICATION.jar	Get hash	malicious	Browse	• 185.244.30.4
	PO.98504_samples.exe	Get hash	malicious	Browse	• 185.140.53.69
	cotizaci#U00f3n.PDF.exe	Get hash	malicious	Browse	• 185.140.53.137
	Order Sheet.exe	Get hash	malicious	Browse	• 185.140.53.139
	EU_SANCTION_LETTER-05052021.exe	Get hash	malicious	Browse	• 185.140.53.230
	purchase order 0234.exe	Get hash	malicious	Browse	• 185.140.53.143
	ORDER-210067.xls.exe	Get hash	malicious	Browse	• 185.165.153.116
	03_pgr.exe	Get hash	malicious	Browse	• 185.140.53.71
	02_tmp.exe	Get hash	malicious	Browse	• 185.140.53.71
	03_pgr.exe	Get hash	malicious	Browse	• 185.140.53.71
	12_tmp.exe	Get hash	malicious	Browse	• 185.140.53.71
	13_pgr.exe	Get hash	malicious	Browse	• 185.140.53.71
	02_tmp.exe	Get hash	malicious	Browse	• 185.140.53.71
	12_pgr.exe	Get hash	malicious	Browse	• 185.140.53.71
	11_tmp.exe	Get hash	malicious	Browse	• 185.140.53.71
	doc_07621DERG7011220213300.exe	Get hash	malicious	Browse	• 185.140.53.230

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation_Order.pdf.exe.log	
Process:	C:\Users\user\Desktop\Quotation_Order.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpAE98.tmp	
Process:	C:\Users\user\Desktop\Quotation_Order.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.177749092284426
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBadItn:cbhH7MlNQ8/rydbz9l3YODOLNdq35
MD5:	E660135146E8CB0D32A8D919D3E5EDFB
SHA1:	C926BAB73227531FCC10FC858EEEA95C2E8F5919
SHA-256:	8ABE6F5D752965C7580F731D6B8913D0411CC11AEA384DF0129E0BD00A6D7B38
SHA-512:	E08C424B67F986918BEDA54E6405C2856CAE743BA1AED87BF355A18957289522591EBB4C22FA1D1AAF610A3D86293F4ECBCE6B08573C5433CD22A3BC7154D41F
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Zpn:7n
MD5:	8B98AB5B5A654BFA8F76362BCD7CF769
SHA1:	F96F39798591F166592E2FC6C9F763EE8AA76C0C
SHA-256:	BB6F884AF6AC368C3CD908AB97CB53B1EDDFE5C38867792A648F93C43D63A2E5
SHA-512:	6FF9761941D6A72BBC25DF41CF4C96F18CC340ACCF9AC50255DEADBB86EB34A8721BF201AB32AA30B46A86FB6CB7A8AE791FE025337E29FDEF23957076414DC6
Malicious:	**true**
Reputation:	low
Preview:	f..(...H

C:\Users\user\AppData\Roaming\NzjsARuyfeoDS.exe	
Process:	C:\Users\user\Desktop\Quotation_Order.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	845312
Entropy (8bit):	7.315929774120675
Encrypted:	false
SSDEEP:	12288:QTVyrD6tJgrDw4bS48LUT6CNVMwZiCckGqE7221yX87Nw6yhVphotxVgxL7s:QjE8LMhzVMPkGhJzJJgphotxVg5s
MD5:	9EC5D09C8ADEFBF30598A5BD5F8D826E
SHA1:	F296A55C93796FA015FB4B071122435062CC995D
SHA-256:	53E8A1A34CDFDD3E81842A5211699596CC2DA10EF2A94554D330F99B749A214E
SHA-512:	2BD331E31A62C443EF655F995B5262DD7BA587011E92B48AEC9F005215A10A58CBCE628B348C3F09EC911DCA8A1F60868515BB154F4F6AD18FFE3178C0284A6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...a.`.....P..6.....T... ...`....@.. .....@.....@.....S..O...`..t..... ..... ..H.....text....4... ...6..... ..`.rsrc...t...`.....8.....@..@.reloc.....@..B.....S.....H.....q.....0.....(...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(....oS...((. ...*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<.....~.....(4 .....,!r...p.....(5...o6...s7.....~.....+..*.0.....

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.315929774120675
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Quotation_Order.pdf.exe
File size:	845312
MD5:	9ec5d09c8adefbf30598a5bd5f8d826e
SHA1:	f296a55c93796fa015fb4b071122435062cc995d
SHA256:	53e8a1a34cdfdd3e81842a5211699596cc2da10ef2a9455 4d330f99b749a214e
SHA512:	2bd331e31a62c443ef655f995b5262dd7ba587011e92b48 aec9f005215a10a58cbce628b348c3f09ec911dca8a1f60 868515bb154f4f6ad18ffe3178c0284a67
SSDEEP:	12288:QTVyrD6tJgrDw4bS48LUT6CNVMwZiCckGqE72 21yX87Nw6yhVphotxVgxL7s:QjE8LMhzVMPkGhJzJJg photxVg5s

General

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...a..`..............P..6...........T... ...`....@.. ....@............@................................

File Icon

Icon Hash:	cc92316d713396e8

Static PE Info

General

Entrypoint:	0x4b540a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609BE761 [Wed May 12 14:34:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb53b8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x1ab74	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd2000	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	0xb3410	0xb3600	False	0.809437608885	data	7.64683515737	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x1ab74	0x1ac00	False	0.146082797897	data	3.15210936606	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb6220	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xb6688	0x162a	PNG image data, 256 x 256, 8-bit colormap, non-interlaced		
RT_ICON	0xb7cb4	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xba25c	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xbb304	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xcbb2c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xcfd54	0x5a	data		
RT_VERSION	0xcfdb0	0x394	data		
RT_MANIFEST	0xd0144	0xa2e	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

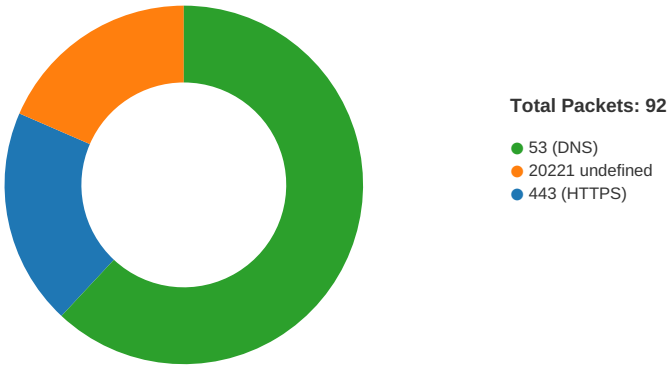
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	EnvironmentVariableTarget.exe

Description	Data
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	LibraryManagementSystem
ProductVersion	1.0.0.0
FileDescription	LibraryManagementSystem
OriginalFilename	EnvironmentVariableTarget.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:09:22.846283913 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846308947 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846324921 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846340895 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846357107 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846373081 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846389055 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846407890 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846426010 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846441984 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846457958 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846473932 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846488953 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846502066 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:22.846523046 CEST	49683	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:22.846616983 CEST	49683	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:22.998435020 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:22.998537064 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:23.059084892 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.059104919 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481117010 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481146097 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481164932 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481180906 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481197119 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481236935 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481252909 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481259108 CEST	49677	443	192.168.2.7	40.126.31.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:09:23.481268883 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481287003 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.481364012 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:23.517539978 CEST	49683	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:23.517594099 CEST	49683	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:23.578279018 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.578300953 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725044012 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725066900 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725083113 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725100040 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725116014 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725131035 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725147009 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725167036 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725186110 CEST	443	49683	40.126.31.4	192.168.2.7
May 12, 2021 19:09:23.725208998 CEST	49683	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:23.725244999 CEST	49683	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:23.777213097 CEST	49683	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:25.063285112 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:25.063342094 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:25.123919010 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.123980999 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.175136089 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280019045 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280054092 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280073881 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280092001 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280133009 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:25.280145884 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280165911 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:25.280169010 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280189037 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280217886 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:25.280247927 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280266047 CEST	443	49677	40.126.31.4	192.168.2.7
May 12, 2021 19:09:25.280294895 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:25.324054956 CEST	49677	443	192.168.2.7	40.126.31.4
May 12, 2021 19:09:38.171716928 CEST	49699	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:38.220172882 CEST	20221	49699	185.140.53.138	192.168.2.7
May 12, 2021 19:09:38.778301001 CEST	49699	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:38.826742887 CEST	20221	49699	185.140.53.138	192.168.2.7
May 12, 2021 19:09:39.481555939 CEST	49699	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:39.529968977 CEST	20221	49699	185.140.53.138	192.168.2.7
May 12, 2021 19:09:43.640548944 CEST	49708	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:43.690107107 CEST	20221	49708	185.140.53.138	192.168.2.7
May 12, 2021 19:09:44.278798103 CEST	49708	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:44.328593969 CEST	20221	49708	185.140.53.138	192.168.2.7
May 12, 2021 19:09:44.966310024 CEST	49708	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:45.014808893 CEST	20221	49708	185.140.53.138	192.168.2.7
May 12, 2021 19:09:49.045957088 CEST	49714	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:49.094362974 CEST	20221	49714	185.140.53.138	192.168.2.7
May 12, 2021 19:09:49.669847012 CEST	49714	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:49.718348980 CEST	20221	49714	185.140.53.138	192.168.2.7
May 12, 2021 19:09:50.279330969 CEST	49714	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:50.328071117 CEST	20221	49714	185.140.53.138	192.168.2.7
May 12, 2021 19:09:54.511395931 CEST	49720	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:54.560018063 CEST	20221	49720	185.140.53.138	192.168.2.7
May 12, 2021 19:09:55.076503038 CEST	49720	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:55.126526117 CEST	20221	49720	185.140.53.138	192.168.2.7
May 12, 2021 19:09:55.779757023 CEST	49720	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:55.828063011 CEST	20221	49720	185.140.53.138	192.168.2.7
May 12, 2021 19:09:59.909446955 CEST	49723	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:09:59.959532022 CEST	20221	49723	185.140.53.138	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:10:00.467593908 CEST	49723	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:10:00.515872955 CEST	20221	49723	185.140.53.138	192.168.2.7
May 12, 2021 19:10:01.077081919 CEST	49723	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:10:01.125736952 CEST	20221	49723	185.140.53.138	192.168.2.7
May 12, 2021 19:10:06.200220108 CEST	49724	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:10:06.248963118 CEST	20221	49724	185.140.53.138	192.168.2.7
May 12, 2021 19:10:06.843153000 CEST	49724	20221	192.168.2.7	185.140.53.138
May 12, 2021 19:10:06.893260002 CEST	20221	49724	185.140.53.138	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:09:23.519428968 CEST	56217	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:23.580670118 CEST	53	56217	8.8.8.8	192.168.2.7
May 12, 2021 19:09:23.810734987 CEST	63354	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:23.874382019 CEST	53	63354	8.8.8.8	192.168.2.7
May 12, 2021 19:09:24.114198923 CEST	53129	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:24.165884972 CEST	53	53129	8.8.8.8	192.168.2.7
May 12, 2021 19:09:25.360261917 CEST	62452	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:25.409053087 CEST	53	62452	8.8.8.8	192.168.2.7
May 12, 2021 19:09:26.311340094 CEST	57820	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:26.335422039 CEST	50848	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:26.376713037 CEST	53	57820	8.8.8.8	192.168.2.7
May 12, 2021 19:09:26.384167910 CEST	53	50848	8.8.8.8	192.168.2.7
May 12, 2021 19:09:26.754836082 CEST	61242	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:26.814997911 CEST	53	61242	8.8.8.8	192.168.2.7
May 12, 2021 19:09:28.012442112 CEST	58562	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:28.061568975 CEST	53	58562	8.8.8.8	192.168.2.7
May 12, 2021 19:09:29.286885977 CEST	56590	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:29.335742950 CEST	53	56590	8.8.8.8	192.168.2.7
May 12, 2021 19:09:30.482445002 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:30.534065008 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 19:09:34.885289907 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:34.937410116 CEST	53	53775	8.8.8.8	192.168.2.7
May 12, 2021 19:09:36.005516052 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:36.057012081 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 19:09:36.989403963 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:37.038420916 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 19:09:38.209544897 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:38.259511948 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 19:09:39.321352959 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:39.371000051 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 19:09:40.033440113 CEST	58739	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:40.095434904 CEST	53	58739	8.8.8.8	192.168.2.7
May 12, 2021 19:09:40.307174921 CEST	60338	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:40.356019020 CEST	53	60338	8.8.8.8	192.168.2.7
May 12, 2021 19:09:41.418868065 CEST	58717	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:41.469022036 CEST	53	58717	8.8.8.8	192.168.2.7
May 12, 2021 19:09:42.424104929 CEST	59762	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:42.475630999 CEST	53	59762	8.8.8.8	192.168.2.7
May 12, 2021 19:09:45.964047909 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:46.026415110 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 19:09:47.856292009 CEST	58052	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:47.920233965 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 19:09:47.953670979 CEST	54008	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:48.003284931 CEST	53	54008	8.8.8.8	192.168.2.7
May 12, 2021 19:09:49.054560900 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:49.103358030 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 19:09:49.995851040 CEST	52914	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:50.046638012 CEST	53	52914	8.8.8.8	192.168.2.7
May 12, 2021 19:09:51.704722881 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:51.756882906 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 19:09:52.970551968 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:53.019751072 CEST	53	52816	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:09:53.854290009 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:53.903247118 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 19:09:54.449297905 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:54.508183956 CEST	53	54230	8.8.8.8	192.168.2.7
May 12, 2021 19:09:54.806654930 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:54.856170893 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 19:09:56.734750032 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:56.785367966 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 19:09:59.847589970 CEST	50860	53	192.168.2.7	8.8.8.8
May 12, 2021 19:09:59.906244993 CEST	53	50860	8.8.8.8	192.168.2.7
May 12, 2021 19:10:06.137185097 CEST	50452	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:06.198914051 CEST	53	50452	8.8.8.8	192.168.2.7
May 12, 2021 19:10:11.983949900 CEST	59730	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:12.041466951 CEST	53	59730	8.8.8.8	192.168.2.7
May 12, 2021 19:10:18.562263966 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:18.625128984 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 19:10:20.379787922 CEST	51919	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:20.438606977 CEST	53	51919	8.8.8.8	192.168.2.7
May 12, 2021 19:10:27.426090956 CEST	64296	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:27.483361959 CEST	53	64296	8.8.8.8	192.168.2.7
May 12, 2021 19:10:32.676578999 CEST	56680	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:32.736129999 CEST	53	56680	8.8.8.8	192.168.2.7
May 12, 2021 19:10:37.929197073 CEST	58820	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:37.989478111 CEST	53	58820	8.8.8.8	192.168.2.7
May 12, 2021 19:10:50.111529112 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:50.174298048 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 19:10:55.205688953 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:55.275978088 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 19:10:58.786215067 CEST	52286	53	192.168.2.7	8.8.8.8
May 12, 2021 19:10:58.849198103 CEST	53	52286	8.8.8.8	192.168.2.7
May 12, 2021 19:11:04.038754940 CEST	56064	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:04.096352100 CEST	53	56064	8.8.8.8	192.168.2.7
May 12, 2021 19:11:09.754262924 CEST	63744	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:09.809561014 CEST	53	63744	8.8.8.8	192.168.2.7
May 12, 2021 19:11:15.814275980 CEST	61457	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:15.913336039 CEST	53	61457	8.8.8.8	192.168.2.7
May 12, 2021 19:11:16.497555971 CEST	58367	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:16.557554007 CEST	53	58367	8.8.8.8	192.168.2.7
May 12, 2021 19:11:17.198498011 CEST	60599	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:17.255631924 CEST	53	60599	8.8.8.8	192.168.2.7
May 12, 2021 19:11:17.736108065 CEST	59571	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:17.742290974 CEST	52689	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:17.811340094 CEST	53	59571	8.8.8.8	192.168.2.7
May 12, 2021 19:11:17.867028952 CEST	53	52689	8.8.8.8	192.168.2.7
May 12, 2021 19:11:18.442326069 CEST	50290	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:18.504839897 CEST	53	50290	8.8.8.8	192.168.2.7
May 12, 2021 19:11:19.367453098 CEST	60427	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:19.432298899 CEST	53	60427	8.8.8.8	192.168.2.7
May 12, 2021 19:11:19.943841934 CEST	56209	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:20.002940893 CEST	53	56209	8.8.8.8	192.168.2.7
May 12, 2021 19:11:20.919472933 CEST	59582	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:20.978926897 CEST	53	59582	8.8.8.8	192.168.2.7
May 12, 2021 19:11:22.055633068 CEST	60949	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:22.104902029 CEST	53	60949	8.8.8.8	192.168.2.7
May 12, 2021 19:11:22.648665905 CEST	58542	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:22.708687067 CEST	53	58542	8.8.8.8	192.168.2.7
May 12, 2021 19:11:30.994379997 CEST	59179	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:31.053859949 CEST	53	59179	8.8.8.8	192.168.2.7
May 12, 2021 19:11:36.273329973 CEST	60927	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:36.331198931 CEST	53	60927	8.8.8.8	192.168.2.7
May 12, 2021 19:11:41.509563923 CEST	57854	53	192.168.2.7	8.8.8.8
May 12, 2021 19:11:41.569755077 CEST	53	57854	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 19:09:23.810734987 CEST	192.168.2.7	8.8.8.8	0x4ac4	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
May 12, 2021 19:09:54.449297905 CEST	192.168.2.7	8.8.8.8	0x1750	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:09:59.847589970 CEST	192.168.2.7	8.8.8.8	0x8283	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:10:06.137185097 CEST	192.168.2.7	8.8.8.8	0xc9a2	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:10:27.426090956 CEST	192.168.2.7	8.8.8.8	0x6c9b	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:10:32.676578999 CEST	192.168.2.7	8.8.8.8	0xf3e3	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:10:37.929197073 CEST	192.168.2.7	8.8.8.8	0x73f8	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:10:58.786215067 CEST	192.168.2.7	8.8.8.8	0xaac1	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:11:04.038754940 CEST	192.168.2.7	8.8.8.8	0x4099	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:11:09.754262924 CEST	192.168.2.7	8.8.8.8	0xb7bf	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:11:30.994379997 CEST	192.168.2.7	8.8.8.8	0xd530	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:11:36.273329973 CEST	192.168.2.7	8.8.8.8	0xb88e	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 19:11:41.509563923 CEST	192.168.2.7	8.8.8.8	0x8659	Standard query (0)	wealth2021.ddns.net	A (IP address)	IN (0x0001)

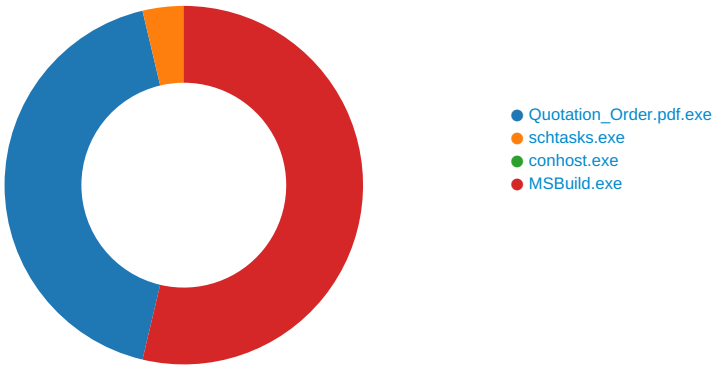
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 19:09:23.874382019 CEST	8.8.8.8	192.168.2.7	0x4ac4	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 19:09:24.165884972 CEST	8.8.8.8	192.168.2.7	0x42cc	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 19:09:54.508183956 CEST	8.8.8.8	192.168.2.7	0x1750	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:09:59.906244993 CEST	8.8.8.8	192.168.2.7	0x8283	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:10:06.198914051 CEST	8.8.8.8	192.168.2.7	0xc9a2	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:10:27.483361959 CEST	8.8.8.8	192.168.2.7	0x6c9b	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:10:32.736129999 CEST	8.8.8.8	192.168.2.7	0xf3e3	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:10:37.989478111 CEST	8.8.8.8	192.168.2.7	0x73f8	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:10:58.849198103 CEST	8.8.8.8	192.168.2.7	0xaac1	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:11:04.096352100 CEST	8.8.8.8	192.168.2.7	0x4099	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:11:09.809561014 CEST	8.8.8.8	192.168.2.7	0xb7bf	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:11:31.053859949 CEST	8.8.8.8	192.168.2.7	0xd530	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:11:36.331198931 CEST	8.8.8.8	192.168.2.7	0xb88e	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
May 12, 2021 19:11:41.569755077 CEST	8.8.8.8	192.168.2.7	0x8659	No error (0)	wealth2021.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Quotation_Order.pdf.exe PID: 3632 Parent PID: 5656

General

Start time:	19:09:28
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Quotation_Order.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation_Order.pdf.exe'
Imagebase:	0xb20000
File size:	845312 bytes
MD5 hash:	9EC5D09C8ADEFBF30598A5BD5F8D826E
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: 00000001.00000002.242494583.0000000003EB9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.242494583.0000000003EB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.242494583.0000000003EB9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.242066967.0000000002EB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.242708300.0000000004005000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.242708300.0000000004005000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.242708300.0000000004005000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown
C:\Users\user\AppData\Roaming\NzjsARuyfeoDS.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	6C3CDD66	CopyFileW
C:\Users\user\AppData\Roaming\NzjsARuyfeoDS.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C3CDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpAE98.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C3C7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation_Order.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D88C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAE98.tmp	success or wait	1	6C3C6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\NzjsARuyfeoDS.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 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 61 e7 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 36 0b 00 00 ae 01 00 00 00 00 00 0a 54 0b 00 00 20 00 00 00 60 0b 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 40 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...a..`.......... ....P..6...........T... ...`....@.. ....@ ....@................	success or wait	4	6C3CDD66	CopyFileW
C:\Users\user\AppData\Roaming\NzjsARuyfeoDS.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	6C3CDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpAE98.tmp	unknown	1662	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 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?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>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registrati	success or wait	1	6C3C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation_Order.pdf.exe.log	unknown	1314	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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D88C907	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	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile

Analysis Process: schtasks.exe PID: 4728 Parent PID: 3632

General

Start time:	19:09:33
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NzjsARuyfeoDS' /XML 'C:\Users\user\AppData\Local\Temp\tmpAE98.tmp'
Imagebase:	0xef0000
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\tmpAE98.tmp	unknown	2	success or wait	1	EFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpAE98.tmp	unknown	1663	success or wait	1	EFABD9	ReadFile

Analysis Process: conhost.exe PID: 4812 Parent PID: 4728

General

Start time:	19:09:33
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 5016 Parent PID: 3632

General

Start time:	19:09:34
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0xcc0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000005.00000002.505268694.00000000056C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.505268694.00000000056C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.505644430.00000000058D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.505644430.00000000058D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.505644430.00000000058D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.501077048.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.504649374.00000000041E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.504649374.00000000041E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.495341010.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.495341010.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.495341010.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D57CF06	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	6D57CF06	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	6C3CBEFF	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	6C3C1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C3CBEFF	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	6C3CBEFF	CreateDirectoryW

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	66 fe 2e 28 b4 15 d9 48	f..(...H	success or wait	1	6C3C1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D55CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	4096	success or wait	1	6D53D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	512	success or wait	1	6D53D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D555705	unknown

Disassembly

Code Analysis